# AFF

# Case

## 1AC

### Russia ADV

#### Advantage one is RUSSIA

#### A dramatic escalation of cyberattacks is imminent---they’ll attempt surgical strikes, but off-target effects guarantee broader damage that collapses critical infrastructure. This sets off an escalation spiral that risks nuclear use.

Frank Umbach 22, professor, researcher, consultant, European government advisor and prolific author, with expertise in energy security and cybersecurity, head of research at the European Cluster for Climate, Energy and Resource Security (EUCERS) at the Center for Advanced Security, Strategic and Integration Studies (CASSIS), University of Bonn; an adjunct senior fellow at the S. Rajaratnam School of International Studies (RSIS) at the Nanyan Technological University (NTU) in Singapore; and executive advisor of Proventis Partners GmbH, Munich, “Russia’s cyber fog in the Ukraine war,” GIS Reports Online, 6/16/22, <https://www.gisreportsonline.com/r/russia-cyber/>

Russia’s state-supported cyberattacks increased both before and during its invasion of Ukraine. The moves are part of Moscow’s broader attempt to disrupt services and create intimidation and confusion. Up until now, however, the Kremlin has not launched a devastating cyberwar against NATO countries, despite numerous warnings in recent months.

Western experts are still uncertain whether fears of American cyber retaliation and the existence of a “Mutual Assured Cyber Destruction” (“cyber-MAD”) are the reason why such attacks have not materialized. But any further Western sanctions (such as the European Union’s declared oil embargo on Russia) will increase the risk of devastating Russian cyberattacks.

Shared targets

On May 10, 2022, the European Union, United Kingdom and the United States officially attributed a February 24 cyberattack to Russia. One hour before the invasion of Ukraine, hackers had targeted the Viasat-operated KA-SAT satellite network to disrupt command and control of the Ukrainian military and government communications.

The disrupted internet access caused collateral damage to commercial and residential internet services. Thousands of modems across Central Europe lost their satellite connection. In Germany, 5,800 Enercon wind turbines could no longer be remotely monitored by their operators.

Since the invasion, Russian attacks have become more frequent and destructive. They are coordinated with the Kremlin’s military actions as part of its hybrid warfare against both Ukraine and the West. Its state-supported hacker groups began preparing for the conflict as early as March 2021, according to new reports on Russia’s relentless cyberattacks as part of its hybrid warfare against Ukraine. These cyber operations require careful planning, targeting and development, which requires months if not years.

In recent years, both the U.S. and EU have intensified their collaboration with Ukraine on cybersecurity. This is because Ukraine has become a testing ground for Russia’s advanced cyberattacks on critical infrastructure, and the West can learn much from Russian cyber strikes against Ukraine.

In 2015, Russia conducted its first deliberate cyberattack on Ukraine’s energy infrastructure and grid system. In 2017, the Kremlin-backed NotPetya virus, designed to disrupt financial, energy and government sectors in Ukraine, spread internationally and cost companies around the world over $10 billion in damages.

For the EU, strengthening the cybersecurity of Ukraine’s critical infrastructure has become increasingly important since the Ukrainian electricity grid is being integrated into the EU’s common electricity market and network (ENTSO-E).

The rising vulnerabilities of Western societies and economies have been highlighted in 2020 after the hack of a leading U.S. security tech company and its software (SolarWinds). It gave the Russian hacker group “Cozy Bear” (also called “Nobelium” or APT-29) access to thousands of companies’ data, as well as critical infrastructure in various countries. The targets of this hacker group are believed to reflect the Kremlin’s geopolitical interests and strategic priorities. Cozy Bear has increased its attacks against Ukraine from a mere six in 2021 to more than 1,200 this year, with particular focus on the Ukrainian government and its state agencies.

There are also lessons to be learned from the ransomware cyberattack on the 8,000-kilometer U.S. Colonial oil pipeline. In May 2021, hackers infiltrated the company’s information technology infrastructure and were able to disable the pipeline’s operation. The hack affected the oil supply for both private consumers and U.S. Armed Forces, leading to panic buying. The attackers stole nearly 100 gigabits of data and requested a ransom of 75 Bitcoin ($4.4 million at the time) to return access to the company’s billing system. The company eventually paid the ransom to the cyber hacker group DarkSide, despite the government’s efforts to prevent this. In response, the Biden administration passed the Strengthening American Cybersecurity Act (SACA) last March. It requires federal agencies as well as owners and operators of critical infrastructure to report cyberattacks within 72 hours and ransomware payments within 24 hours. But how to better mitigate threats and enhance resilience collectively across industries and sectors is not addressed in the SACA.

Mutual escalation

Since the war in Ukraine began, Russia’s state-backed cyberattacks against Western critical infrastructure have increased – by as much as 72 percent in the U.K. Alongside ever more Western sanctions and the increasing supply of heavy weaponry, NATO countries fear that Russia could escalate its nascent cyberwar with sophisticated strikes against critical infrastructure. NATO governments and the European Central Bank have repeatedly warned that the West should be prepared for this eventuality.

The Five Eyes intelligence-sharing network among the U.S., the UK, Canada, Australia and New Zealand stated in April that Russia was planning massive cyberattacks against Western countries supporting Ukraine. A dozen hacking groups were designated as threats, since they are part of, or close to, Russian intelligence and military institutions. They have the ability to anonymously compromise IT networks, steal large amounts of data, deploy destructive malware and bring down networks.

Last October, Microsoft warned in its 2021 Digital Defense Report that Russia was the state that posed the greatest cyber threat. Russian hackers are considered much more prolific than those from China, Iran and North Korea. In 2020, 58 percent of all state-backed cyberattacks identified by Microsoft came from Russia. Cozy Bear accounted for more than 92 percent of all detected Russian activity. Microsoft also warned that its attacks targeting enterprise VPN software have become up to 32 percent more successful. Attacks are mainly carried out as espionage and intelligence campaigns against government agencies and think tanks. The top target countries are the U.S., Ukraine, and the UK.

In March, the White House issued a strongly worded warning that Russia is planning major cyberattacks against the U.S. in retaliation for its harsh economic sanctions. In April, a U.S. federal advisory warned that hackers with ties to foreign governments are targeting specific industrial processes and their information and control systems, including the supervisory control and data acquisition devices to disrupt, sabotage and physically destruct them.

Last June, U.S. President Joe Biden, embarrassed by the SolarWinds hack and facing political pressure to retaliate against Russia, issued a warning to President Vladimir Putin. At the first bilateral cybersecurity summit since the Kremlin’s annexation of Crimea in 2014, Mr. Biden stated that 16 areas of critical infrastructure, including energy, health and water, should be “off-limits to attack” by cyberattacks or other means.

He also urged the Kremlin to take action against criminals conducting ransomware attacks. But bilateral cybersecurity cooperation has not made any significant progress since last summer. Illicit ransomware activities by criminal groups appear to have continued unabated. The trend goes hand in hand with the booming cryptocurrency industry, which provides anonymous digital assets that can be used for money laundering.

‘Cyber-MAD’ and cyber deterrence

Alongside diplomatic efforts to de-escalate cyber tensions between the West and Russia during the last few years, Western allies have warned Russia of “massive consequences” for its largest banks and trading companies in the case of escalating cyberwarfare against NATO and EU countries.

Despite Russia’s undeniable offensive cyber capabilities, the Kremlin has not initiated any larger devastating cyberwar against the West since its military invasion began – despite unprecedented sanctions.

One explanation could be that both the U.S. and NATO have stated that a highly damaging cyberattack on any member of the alliance could trigger Article 5 of the treaty, which guarantees mutual defense. This could indicate that some form of “cyber MAD” still functions between the U.S. and Russia. Many cyber experts have warned that the West cannot afford to bet on that as a deterrent. However, defining a more assertive cyber retaliation strategy must also consider the possibility of an escalatory spiral that could even result in Russia resorting to use nuclear weapons, even perhaps preemptively.

During its 2014 annexation of Crimea, Russia learned that it is much more difficult to conduct a surgical cyber strike than an indiscriminate one. If the Kremlin decides to directly attack major Western infrastructure, it will face retaliation. But the situation could also escalate because Russia might not always be able to control its own cyber operations on selected targets, potentially leading to unwanted escalation and collateral damages far beyond what was initially intended.

Since the beginning of the war, Russia itself has become the target of numerous international pro-Ukraine cyber groups and hackers, shattering illusions of Moscow’s cyber superiority. Cyberattacks on the Russian government and military institutions have increased significantly. The active Anonymous group has stolen hundreds of millions of documents from governmental and industrial websites, including the Ministry of Defense. Others have blocked or slowed freight trains carrying Russian military equipment or tampered with the automatic ticket system for passengers.

Ukraine itself has built an “army” of IT volunteers (like Network Battalion 65) to protect the country against Russian hackers, but also to launch counter operations against Russian cyber threats. The Ukrainian cybersecurity company Hacken claims that 10,000 hackers from 150 countries have volunteered to disrupt Russian media sites and promote pro-Ukrainian messages across Russian social media.

But these international and private Ukrainian hacker groups have acted without any kind of coordination, in contrast to Russia’s state-supported cyber groups controlled by the foreign intelligence agency (SVR) or the military intelligence agency (GRU). Hence, the impact of these international cyberattacks against Russia has yet not been significant enough to shift the Kremlin’s cost-benefit calculation of its invasion of Ukraine.

Scenarios

Russia’s red lines and escalation strategy could further change in the weeks and months ahead. How the military, political and economic aspects evolve, and war aims change will influence how the Kremlin decides to use its cyber capabilities in the conflict.

Beyond the Russian-Ukrainian war, if adversarial threats increase, so too will the vulnerabilities, as the world increasingly relies on digital technology. In 2021, a record-breaking number of cyberattacks took place – a 50 percent increase from the previous year according to the cybersecurity firm Check Point Research. New forecasts suggest that 2022 could be even worse. Cyber threats to civilian and military critical infrastructure are likely to multiply and grow even more consequential as the digital and physical worlds become increasingly intertwined. While awareness of the need for cyber resilience has grown in the West, it is too little to prevent disastrous cyberattacks on critical infrastructure.

#### Russia’s aggressive---they won’t stop at Ukraine. Getting response policy in order in advance is key.

Thomas D. Grant 22, served as Senior Advisor for Strategic Planning in the Bureau of International Security and Nonproliferation at the U.S. Department of State, 2019-2021, “No Respite: Why Putin’s Nuclear Threats Must Not Deter the Defense of the Free World,” Real Clear Defense, 3/3/2022, https://www.realcleardefense.com/articles/2022/03/03/no\_respite\_why\_putins\_nuclear\_threats\_must\_not\_deter\_the\_defense\_of\_the\_free\_world\_819782.html

As Vladimir Putin’s war of aggression against Ukraine enters its second week, the Russian autocrat escalates his threats of nuclear war. Some policy commentators say this means we should look for easy “offramps” that Putin can exploit to save his failing régime. They are badly mistaken. There are no offramps for Putin now, and trying to build them for him will only invite far more dangerous aggression.

Putin’s invasion has not gone according to plan. No swift victory came from his opening salvo: murder squads pre-positioned in Kyiv and an airborne attack on Antonov Airfield did not decapitate the democratically elected government of President Volodymyr Zelenskyy. A week later, the supply train for Putin’s troops is in shambles, and Russian army units are reportedly running out of food and fuel. The Russian air force has not established uncontested control of Ukraine's airspace. As yet unclear is whether Ukraine’s Bayraktar drones will outdo those Azerbaijan employed in 2020 to devastating effect against Armenia, but they already have had an impact; and Russia is only now encircling Kharkiv and Kyiv with rocket launchers and their supply elements, creating a truly target-rich environment for the defenders’ unmanned systems. Most seriously at variance with Putin's plan, Ukraine's army and citizens are resisting with ferocity, and nobody has ousted Ukraine's leaders as Putin implored unnamed persons in Kyiv. Reports that at least some Russian soldiers are refraining from fighting when they meet Russian-speaking Ukrainians in the east should be as alarming to Putin as drone strikes, Javelins, or the prospect of a drawn out war against a nation with a history of partisan resistance second to none in the world. Meanwhile, with unprecedented speed and strength, international sanctions are starting to throttle the Russian economy.

Experts on Russia’s armed forces note that Russian military doctrine calls for escalation, at least to the level of tactical nuclear weapons, when a conventional operation fails. Putin’s conventional operation in Ukraine is failing. Moreover, Putin has raved that a threat to his régime is a threat to Russia’s very existence, and he says Russia will use strategic nuclear weapons if confronted with an existential threat. These are not considerations to be taken lightly. It would be foolish to blunder into escalation if nothing else were at stake and if an obvious way out—an "offramp"—were readily available. The problem is, the stakes are enormous, and there is no offramp for Putin.

Emboldening the aggressor

If the West resiles from supporting Ukraine, then Putin will return emboldened to pursue even more audacious aggression. This is not speculative. He has rambled in speeches for years about the loss of the Russian Empire—not just the Soviet Empire but also the Tsarist one. Indeed, his aesthetic sensibilities and ostentatious embrace of the Russian Orthodox Church suggest that Putin takes the pre-1917 Empire as his preferred model. He makes threats against Poland, the largest part of which belonged to Russia before 1917, and the Baltic States, all of which were in the Tsar's Empire before Stalin forcibly seized them again in 1939 in collusion with Hitler. Kazakhstan has also drawn Putin's ire with a substantial Russian-speaking population like Ukraine but vastly more natural wealth. The Kremlin leader dismisses that country too as non-existent and lacking any real sovereignty. Once a grand duchy of the Tsar's, even Finland has not escaped Putin's attention. His government has threatened unspecified military actions in response to Finland’s expression of concern over Russia’s aggression. Putin’s declarations about lost territories and the grandeur of the Russian past indicate his real aims. He was not bluffing about Ukraine. It would be folly to conclude that he is bluffing about his further territorial ambitions. His ambitions will not disappear if the West finds a way out for him from his current war of aggression. Nor will his ability to make nuclear threats.

Putin’s revanchism is not limited to taking territory from neighboring countries whose borders Russia solemnly and bindingly recognized as settled and final at the end of the Cold War. Putin seeks vengeance against a wide ranging and relatively abstract set of institutions and ideas. Western democracy and the rule of law are the key enemies in Putin's worldview. The European Union and NATO are the institutional expressions of those ideas. Perverse as it sounds, a war aim of Putin's in Ukraine might well be to instigate the largest refugee crisis in Europe since 1945. Some 600,000 people had already fled Ukraine by March 1st. The Office of the United Nations High Commissioner for Refugees estimates that Russia’s war against Ukraine might result in 4 million refugees. It is a mistake to assume that this is only a byproduct of Putin’s aggression. It could well be one of Putin’s main goals. Refugees in such numbers would place an enormous strain on the governments of Europe and on the union that Putin considers to be inimical to his régime. This atrocity, too, and more like it in the future, Putin can perpetrate only if he cows the West through threats of nuclear war.

Indeed, his nuclear threats are the only means available to Putin that could possibly enable him to realize his aims in the face of the concerted effort that we now see emerging against him. He calculates that the world will back off, and then he can return when he is ready and take whatever lands he declares are his and inflict whatever harm on people and institutions he chooses. The very scope of Putin's aims must lead us to temper the horror and revulsion we naturally feel when Putin brandishes Russia’s nuclear weapons. Consider what will follow if we allow Putin respite and he wins time to lick his wounds. It is inconceivable that he will not come back—and soon—for more. This could mean completing the destruction of whatever part of Ukraine is still intact. It could also mean—and almost inevitably will in time—escalating his threats and moving against the Baltic States, Poland and others still. Then there is Putin’s role as chief in a régime of oligarchs, a role that will grow if he is allowed to resume exploiting international trade and investment for that régime’s kleptocratic purposes. His subversion of western democracies will not cease either.

None of these lines of attack are distant hypotheticals. They are underway already or are logical extensions of what Putin has already done. The question is whether he will get a chance to continue his aggression at a future date in future places. If he does, then the nuclear risk will be greater, not less, than it is today because Putin will need the nuclear threat more, not less, the further his assault on the free world goes.

#### A full-scale NATO response risks nuclear escalation

Erica Longergan & Keren Yarhi-Milo 22, Lonergan is an assistant professor in the Army Cyber Institute at West Point and a research scholar at the Arnold A. Saltzman Institute of War and Peace Studies at Columbia University; Yarhi-Milo is the Arnold A. Saltzman Professor of War and Peace Studies in the political science department and the School of International and Public Affairs, “Cyber Signaling and Nuclear Deterrence: Implications for the Ukraine Crisis,” War on the Rocks, 4/21/22, <https://warontherocks.com/2022/04/cyber-signaling-and-nuclear-deterrence-implications-for-the-ukraine-crisis/>

From its opening moments, the conflict in Ukraine has involved a nuclear dimension. On Feb. 24, Russian President Vladimir Putin ominously warned of “consequences you have never seen” if other countries tried to get involved in Ukraine — an implied nuclear threat. Several days later, Putin announced that Russia’s nuclear forces would be put on a “special combat readiness” status. More recently, Dmitry Medvedev, a senior Russian official, warned that if Finland and Sweden join NATO, “there can be no more talk of any nuclear-free status for the Baltic.”

So far, the Biden administration has attempted to dismiss Russia’s announcement as irresponsible saber-rattling. But as Putin continues issuing nuclear threats, policymakers are likely to feel growing pressure to respond. In particular, they may be tempted to find ways to signal to Russia to deter the use of nuclear weapons. One way this might be done is through cyber operations. In fact, some cyber experts are already calling for the United States to consider cyber attacks for signaling purposes. For example, writing in the Washington Post, Dmitri Alperovitch and Samuel Charap call on the Biden administration to consider a cyber “shock-and-awe demonstration” in response to a major Russian cyber attack against the West. They claim that such a response, which could include disrupting the Internet throughout Russia, would signal U.S. resolve and help prevent further escalation that they fear “could result in nuclear war.”

However, conducting cyber operations to signal deterrence would, paradoxically, increase risks of escalation. This risk is not just hypothetical, especially in light of Russia’s updated declaratory policy for the first use of nuclear weapons, which may include responses to cyber attacks. Russia has reinforced this message during the war in Ukraine. In early March, a hacking group affiliated with Anonymous claimed that it had shut down the control center of Russia’s space agency. While denying that the attack took place, Russia nevertheless warned that a cyber attack against its satellites would be a justification for war.

The Biden administration should clearly communicate that cyber operations for nuclear signaling are out of bounds, just as it declared restraint in other aspects of this conflict, like the deployment of American troops to Ukraine.

How Cyberspace Is Creating Nuclear Risks

Policymakers and academics are attuned to the cyber risks to nuclear command and control. The practitioner community has largely focused on U.S. vulnerabilities and how to mitigate them. Scholars, in turn, worry about how cyber operations could have unintended escalatory consequences. But less attention has been paid to another likely scenario: the use of cyber operations for signaling purposes (operations with visible effects that aim to convey a message to another state) in a nuclear context. The ambiguity of cyber operations can sometimes be useful for signaling — but the same ambiguity can be dangerous during a nuclear crisis. The problem is that civilian leaders in particular, distinct from the military, are inclined to see cyber attacks as effective signaling tools.

Cyber operations could have nuclear implications, especially because modern nuclear command and control systems, like those in Russia and the United States, are becoming increasingly dependent on digital infrastructure. Nuclear command, control, and communications systems, which include early warning, information collection, and communications capabilities, alert decision-makers to impending nuclear strikes and also enable leaders to control decisions about nuclear use (or non-use). But their digital dependencies are creating opportunities for exploitation using cyber means. In a 2020 report, the Nuclear Threat Initiative found that “almost 9 out of 10 planned nuclear modernization programs involve at least some new digital components or upgrades.”

Vulnerabilities inherent in the digital infrastructure that undergird modern nuclear systems provide opportunities for actors to engage in cyber espionage — gaining access to a network or system to steal information — or even conduct cyber attacks. Hypothetically, a cyber power like Russia could conduct a cyber attack against a U.S. early warning satellite to degrade its functionality. This has become an urgent concern for practitioners. U.S. Strategic Command, for instance, is currently working to “operationally harden NC3 systems against cyber threats.” Congress has also gotten involved, requiring the Defense Department to evaluate the cybersecurity of major weapon systems. And the Government Accountability Office has published multiple reports decrying the state of cybersecurity and scope of vulnerabilities of weapon systems, including elements of the nuclear triad.

From an academic perspective, scholars have investigated how cyber operations targeting nuclear systems could exacerbate escalation risks. Focusing on nuclear forces, early research, such as work by Martin Libicki, was skeptical of the dangers posed by cyber operations. Nuclear forces were seen as being largely immune from digital attacks because they were “air gapped,” meaning that they were separated from information technology systems.

However, as nuclear systems have become increasingly intertwined with the digital environment — not to mention the dual-use nature of many elements of nuclear command, control, and communications systems (like early warning or position, navigation, and timing satellites) — the protection offered by being segregated from the internet is less robust. Jacquelyn Schneider, Benjamin Schechter, and Rachael Schaffer, for instance, ran a series of wargames demonstrating that decision-makers in hypothetical crises are likely to use their cyber exploits against an adversary’s nuclear systems. They found that this could have negative effects on states’ respective nuclear strategies, especially decisions to pre-delegate nuclear launch authority or automate nuclear responses. Erik Gartzke and Jon Lindsay argue that the clandestine nature of cyber operations means that one state could secretly gain access to an adversary’s nuclear command, control, and communications systems, giving the former an information advantage or even creating an incentive for the latter to use its nuclear weapons out of the fear that it may lose them. James Acton notes that the difficulties of distinguishing between cyber espionage and attack could lead a state to misperceive the intent behind a cyber operation, generating a similar “use it or lose it” calculus.

#### It causes global posture shifts that make accidental nuclear use far more likely.

Erica Longergan & Keren Yarhi-Milo 22, Lonergan is an assistant professor in the Army Cyber Institute at West Point and a research scholar at the Arnold A. Saltzman Institute of War and Peace Studies at Columbia University; Yarhi-Milo is the Arnold A. Saltzman Professor of War and Peace Studies in the political science department and the School of International and Public Affairs, “Cyber Signaling and Nuclear Deterrence: Implications for the Ukraine Crisis,” War on the Rocks, 4/21/22, <https://warontherocks.com/2022/04/cyber-signaling-and-nuclear-deterrence-implications-for-the-ukraine-crisis/>

The problem is that, more often than not, cyber operations are ambiguous signals. There is evidence that states can use cyber operations under some (narrow) conditions to signal a desire to de-escalate international crises. But these findings do not extend well to nuclear crises where clarity, rather than uncertainty, is important for stability. The use of cyber operations to defuse crises have involved cyber signaling short of war, not during an ongoing conventional conflict involving nuclear powers. And they have not involved cyber operations targeting a state’s nuclear command and control where states, like Russia, have already staked out declaratory policies. Moreover, states are still at a nascent stage in developing shared indices to inform assessments of intent in cyberspace, especially when it comes to cyber operations in nuclear crises.

Therefore, even if Russia would not take the cataclysmic step of escalating to the first use of nuclear weapons in response to a U.S. cyber operation, it could misinterpret U.S. signaling efforts and take measures to make nuclear use easier (such as making warheads operational, dispersing forces, pre-delegating authority, or increasing automaticity). These readiness measures could increase the chances of inadvertent or even accidental escalation.

The Biden administration has been commendable in clearly and consistently communicating to Russia, and other audiences, what the United States will not do in the Ukraine crisis — like sending American forces to Ukraine or establishing a no-fly zone. In addition, the administration should be equally clear about what is off the table in cyberspace — what Jacquelyn Schneider has termed a “strategic no-first-use” policy in cyberspace. Specifically, the United States should unequivocally convey to Russia that it will refrain from taking actions in cyberspace during this crisis that would undermine nuclear stability, such as conducting disruptive cyber-attacks against early warning satellites. This is different — the opposite, in fact — from drawing “red lines” in cyberspace, which are meant to deter unwanted behavior but can often backfire. Instead, the United States should communicate where it will exhibit restraint in cyber operations — a form of confidence-building. This could be conveyed publicly through statements by administration officials, similar to statements that Biden has made about other aspects of America’s role in Ukraine. It could also be privately communicated through ongoing backchannels taking place between U.S. allies, like France, and Russia.

There are also policy implications beyond the Ukraine conflict, especially in an environment in which the United States confronts potential future crises with other nuclear powers. In particular, senior national security officials have repeatedly emphasized that China represents a “pacing challenge” for the United States, including across the nuclear and cyber realms. In fact, Gen. Nakasone recently announced the creation of a China Outcomes Group under Cyber Command and the NSA. And researchers have identified how hypothetical crises involving the United States and China could escalate along dangerous trajectories, including to the use of nuclear weapons. The consequences of misunderstanding the utility of cyber signaling in this area are significant. Therefore, policymakers must consider how to improve civil-military coordination and cohesion so that the employment of military cyber power — especially when used against sensitive adversary systems, particularly nuclear ones, during delicate periods — is not out of sync with strategic objectives. The United States should also develop a more robust effort to clarify to adversaries, including China, how it will constrain its own behavior in cyberspace specifically during nuclear crises. The potential implications of misperceptions surrounding cyber operations targeting nuclear systems during a future crisis with a nuclear-armed adversary are simply too significant.

#### Even without escalation, successful attacks trigger a ‘black start’ scenario---distinct from blackouts AND an existential risk

Benjamin Monarch 20, University of Kentucky College of Law, J.D. May 2015, LLM in Energy, Natural Resources, and Environmental Law and Policy from the University of Denver Sturm College of Law, Deputy District Attorney at Colorado Judicial Branch, and Term Member at the Council on Foreign Relations, “Black Start: The Risk of Grid Failure from a Cyber Attack and the Policies Needed to Prepare for It,” Journal of Energy & Natural Resources Law, vol. 38, no. 2, Routledge, 04/02/2020, pp. 131–160

In the industrial world, when a switch is flipped, we take for granted that it will produce light, boot a computer, illuminate a stadium or activate a power plant. We know, of course, that power losses can and do occur. Many of us have lit candles during a thunderstorm or brought out extra blankets when a blizzard takes down transmission lines. As of this writing, the most populated state in the United States, California, is experiencing rolling blackouts.1 Yet even in prolonged power outages, we expect that electricity will be restored and, consequently, life will return to normal. Perhaps we need ask, however, what if power cannot be restored in a timely manner? Concern is growing that in the not-too-distant future our electricity supply could be irreparably compromised by a cyber attack. The issue when considering a systemic grid failure of this nature is twofold: how did we reach a point where something so critical to routine life now presents an existential threat, and what can we do to mitigate the risk of a catastrophic grid attack?

This article posits that the emergence of cyber attacks on industrial control systems, as a means of war or criminal menace, have reached a level of sophistication capable of crippling those systems. This article argues that a new grid security policy paradigm is required to thwart catastrophic grid failure – a paradigm that recognises the inextricable link between commercial power generation and national security. In section 5, seven policy recommendations are outlined that may, in part, mitigate a future where grid attacks pose existential risk to nations and their citizenry. Those recommendations are: first, develop a comprehensive insurance programme to minimise the financial risk of grid disruption; second, train more cybersecurity professionals with particular expertise in industrial control systems; third, institute a federally mandated information-sharing programme that is centralised under United States Cyber Command; fourth, subsidise and/or incentivise cybersecurity protections for small to mid-size utilities; fifth, provide university grants for grid security research; sixth, integrate new technologies with an eye towards securing the grid; and, lastly, formulate clear rules of engagement for a military response to grid disruption.

The purpose of this article is to provide the reader with an introduction to this complex topic. It is the aim of the author to give orientation to this issue and its many branches in the hope that better understanding will animate further curiosity and, ultimately, positive action on the part of the reader. Although many skilled and earnest people work tirelessly to prevent a grid failure scenario, it is essential that more be added to their ranks each day. Advisors, engineers, regulators, private counsel to power generators, and many others who play roles in electric power production are crucial to this subject. So, while this article provides entrée to the topic of grid security, its long-term objective is to spur action by the entire energy-related community. In the end, no one is immune to consequences of grid failure and, therefore, everyone is responsible, in part, for promoting grid integrity.2 In this regard, lawyers who represent various actors in the energy sector are going to be faced with questions and potential legal risks of a magnitude that they have never experienced before.

1.2. Turning the power back on in a powerless world

‘Black start’, not to be confused with the term ‘blackout’, is the name given to the process of restoring an electric grid to operation without relying on the external electric power transmission network to recover from a total or partial shutdown.3 At first glance, this description is unremarkable, but it implies a disturbing catch-22 – how might one restore power if the entire external transmission network is compromised?

If an electric disruption occurs at a household level, some homes may be equipped with a modest gasoline generator to temporarily restore power. If a hospital loses power, it will almost invariably be resupplied by automatic, industrial-scale generators. These micro considerations hardly give anyone pause; they are hiccups on a stormy night or a snowy day. In other words, their ‘black start’ is a quick and effective process for restoring power. But what happens, at a macro level, when an electric grid supplying power to large portions of the United States goes black, or worse, what happens if all of the United States’ electric grids go down simultaneously?4 In that scenario, how might enough non-grid power be harnessed and transmitted to turn the United States’ lights back on? Moreover, how might such a catastrophe occur in the first place? Perhaps the more ominous question is not how, but whether or not we can survive such circumstances if they persist in the long term.

The United States electric grid (‘the grid’) is the ‘largest interconnected machine’ in the world.5 It consists of more than 7000 power plants, 55,000 substations, 160,000 miles of high-voltage transmission lines and millions of low-voltage distribution lines.6 The scale and complexity of the grid in the context of the modern digital world are beyond comprehension because within it are innumerable industrial control systems; incalculable connections to digital networks; millions, if not billions, of analogue or digital sensors; many thousands of human actors; and trillions of lines of programming code.7 Further complexifying the grid is that it is comprised of generations of technologies, stitched together in ways that are not inherently secure in a world of cyber threats.8 The vastness of the grid makes security of it challenging. Likewise, the vastness of the grid makes the opportunities for intrusion seemingly infinite.

By any measure, grid failure will unleash a parade of horrors. Stores would close, food scarcity would follow, communication would cease, garbage would pile up, planes would be grounded, clean water would become a luxury, service stations would yield no fuel, hospitals would eventually go dark, financial transactions would stop, and this is only the tip of the iceberg – in a prolonged grid failure social chaos would reign, once-eradicated diseases would re-emerge and, increasingly, hope of returning to a normal life would fade.9 The notion of complete grid failure, once relegated to science fiction comics or James Bond movies, is now not only possible but also one of the most pressing national security threats today.10

Attacks on electric facilities are already occurring. In 2017, Duke Energy Corporation, one of the United States’ largest electricity producers, recorded more than 650 million cyber attempts to breach its utility systems.11 Duke Energy provides electricity to 7.6 million customers in six states.12 Aside from the obvious risk that a successful breach poses to Duke Energy, the effort to combat these attacks is costing the company hundreds of millions of dollars in security upgrades.13 Duke Energy is not alone; according to a recent study conducted by the cybersecurity firm BitSight, about ten per cent of electric utility companies are infected by malware.14 Perhaps one the most worrisome instances of a cyber intrusion came recently when a Kansas nuclear facility was hacked – the perceived purpose of the hack remains either unknown or undisclosed.15

Thus far, intrusions into United States grid assets have not resulted in damage to such facilities (or, at least, such an event has not been disclosed). These events are often classified as ‘surveillance’ tactics, not disruptive.16 However, evidence abounds of utility hacks that have resulted in real-world, negative impacts. In 2015, a ‘Russian intelligence unit shut off power to hundreds of thousands of people in western Ukraine’.17 Although the power was only off for a few hours, American investigators discovered similarities between the Ukraine disruption and surveillance of comparable United States utilities.18 A year later, in 2016, Ukraine was attacked again, and the results were similar to those of the 2015 attack.19 However, the sophistication of the reconnaissance and the attack method had improved noticeably.20 Events like this are not unique to Ukraine; for example, a petrochemical plant in Saudi Arabia was attacked in 2017.21 That breach focused on the safety control system of the plant, which could have resulted in wide-scale destruction and/or deaths of plant workers.22 In the past several weeks, reports of Iranian attacks on United States grid operations have been disclosed.23 These are just a few publicised incidents, and they illustrate the breadth of the threat and the potential consequences facing industrial nations. Should an attack akin to the Ukraine intrusion come to fruition in the United States, the results could be catastrophic in scope.

In light of the severity of this risk and the ever-growing likelihood of attack success, nations must take immediate action to both prevent a blackout scenario and, if needed, be prepared to confront a black start. Blackouts are troubling in their own right, but the crux of this entire topic rests on one overarching concern – when faced with a black start, how will power be restored and how long will it take? A blackout lasting a few hours is very different from a blackout that lasts weeks or months. Thus, the lynchpin in thinking about grid security is how to prevent a failure so that we may avoid the immense challenges that would surely follow.

In the coming sections, this article will explain why we find ourselves faced with this troublesome challenge. It will also delve into some of the technical aspects of grid security as well as offer a step-by-step look at how an attack occurs. Finally, this article will provide solutions aimed reducing the peril of a black start reality.

2. A brief history of the grid and what threatens it

2.1. How the United States produces and distributes power

The power transmission grid of the United States at its most expansive level is known as the North American Reliability Councils and Interconnections (or, as it is commonly called, the ‘North American Grid’).24 The North American Electric Reliability Corporation (NERC) governs the North American Grid.25 The North American Grid includes two major and three minor NERC interconnections, which extend as far north as Alaska and as far south as Baja California near Mexico.26 In effect, the United States and Canada share power through various interconnection networks.27

The contiguous United States grid is generally comprised of three distinct grid systems.28 The Eastern Interconnection grid comprises most of the Great Plains eastward to the Atlantic coast (excluding Texas).29 The Western Interconnection includes the Rocky Mountain States, portions of the Great Plains, and all states westward to the Pacific Ocean (excluding Texas).30 Finally, the Electric Reliability Council of Texas (ERCOT) covers most of Texas.31 These interconnections make up the electric power system of the contiguous United States.32 For purposes of considering grid failure, it is critical to note that the three interconnections discussed here function as largely independent systems with limited exchanges of power between them. Thus, when the phrase ‘grid failure’ is used, it could refer to the failure of one of these interconnections, all of these interconnections or some combination of them.

Each of the aforementioned interconnections has a grid architecture that is similar and is generally divided into two categories: the ‘bulk power system, often referred to as the “transmission grid,”’ and the smaller distribution grids.33 The bulk power system is the backbone of the grid. ‘It connects high-capacity power plants, transmission wires and substations that collectively generate and transport huge quantities of electricity over hundreds or thousands of miles’.34 At this macro level of power generation and transmission, regulatory standards are at their most uniform and strongest. Moreover, at the bulk power system level, most security regulations are mandatory, which yields consistent safeguards across large swathes of the grid.35 Collaboration among utility companies at the bulk power system level is often proficient, and their cybersecurity practices are often cutting edge. This is not to suggest, however, that the bulk power system is impervious to disruption.

The bulk power system has three fundamental weaknesses. First, even with the most advanced cybersecurity monitoring technology and personnel resources to prevent an attack, it can still be hacked.36 Second, an attack on the bulk power system could have systemic ramifications given its overall importance to power generation and transmission throughout the United States. Third, the bulk power system is integrated with smaller distribution grids that are far less secure. This characteristic creates a weak link in even the best cyber defence of the bulk power system because the smaller distribution grids are less secure against cyber intrusion.37

The smaller distribution grids (ie the non bulk power system) that are connected to the transmission grid are key in delivering electricity to homes and businesses. Additionally, smaller utility companies, as opposed to the corporations that manage the bulk power system, readily manage these smaller distribution networks.38 To put this in some context, the United States has approximately 3000 utilities, and many of those oversee small portions of the overall grid.39 With fewer resources than large public utilities as well as fewer regulatory safeguards, small utilities companies are less equipped to thwart cyber attacks.40 Hackers, notably those connected with Russia, have taken notice of this fact and have exploited smaller, weaker utilities.41 These utilities ‘have trouble finding sufficiently skilled workers who understand how the computerized and physical components of the grid work together and how to protect them’.42 Although bigger utility companies often establish best cyber defence practices, smaller utility companies either cannot afford or are not inclined to adopt those protections.43 The only upside when assessing the vulnerabilities of smaller distribution grids is that if an attack is limited to a single, minor grid, then the attack will likely have fewer negative consequences.

While efforts are underway to promote better cyber defence management across the entire grid, small or large, another element of power generation and distribution poses a risk: the grid component supply chain. All utilities rely on complex, global supply chains for equipment and software.44 It is not easy nor is it customary to ensure the integrity of each component of grid technology. For instance, an industrial control system in a safety component of a power planet may have software developed in Germany and hardware developed in China. Unbeknownst to the utility, the Chinese hardware may be equipped to provide Chinese hackers with backdoor access to the device because of an undetected bug in the German software. This scenario could, in effect, give Chinese hackers direct and surreptitious control of the safety equipment. This type of intrusion is known as ‘phoning home’.45 The burden and cost that would be inflicted upon utility companies to inspect integrity at each step of their supply chains is significant.46

Thankfully, the federal government has recognised the supply chain dilemma and has taken steps to mitigate this danger. The Committee on Foreign Investment in the United States (CFIUS), which is an inter-agency committee of the federal government, promotes national security by regulating foreign commercial efforts to influence United States business.47 In 2018, Congress expanded CFIUS’ authority by passing the Foreign Investment Risk Review Modernization Act (FIRRMA).48 Among many expansions of authority, FIRRMA equipped CFIUS to review transactions that may impact ‘critical infrastructure’ such as the grid.49 While this is an improvement, the change does not go so far as to give CFIUS authority over vendor relationships that lack an investment component.50 Thus, utility companies, large and small, continue to rely on technology from third-party vendors that may contain exploitive features that permit grid disruption.

In effect, the United States grid is a patchwork quilt of digital and physical technology from innumerable sources. To provide absolute cyber defence of this system would require surveillance and analysis of every single component of the grid, yet it is impossible to even properly inventory every single component of the grid let alone monitor it perfectly.

To add further complexity to the grid, new technology is emerging each day that expands the vectors of potential cyber attacks. The phrase ‘Internet of Things’ is used to describe physical devices that are linked to Internet communication systems.51 An example of an Internet of Things device would be a refrigerator that automatically orders more avocadoes from Amazon when only one avocado remains within it.52 This may seem like an innocuous and overall convenient approach to modern life, but such devices pose immense security challenges.

In the world of electricity distribution, Internet of Things instruments often come in the form of so-called ‘smart meters’.53 A smart meter is a device that monitors electricity consumption in real time and relays that information back to consumers and/or utilities.54 This is done through a two-way communication system, much like the download/upload function of a smart television.55 Smart meters also have the ability to decrease or increase energy supply based on real-time energy-demand monitoring.56 It is expected that 588 million smart meters will be installed worldwide by 2022.57

The problem here is the vast amount of infrastructure needed to support such a setup. Any smart electric grid needs a parallel telecommunications network to collect and harness the volumes of data it will generate, and that makes every connected thermostat or smart refrigerator a potential entry point for cyber intruders.58

The bottom line is that Internet of Things devices have the potential to transform the ‘largest interconnected machine in the world’ into a machine that is infinitely more complex and more vulnerable that it is presently. That being said, if smart grid technology is developed with grid security as a fundamental objective then it may afford greater security, rather than less.59

Finally, no understanding of the grid is complete without a glimpse at its regulator. The US Department of Energy is the principal federal agency responsible for regulating the nation's electricity generation and distribution system. The specific division of the Department of Energy tasked with grid integrity is the Office of Electricity Delivery & Energy Reliability (OEDER).60 The OEDER works in coordination with other federal agencies tasked with cybersecurity matters, but it spearheads the Department of Energy’s planning and implementation of grid security. The OEDER Multiyear Plan for Energy Security Cybersecurity (‘plan’), released in March 2018, details how the federal government will deepen partnerships with energy sector producers – notably, however, the plan states that ‘energy owners and operators have the primary responsibility to protect their systems from all types of risk’.61 The plan states that it has three priorities: first, strengthen energy sector cybersecurity partnerships; second, coordinate cyber incident response and recovery; and, third, accelerate game-changing research and development of resilient energy delivery systems.62

Among the Department of Energy's various grid security concerns, one overarching point of frustration is the high cost that energy providers must absorb to protect their utilities. In 2015, cybercrime attacks generated an average direct cost per company of $27 million per year, which is added on top of the $150 million to $800 million spent by the average utility to protect its assets.63 Moreover, these costs are increasing at approximately 11 per cent per year.64 At the present time, there is little reason to believe that the US federal government will absorb some or all of these costs, although efforts are underway to nationalise grid security protocols.65

The Department of Energy may have the most direct regulatory authority over the electric grid, but as the grid becomes more elemental to broader national security concerns, oversight of the grid will broaden to other federal agencies. In the event of a crippling grid attack, the United States would face three overarching issues: first, there would be a national security issue related to defending the United States from a potential aggressor; second, there would likely be immediate and severe economic disruption; and, lastly, there would be social dislocation and a burden placed on emergency services.66 Due to these concerns, federal management of the grid is likely to expand beyond the purview of the Department of Energy and become more of an interagency concern.67 This is already occurring, but as grid attacks multiply the interest of a wider government role becomes essential. The principal agencies that will likely continue to expand their authority over grid management are the Department of Homeland Security, Department of Defense, Department of Commerce and Department of the Treasury. This underscores the fact that the electric grid is essential to multiple facets of modern life. It is in effect a keystone to national security, and to economic and social normalcy.

2.2. What are cyber attacks, and how do they impact the grid?

Cyber attacks manifest in numerous ways, from credit-card-data heists to physical destruction of uranium enrichment facilities.68 Because of this feature, it is often challenging to sufficiently define a cyber attack, but Merriam-Webster defines it as ‘an attempt to gain illegal access to a computer or computer system for the purpose of causing damage or harm’.69 It is in the nature of the damage or harm inflicted that cyber attacks take on so many forms. Generally, cyber attacks come in two varieties, either cybercrime or cyber warfare.70

Cybercrime includes financial fraud, identify theft, corporate espionage, hacktivism and a myriad of other forms that are notable for their lack of national security implications.71 Frequently, the tools of the trade used in cyber aggression are developed and honed in the cybercrime domain. In cybercrime, the individual or entity initiating an attack may go up against a secure system, but one that is not as well equipped to respond as the United States military or other branches of the government. Russian hackers in the Heartland Payment Systems data breach, although ultimately caught and sentenced to time in a federal prison, gained valuable training in the cyber attack field when they stole 130 million credit card numbers.72 Similarly, ongoing acts of Chinese cyber espionage, known as ‘Titan Rain’, have resulted in extensive data collection from federal government systems (including, but not exclusive to, the United States Department of Defense).73 Cybercrime, not to be discounted in its severity and destructive capacity, can be thought of as a precursor for the more sophisticated and existential threats posed by cyber warfare. The data collected through cybercrime, along with the tools and tactics that are honed, in effect sharpen the sword that can be used in cyber war.

Cyber war, much as the name suggests, is the execution of war strategies through cyber attacks.74 Unlike cybercrime, cyber war is often the result of state action as opposed to non-state actors, and it often carries higher stakes than cybercrime. A caveat to this point, however, is that state actors may rely on non-state actors to administer cyber attacks as a means of making attribution more difficult.75 In its most direct form, cyber warfare involves attacks on military assets. However, the National Intelligence Council Report Global Trends 2025 made a distressing comment that suggests cyber attacks could extend beyond the battlefield of traditional military targets: ‘Cyber and sabotage attacks on critical US economic, energy, and transportation infrastructure might be viewed by some adversaries as a way to circumvent [United States] strengths on the battlefield and attack directly [United States] interests at home’.76

For purposes of this article, it is the National Intelligence Council's reference to critical infrastructure that is most relevant. Properly functioning transportation systems, energy production, Internet services and financial markets are essential to modern life, but among the various forms of critical infrastructure none is perhaps more essential than electricity production and distribution. Without a functioning grid, the aforementioned elements of society are all diminished. This fact makes grid security a leading concern in any discussion of cyber attack risk. In other words, we have entered a phase in modern life where war strategy may, and likely will, include tactics designed to disrupt or disable an essential element of our civilisation – our ability to produce and distribute electricity to our population. At the risk of hyperbole, this feature of 21st century war-making turns a cyber threat into a potential existential threat.

3. The current situation

3.1. Global order vs global mayhem

It is fair to question whether our electric grid is truly at risk of a major attack and subsequent disruption. After all, it is a premise that supports billions of dollars of private security expenses, animates fear among the public and could prompt elected officials to over-react and over-regulate, and it may be used by military institutions to justify expanded powers into everyday life. Therefore, we must ask ourselves if catastrophic grid failure as a result of a cyber attack is really the risk that it might appear to be in modern life. Put differently, are we in a pre-September-11 moment or are we simply dabbling in apocalyptic paranoia?

The topic of nation state hacking often leads to Russia because few countries have demonstrated both the will and the acumen needed to execute large-scale cyber attacks.77 To answer the question of whether electric grid hacking is a figment of science fiction or a tangible threat, we start with Ukraine.

The first wave of Ukrainian grid attacks occurred on 23 December 2015, when a third party successfully gained entry into and control over electricity distribution substations (the systems of a distribution network essential to transmit electric power to end consumers).78 The outages lasted several hours, shut off power for approximately 225,000 individuals, and occurred through discrete attacks about every half hour.79 Switching to manual override systems eventually restored power, which is an essential component of attack mitigation. To add insult to injury, the responsible party also jammed call centres to prevent affected customers from reporting power outages.80

Robert Lee, a former cyber warfare operations officer for the United States Air Force and co-founder of Dragos Security, said the Ukraine attack was ‘brilliant’.81 He went on to highlight that the attack was sophisticated in terms of logistics, operations and the malware tools used.82 Lee also suggests that the attack was likely coordinated among various actors, including but not exclusive to cybercriminals and nation states.83 Lee is reluctant to attribute the hack to any one actor, including Russia; however, that has not stopped Ukraine from blaming their former Soviet master.84 This highlights a recurring problem with cyber attacks: namely, that it is often difficult, if not impossible, to attribute blame to the responsible party.85

It may be that the 2015 Ukrainian grid attack was simply a harbinger of things to come, because the Ukrainian grid was struck again almost a year later, in 2016.86 The 2016 attack impacted fewer electric customers, but demonstrated improved sophistication compared with the 2015 shut down.87 Marina Krotofil, a Ukrainian researcher for Honeywell Industrial Cyber Security Lab, surmised that the 2016 hack was more of a ‘demonstration of capabilities’ than an attack meant to cripple Ukraine's grid.88

In the end, Ukraine emerged from these attacks mostly unscathed, but the events marked a far more troubling revelation: that Ukraine is merely a testing ground for cyber warfare tools and tactics.89 Since 2016, Ukraine has become ground zero for cyber war shows of force:

‘Ukraine is [a] live-fire space’, says Kenneth Geers, a veteran cybersecurity expert and senior fellow at the Atlantic Council who advises NATO's Tallinn cyber center and spent time on the ground in Ukraine to study the country's cyber conflict. Much like global powers [that] fought proxy wars in the Middle East or Africa during the Cold War, Ukraine has become a battleground in a cyberwar arms race for global influence.90

While it may at first seem desirable to other nations for Ukraine to bear the burden of being a proverbial testing ground, what happens in Ukraine is not staying in Ukraine. Rather, Ukraine is simply a sharpening stone for the swords that are likely to be used against stronger adversaries like the United States and its NATO allies.

Contemporaneous with the Ukraine attacks, US grid systems were suffering similar intrusions. Unlike the Ukraine hacks, the US grid intrusion did not result in a lights-out scenario; however, Jonathan Homer, chief of industrial-control-system analysis for the Department of Homeland Security, said that attacks ‘got to the point where they could have thrown switches’.91 To this day, the grid is still under frequent attack.92 Many grid security experts suspect Russia is involved in the bulk of the grid intrusion efforts, but also express concern that Iran and North Korea are probing weaknesses in grid defence.93 Attempts to infiltrate and possibly disrupt power distribution has extended to attacks on nuclear power plants.94 The plant in question – the Wolf Creek Generating Station in Burlington, Kansas – suffered intrusions into its business network, which suggests that hackers were probing for possible ways to access industrial control systems within the plant.95 Fortunately, the intrusion did not result in an operational impact. However, the incident proves that efforts are underway to exploit even the most sensitive and dangerous components of the grid.

The testing of cyber weaponry abroad and the discoveries of foreign reconnaissance at home all raise the same alarming question: if these are the means, what is the end? In part, foreign actors likely see cyber warfare as a way of asymmetrically confronting the vast power of the United States military (and its NATO allies).96 It remains merely speculative at this time whether a large-scale grid disruption is the goal of foreign actors engaged in these activities. Nonetheless, it is evident that the will is present and the methods are growing more sophisticated; thus, it is reasonable to conclude that under certain geopolitical circumstances a massive grid attack in the United States could occur as a consequence of advancing larger asymmetrical military and/or political objectives. This possibility, combined with the increasing volume of threats in the cyber realm, suggests that world affairs are trending more towards conflict and less towards peace, and it further suggests that such conflict may manifest itself in ways that extend beyond the confines of traditional battlefields.

3.2. What the United States is doing now – offence and defence

There is no question that grid security is a top issue for policymakers, and, relatedly, there is no shortage of efforts underway or aspired to for purposes of fortifying the grid. At a federal level, the Federal Energy Regulatory Commission (FERC) has been stepping up its reporting mandates. New standards published by FERC last summer require the NERC to report cybersecurity attacks that ‘compromise or attempt to compromise electronic security perimeters, electronic access control or monitoring systems, and physical security perimeters’.97 While this is certainly a positive development favouring a stronger grid, there is wide discretion granted by FERC to NERC on what sorts of attacks constitute an incident98 that would then trigger disclosure.

In addition to disclosure requirements, the government recently announced the Pathfinder programme, which is a collaborative effort among the Departments of Energy, Homeland Security and Defense.99 The purpose of Pathfinder is to ‘advance information sharing, improve training and education to understand systemic risks, and develop joint operational preparedness and response activities … ’.100 In addition to Pathfinder, there are more than 27 other programmes within the federal government tasked with protecting the electric grid from some form of failure.101

At a legislative level, the United States Congress has been busy as well. Most notably, the Securing Energy Infrastructure Act (SEIA), which passed last summer, establishes a pilot programme designed to decrease grid digitisation and bolster manual backup systems.102 The idea behind SEIA is that if grid systems have a reliable manual backup available to operators in the event that a cyber attack disrupts digital systems, then the duration of potential blackout will be less severe.103 Inspiration for this approach is varied, but it is supported in part because the Ukrainian grid attack of 2015 was mitigated somewhat by the use of backup manual controls.104

At a regulatory level, states are also taking an active role in grid security. This is particularly important because much of the power distribution system in the country falls outside of federal jurisdiction (the federal government focuses mainly on the bulk power system).105 Therefore, states are establishing cybersecurity taskforce groups, promulgating rules and standards, and establishing state-specific disclosure requirements. In 2019, 16 states considered enacting measures aimed at promoting grid resilience; California and Texas are leading the pack in implementing cyber defence policies.106 Should this trend continue, then it will help ameliorate a major concern in grid protection, which is the need to standardise and monitor small utility platforms that may not receive the attention they deserve at the federal level.

Lastly, the United States has made clear that cyber offence is an essential complement to cyber defence. The United States government has made clear through word and deed that it is prepared to wage cyber attacks in an offensive capacity as may be necessary. In September 2019, Secretary of Defense Mark Esper, while addressing the annual Cyber Security Summit in Washington, DC, stated, ‘We need to do more than play goal line defense. As such, the department's 2018 Cyber Strategy articulates a proactive and assertive approach to defend forward our own virtual boundaries’.107 Secretary Esper elaborated that to ‘defend forward’ means to ‘disrupt threats at the initial source before they reach our networks and systems’.108 The government has articulated this point in greater detail in both the White House Cyber Policy and the Department of Defense Cyber Strategy.109 In the former, the Trump administration details that consequences will be imposed on any actors that threaten or attack the United States through cyber means. Moreover, the White House asserts that it will establish a cyber deterrence initiative with partnering nations. The international coalition envisioned by the deterrence initiative mirrors prior collective defence arrangements that have been used in more traditional military contexts.110

Beyond rhetoric and policy pronouncements, there is strong evidence to suggest that the United States government has already used cyber weaponry to disrupt industrial control systems in other countries. The most well-documented instance of such an effort is the Stuxnet computer virus.111 This virus, which emerged worldwide in 2010, was a cyber weapon designed to infect the industrial control systems of the Iranian nuclear programme, such that nuclear centrifuges used to produced weapons-grade fissile material would spin out of control to the point of self destruction.112 To that end, Stuxnet was successful. It is estimated that approximately 1000 centrifuges were destroyed at the Natanz nuclear facility, or approximately ten per cent of the centrifuges at that location. Although Stuxnet achieved a significant policy objective of the United States, namely to set back the Iranian nuclear programme, there has never been an official acknowledgement that the United States had anything to do with Stuxnet. However, it is believed that the United States and Israel jointly engineered Stuxnet to strike at the core of Iran's nuclear ambitions. Regardless of whether Stuxnet can be firmly attributed to an American-led effort, the virus illustrates that computer code can cause tangible damage to industrial control systems. Moreover, if the United States did originate Stuxnet, then it demonstrates the United States is both capable of inflicting and willing to inflict a kinetic blow against its enemies through the use of cyber weaponry.

4. Anatomy of an attack

4.1. A grid attack, step by step

Building on the information discussed in the prior sections of this article, this section will explore what a grid attack could look like at the micro level. Understanding the nature of the threat on a global scale is essential for appreciating the nature and extent of the risk posed to grid security, but ultimately this challenge will be met on a detailed operational level. Therefore, it is key for individuals or entities that may have responsibility for thwarting a grid attack to comprehend on a granular level how such an attack could occur.

It is the aim of the author to equip the reader of this article with a general knowledge of how a grid attack may unfold so that the reader may become aware of instances in which their role or responsibilities might entail opportunities to mitigate the risk of grid disruption. For example, a reader of this article advising a power distribution company should know that marketing materials for the company should never include photographs of equipment (specifically, industrial control systems) used at the power generation facility. Cyber aggressors, in reconnaissance missions, may use imagery that unintentionally reveals critical systems. Furthermore, this section borrows heavily from the critical infrastructure report titled When the Lights Went Out, published by Booz Allen Hamilton.113

Lastly, it is important to bear in mind that this overview is hypothetical and simply one of many possible strategies to effectuate a cyber attack. An actual attack may mirror many of the steps discussed here, could vary slightly or significantly, and/or could utilise methods that are presently unknown to the author or to the cybersecurity community. Therefore, the reader should appreciate that the following is but one script among many that a utility cyber attack could follow. Accordingly, it is imperative to stay abreast of changes in cyber offensive capabilities as well as to understand that the greatest threats likely come from attack strategies that are novel and not yet clearly envisioned.

(1) Reconnaissance and intelligence gathering:114 In advance of an attack, the cyber aggressor will research the target through any manner of publicly available information and/or through surreptitious non-digital means. The example alluded to above of a marketing brochure containing a photo of an industrial control system is the type of publicly available information that may be instrumental in planning an attack. If an attacker can determine the type of operational platform in use, then that attacker can begin a plan to exploit that device. This step may also include traditional spycraft methods, such as gaining access to a target facility by seeking employment at that facility or attempting to leverage someone presently employed at that facility, perhaps through blackmail. Although a cyber attack against a grid facility is a sophisticated, technical operation, it often begins with non-technical fact gathering activities. Facilities should, therefore, develop thorough employee monitoring procedures, prohibit visual or photographic access to critical systems, eliminate public tours of critical facilities, install port-scanning detection sensors, deny employees use of personal email or similar applications while using facility networks, etc.

(2) Malware development and weaponisation: Once an aggressor gains insight into the systems used by a target facility, the aggressor will commence procurement or development of the malware necessary to effectuate an attack. Depending on the target, an attacker may need to develop a novel cyber tool to gain access. In other instances, if an attacker can utilise existing malware then they will often take that course rather than write an entirely new programme. This is known as ‘living off the land’.115 An infamous example of this occurred in 2017 when National Security Agency hacking tools were leaked in the EternalBlue exploit.116 The malware gained from EternalBlue has been used repeatedly to ransom data held by governments and corporations.117 While development and weaponisation occur external to a target, it is critical that a target facility take steps to understand the types of malware that are available and test those exploits against their own systems in an effort to strengthen and inoculate critical operations against known malware threats.

(3) Deliver remote access trojan: Once an attacker has determined the vulnerabilities of a facility and developed or procured the malware necessary to exploit those vulnerabilities, the next step is to begin the intrusion. The first step of intrusion is the delivery of a remote access trojan (‘RAT’) or some similar software to the business network. The business network is distinct from the network that controls industrial operation systems because the business network is where routine corporate activity occurs, such as financial activity, legal work, human resources, customer service and so forth. The industrial network, on the other hand, is how the facility operates electricity generation and distribution. Gaining access to a corporate network is a necessary step towards gaining access to an industrial control network, which is the ultimate target in successfully disrupting the grid. The RAT or similar software grants the attacker access to the corporate network, which then opens doors to a wider reconnaissance of the facility. RATs achieve this end often by tricking corporate personnel into granting the attack deeper network access; the trick can come in the form of a phishing email that prompts a corporate employee to give their network credentials or to download a seemingly innocuous file to their computer. In the end, this step affords the attacker deeper intrusion into a facility and puts the attacker one step closer to disrupting operations. Methods of combating delivery of a RAT range from having effective malware detection software to a prohibition on using USB drives or accepting files from untrustworthy sources.

(4) Install RAT: Secondary to the delivery of the RAT, the RAT must be installed. This typically occurs when an employee of the business unwittingly installs the RAT to the corporate network. This is often through a ‘social engineering’ method of attack because it exploits human weakness to achieve an objective. An example of this would be sending what appears to be an email from an employee's friend, spouse, etc, that encourages the employee to download a file, such as a party invitation, whereas it is actually an email from the attacker with malware cloaked in a benign attachment. Another example of this would be an attack where the attacker ostensibly applies for a job by sending an application to human resources, but has embedded malware within the attached resume. To combat RAT installation, much like the methods discussed in the previous section, requires both employee education and file monitoring on the corporate network.

(5) Establish command-and-control connection: Once malware is successfully installed within a corporate network, the attacker utilises that malware to establish a command and control connection (CCC) back to an external server of the aggressor. It is at this point that the attacking party gains actionable and unauthorised access to a grid facility's corporate network. Having gained this access, the attacker can now monitor traffic on the corporate network, research files held on the network, harvest network user credentials such as passwords and critical facility codes, upload additional malware and so on. For facility defence at this level, a robust network firewall is essential because by monitoring all communication done with an external server a facility has a strong chance of detecting the attacker's activities.

(6) Deliver malware plugins: Building upon recently installed malware, the attacker will now deliver malware plugins. The purpose of additional plugins is to expand the range of network reconnaissance. An example of a malware plugin would be a keystroke logger, which functions as a recording device on an employee's computer that records each keyboard input and then transmits that keystroke record back to the attacker. Much like the antidote for other forms of malware, the target can defend against this manner of intrusion with sophisticated and updated malware detection software.

(7) Harvest credentials: Similar to the delivery of malware plugins, the attacker will pursue a strategy of credential harvesting, or, in lay terms, username and password theft. This is a critical step, because by obtaining the login credentials of individuals with broad network authority access the attacker can expand their reach throughout the corporate network and, most importantly, into the industrial control system network. This is a significant step towards both the disruption of the grid and the attack's ability to navigate network traffic largely undetected. In effect, the attacker subsumes the grid control authority and access of an individual or individuals with the ability to alter conditions of the industrial control network.

(8) Lateral movement and target identification on the corporate network: This stage marks when an attacker effectively maps an entire corporate network, or at least its essential components. This step may require months of execution, but by the end of this phase the attacking party should have full understanding of and access to relevant servers, employee work stations, telecommunication infrastructure, power supply and so on. Aside from monitoring for suspicious activity, network defence should make efforts to compartmentalise network functions as a means of thwarting comprehensive network movement. Another strategy to detect intrusion at this level is to establish what are known as honeypots, or network decoys, which are network files that serve no useful purpose and would not be accessed by any employees in the normal course of their work. If a series of these decoy files were accessed, this would suggest some form of nefarious reconnaissance is underway.

(9) Lateral movement and target identification on Industrial Control System (ICS) network: This is the stage of the attack in which the attacking party jumps from the corporate network to the industrial control network, ie the systems that provide operational control of the facility's power generation and distribution network. An industrial control system functions like a traditional, manual system except that at key points of its operation it receives digital commands from either automated operating instructions or human input. For example, a hydroelectric power plant may continue producing power through the physics of water-pressure-driven turbines until a human actor, interacting with the facility through a digital control system like a computer or more basic workstation, gives an instruction to the plant control system to either cease power production or ramp it up, or to do something else. These command systems can take many forms, but a basic form is a human–machine interface workstation, which would likely be a laptop type device that is directly connected to an industrial control system, like a programme that has the authority to adjust the speed of a hydroelectric turbine. Within the physical world of the facility, a properly credentialed employee would be able to walk up to this human–machine interface workstation and send a command to the control system for the turbine to alter its operation. In the case of an outside attack on the grid, the attacker would gain access to this workstation remotely and use it to give a command as if the attacker were physically present at the facility. At this stage, an attacker would not yet know how to initiate an attack, but this would be the time when the attacker explores the industrial control system network in an attempt to uncover its vulnerabilities and to identify targets necessary to disrupt the facility's operation. To prevent this stage from occurring, the facility should configure a third, intermediate network between the corporate network and the industrial control system network, wherein the intermediate network acts as holding centre for cross-network traffic to be evaluated. This is akin to a decontamination room that is used when a virologist exits a secure room where they have been studying a dangerous pathogen; the virologist is not permitted to exit a possibly contaminated room without first going through a decontamination room and then, upon approval, being released from that room back into a normal, presumably virus-free environment. While this is not a foolproof method of defending an industrial control system network, it does ensure that an attacker's efforts are more closely scrutinised. Of note, this measure is not the same as an air-gap system, ie a system that separates the industrial control system network from the corporate network. It has been demonstrated that an air-gap system is not practical nor is it as secure as it may seem in theory.118

(10) Develop malicious firmware: Once an attacker has explored the industrial control system network, uncovered its vulnerabilities, and established control system targets, the attacker will develop a weapon appropriate for disrupting those targets. The weapon will be some form of malicious firmware. The attacker does not require access to either the corporate or the industrial control system network during the malicious firmware development stage; rather, the actor will perform this process completely externally to the target facility. However, the attacker may test the malicious firmware on other, similar targets as a means of fine-tuning the efficacy of the weapon. This brings us back to the issue of Ukraine. Ukraine has been and is the testing ground for a host of cyber weapons, and it is generally accepted that malware developed to strike grid-critical facilities are often tested in Ukraine before being executed against their actual target.

(11) Deliver data destruction malware: Preceding an attack, the aggressor will utilise its access to the facility networks (both corporate and industrial control systems) to upload data-destruction malware. The purpose of this malware is to preschedule the deletion of pertinent data that would be relevant to restoring a system's operational integrity. Although the deletion itself is not formally the attack, it complements the attack by frustrating the assessment of what is occurring during an attack as well as hobbling a defensive response to an attack. The only means of confronting this stage of the attack is to maintain robust scanning measures for malware.

(12) Schedule uninterruptable power supply disruption: Grid facilities rely a continuous operation of critical systems during normal operation. During an attack it is even more important to maintain power as a means of ameliorating the disruption. However, using harvested credentials, an attacker will preschedule the termination of otherwise uninterruptable power supply (UPS) sources so that it becomes easier to execute multiple attacks, to do so undetected and to debilitate restoration efforts. A method of combating this tactic is to isolate UPS systems from the corporate and/or industrial control system networks.

(13) Trip breakers: After months or even years of preparation, the attack finally commences. Using access to the industrial control system network and credentials that enable the manipulation of human–machine interface systems, the attacker will issue a command to open the breakers within the facility's power generation and distribution system. The end result will be the disruption of power to a wide range of consumers, measurable in the hundreds of thousands or millions. As discussed above, it is essential to tightly control user access to the industrial control system network, both internally and externally. At this stage, the attack will become known to the facility and corrective measures will likely ensue. For this reason, the attacker will then commence additional attacks to derail any attempted defensive procedures.

(14) Sever connection to field devices: Knowing that a facility control centre will take immediate steps to close the breakers and restore power to the grid, the attack will trigger malware that disrupts power converters and cuts communication between the facility control centre and its substations. The result is that breakers cannot be closed remotely over the network and can only be closed manually. While this may sound like an easy solution, the larger the attack, the longer manual restoration will require. A robust system for monitoring industrial control system network traffic and simulated attack and restoration exercises are necessary to avoid this scenario.

(15) Telephony denial-of-service attack: At a corporate network level, measures will immediately commence to register consumer complaints and formulate a company action plan. As with most power outages, consumers will begin calling the corporate call centre to report a disruption, only now the attacker will flood the call centre with a telephony denial-of-service attack so that the call centre effectively drowns in fake calls and is rendered incapable of addressing legitimate consumer complaints. In order to avoid this frustration, a power company should partner with its phone service provider to develop a means of filtering legitimate from fraudulent calls.

(16) Disable critical systems via UPS: At this stage, step 12 becomes relevant as the attacker's prescheduled power outages begin to wreak havoc on the response effort. Commonly, facility operators will take steps to rely on backup power systems, but here they will find them suspended and useless. This will add more chaos to an already chaotic situation.

(17) Destroy critical system data: Finally, with the power disrupted, control stations neutered and the power company thrown into a technical maelstrom, the attacker will cut the jugular of the facility. With vast access to the corporate and industrial control system networks, the attack will trigger malware that systematically deletes data critical to the operations of the facility. This step of the attack has the potential to make internal restoration of power impossible. Moreover, with the physical components of the facility effectively turned off and the digital systems wiped of all critical data, the likelihood of power restoration in the foreseeable future becomes questionable at best.

(18) Physical destruction of plant systems: Although the 17 prior steps are adequate to turn the lights out, another element of a successful attack warrants attention. Had the attacker initiated a command that caused a power surge sufficient to burn up necessary critical infrastructure, then not even manual restoration would remedy the disruption.119 Under this scenario, power could only be restored by installing new equipment, which, depending on the severity of the attack, could be a protracted solution that requires years of work.

4.2. Post-mortem or restoration

If a large-scale cyber attack does come to fruition, what might be some of the second-order effects? One example comes from a situation that occurred in Wyoming in February 2017, when a strong windstorm knocked down a large number of power lines.120 Because of the inoperable power lines, along with heavy snow, power was not restored for approximately a week. Generators initially powered sewage treatment facilities, but eventually the generators began to fail and as a result sewage began backing up. To avoid wastewater flooding into homes, the area's water supply was cut off. One needs only a modest imagination to consider the impact that a similar situation might have in New York City, Los Angeles, London or any other major metropolitan area. And, to make matters worse, curtailment of clean water could be only one of many challenges resulting from lost power.121 This grave concern prompted Lawrence Susskind at Massachusetts Institute of Technology (MIT)'s urban systems department to remark, ‘Millions … could be left with no electricity, no water, no public transportation, and no waste disposal for weeks (or even months) … . No one can protect critical urban infrastructure on their own’.122

Combined with the social and economic turmoil that could be caused by a crippling grid attack, there could be further difficulties caused by the disruption to supply chains that would be necessary to restore power. At an MIT facility doing work on wind turbine power generation, a mechanical failure to the turbine took almost three months to fix because a necessary part had to be developed and delivered from Germany.123 Expand a situation of this type across an entire grid system, and it could take years to return all systems to normal working order. This sort of dismal situation is known as a black start, and it could prove extremely difficult to overcome. Moreover, one need to only look at the present challenges created by the COVID-19 viral pandemic to appreciate how delicate these critical infrastructure systems are when placed under unexpected and severe stress. An attack on the grid resulting in prolonged power loss would in many ways mirror, and in some ways far exceed, the disruptions presently occurring as a result of the virus pandemic.

#### Current doctrine relies on threshold ambiguity for cyber Article 5 to deter attacks in cyberspace. This approach fails and backfires:

#### 1) CREDIBILITY---Russia’s focused on low-level, deniable attacks, for which Article 5 isn’t credible---but ambiguity ensures every attack triggers debilitating debates that crack the alliance on other issues.

Erica D. Lonergan & Sara B. Moller 22, Lonergan is an assistant professor in the Army Cyber Institute and a research scholar at the Saltzman Institute of War and Peace Studies at Columbia University; Moller is a former Eisenhower Fellow at the NATO Defense College and will be joining the Center for Security Studies at Georgetown University later this year, “NATO’s Credibility Is on the Line with its Cyber Defense Pledge. That’s a Bad Idea.,” Politico, 4/27/22, https://www.politico.com/news/magazine/2022/04/27/nato-credibility-cyber-defense-pledge-russia-ukraine-00027829

President Joe Biden has issued grave warnings that Russia might launch a cyberattack against the United States in retaliation for the punishing sanctions levied after Moscow’s invasion of Ukraine. He’s advised American companies to “accelerate efforts to lock their digital doors,” and many officials expect an attack against critical U.S. infrastructure to be inevitable.

One way Biden and other Western leaders are attempting to deter potential Russian cyber retaliation during the Ukraine crisis is through NATO’s Article 5 collective defense pledge — that an attack on one is an attack against all. That’s because since the 2014 NATO summit in Wales (which, coincidentally, took place following another Russia-Ukraine crisis), the alliance has affirmed that Article 5 extends to cyberspace. In other words, a cyberattack against any NATO member could conceivably represent an attack against the entire alliance. The pledge is the embodiment of the allies’ security guarantee to each other and the beating heart of NATO.

After Russia invaded Ukraine, NATO Secretary General Jens Stoltenberg confirmed that NATO policy on collective defense and cyberspace holds strong, noting that NATO has “decided to make clear that a cyberattack can trigger Article 5.” And following an extraordinary meeting of heads of state and government on March 24, the alliance reinforced that it is “ready to impose costs on those who harm us in cyberspace.”

But despite this rhetoric, exactly how and when Article 5 applies to cyberspace remains unclear. This ambiguity is a problem — with potentially disastrous consequences. Staking the credibility of Article 5 to what are often murky activities in cyberspace threatens to undermine the broader principle of collective defense. We can’t risk fracturing the transatlantic alliance at a critical juncture in its history over a debate on what constitutes a major or minor cyberattack. For that reason, NATO should move quickly to clarify its policy on cyberattacks and explicitly state the threshold for what would trigger an Article 5 response. Furthermore, NATO members should commit to treating cyberattacks that do not rise to the level of a major attack as a national matter — not one for the alliance.

Such a shift might face some initial resistance, particularly in light of the Kremlin’s history of malicious cyber activities. One of the first state-initiated cyberattacks was perpetrated by Russia against Estonia, a NATO member, in 2007. In the intervening years, Moscow has increased its malicious cyber activities, such as the SolarWinds breach uncovered in December 2020 in which Russia gained access to a treasure trove of U.S. data. Russian President Vladimir Putin’s maneuvers against NATO members, along with the annexation of Crimea in 2014, spurred the alliance to adopt a Cyber Defense Pledge in 2016 that recognized cyberspace as a military domain. Two years later, NATO created a Cyberspace Operations Center in Mons, Belgium to improve situational awareness and coordinate cyber operations. Since then, the alliance has consistently reaffirmed the application of Article 5 to cyberspace. At the 2021 summit in Brussels, NATO committed to a new Comprehensive Cyber Defense Policy, with allies agreeing to employ the “full range of capabilities” at all times to “deter, defend against, and counter the full spectrum of cyber threats.”

Notably, NATO refined its language with last summer’s summit communique to account for the fact that some cyber incidents may not be individually decisive, but nevertheless significant when viewed in the aggregate. Specifically, the allies recognized “the impact of significant malicious cumulative cyber activities might, in certain circumstances, be considered as amounting to an armed attack.” In practice, however, NATO leaders have avoided clarifying the conditions under which a cyberattack would trigger Article 5 and how NATO would respond. When pressed about Russian cyberattacks in the Ukraine context, Stoltenberg cautioned that, “we have never gone into the position where we give a potential adversary the privilege of defining exactly when we trigger Article 5.”

This equivocation is not surprising, for several reasons. The nature of cyberspace often confounds unequivocal deterrence declarations. States tend to operate in cyberspace with plausible deniability, which can make it difficult to rapidly ascertain responsibility for cyber incidents. Also, it can be challenging to understand the intent behind observed cyber behavior, and there is often a substantial time lag between when an initial penetration of a network occurs and when the target even realizes the breach. And the vast majority of cyber operations cause virtual, not physical, damage, complicating efforts to assess and evaluate the implications of the costs inflicted. Moreover, it can take time to develop and identify a way to infiltrate a network as well as the computer code that takes advantage of a vulnerability for malicious ends. This means states may lack a palatable cyber response option for retaliatory purposes at the desired time.

This creates a slew of practical problems if Article 5 were to be invoked for a cyberattack. From an implementation perspective, it would trigger deliberations within the North Atlantic Council, NATO’s primary decision-making body. Decisions made within the NAC require unanimity, which can be difficult to achieve for many issues but is especially burdensome for cyber ones, given all of the ambiguities outlined above. The most likely outcome of this process would be a long, drawn-out deliberation resulting in a divided alliance unable to agree on how or whether to respond. Quite simply, some allies are unlikely to want to risk World War III for a cyberattack that disrupts the financial infrastructure, for instance, of another country but doesn’t lead to loss of life or sustained damage.

These challenges have major strategic implications for NATO. After years of publicly and repeatedly linking Article 5 to cyberspace and reinforcing that policy in response to the Ukraine conflict, a failure to achieve consensus and respond to a Russian cyberattack against a NATO member could imperil Article 5 in other areas. The disunity that is likely to be revealed during NAC deliberations would then undermine the broader political cohesion that has, for the most part, been remarkably strong throughout the war in Ukraine. This would make it more difficult for the alliance to respond to other forms of Russian behavior. As Biden emphasized at a press conference last month, “the single-most important thing is for us to stay unified … We have to stay fully, totally, thoroughly unified.”

#### That triggers broader deterrence failures---it’s existential

Łukasz Kulesa 18, Research Director at the European Leadership Network, “Envisioning a Russia-NATO Conflict: Implications for Deterrence Stability,” EURO-ATLANTIC SECURITY REPORT, February 2018, https://www.jstor.org/stable/pdf/resrep17437.pdf

“Hybrid” scenarios: trigger for conflict?

One can envisage a number of “hybrid” scenarios of Russia-NATO conflict where operations which started in the cyber, economic, criminal, or “active measure” domains, below the threshold of conflict, trigger a military response or are followed by the physical use of force. As noted in the discussion on the definitions of a conflict, the threshold between crisis and military conflict may not be explicitly stated or otherwise clear to all sides; and it may also be ignored during a crisis. This aspect is especially relevant in the current period of increased interference in the internal affairs of NATO countries attributed to Russia and of the high volume of information ‘warfare’ between Russia and NATO countries.

Russia remains vigilant about foreign interference in its internal affairs and the threat of subversion leading to a severe destabilization of the regime. In the past, Moscow has made accusations about foreign sponsorship of Chechen and radical Islamic terrorists targeting Russia, and has alleged the existence of training camps on the territories of NATO states for activists planning colour revolutions in Ukraine and Belarus. In the extreme circumstances of a crisis, if the Russian leadership became convinced that a non-military campaign against it (which might also involve cyber activities and what Russia calls attempts to instigate colour revolutions) had intensified, this could lead to a military response.

With regards to NATO, some of its members’ views mirror the Russian assessment that we are already in a state of conflict, in which the boundary between peace and war is blurred, and that their defences are being actively attacked through nonmilitary means. They are thus concerned about a scenario in which Russia initiates an attack that moves swiftly from non-military to military means. This scenario should be not dismissed. At the same time, one needs to be wary of interpreting all disturbing developments as part of a grand Russian plan culminating in a provocation or use of force. So there should be prudence before any country presses the “panic button” at the national or NATO / European Union level. There should also be close analysis of early warning indicators related to the gravity, intensity and diversity of incidents and to connections between them. The overall political context and state of the RussiaNATO relationship would also be important: what would be the political and strategic reasons for Russia to move from sub-threshold to abovethreshold activities?

Escalation: Can a NATO - Russia conflict be managed?

Once a conflict was under way, the “fog of war” and rising unpredictability would inevitably set in, complicating the implementation of any predetermined theories of escalation, deescalation and inter-conflict management. The actual dynamics of a conflict and the perceptions of the stakes involved are extremely difficult to predict. Simulations and table-top exercises can give only limited insights into the actual decisionmaking processes and interactions.

Still, Russian military theorists and practitioners seem to assume that a conflict with NATO can be managed and controlled in a way that would bring it to a swift end consistent with Russian aims. The Russian theory of victory would seek to exploit weak points in an Alliance war effort. Based on the conviction that democracies are weak and their leaders and populations are risk-averse, Russia may assume that its threats of horizontal or vertical escalation could be particularly effective. It would also try to bring home the notion that it has much higher stakes in the conflict (regime survival) than a majority of the NATO members involved, and thus will be ready to push the boundaries of the conflict further. It would most likely try to test and exploit potential divisions within the Alliance, combining selective diplomacy and activation of its intelligence assets in some NATO states with a degree of selectivity in terms of targets of particular attacks.

Any NATO-Russia conflict would inevitably have a nuclear dimension. The role of nuclear weapons as a tool for escalation control for Russia has been thoroughly debated by experts, but when and how Russia might use (and not merely showcase or activate) nuclear weapons in a conflict remains an open question. Beyond catch phrases such as “escalate to de-escalate” or “escalate to win” there are a wider range of options for Russian nuclear weapon use. For example, a single nuclear warning shot could be lethal or non-lethal. It could be directed against a purely military target or a military-civilian one. Detonation could be configured for an EMP effect. A “false flag” attack is also conceivable. These options might be used to signal escalation and could significantly complicate NATO’s responses.

Neither NATO nor its member states have developed a similar theory of victory. Public NATO documents stipulate the general goals for the Alliance: defend against any armed attack and, as needed, restore the full sovereignty and territorial integrity of member states. It is less clear how far the Alliance would be willing to escalate the conflict to achieve these goals, and what mechanisms and means it would use while trying to maintain some degree of control over the conflict.

The goals and methods of waging a conflict with Russia would probably have to be limited in order to avoid a massive nuclear exchange. Such limitations would also involve restrictions on striking back against targets on Russian territory. But too narrow an approach could put too much restraint on NATO’s operations: the Russian regime’s stability may ultimately need to be threatened in order to force the leadership into terminating the conflict. NATO would thus need to establish what a proportional self-defence response to Russian actions would involve, and to what extent cyber operations or attacks against military targets in quite different parts of Russia would be useful as tools of escalation to signal NATO’s resolve. Moreover, individual NATO Allies, especially those directly affected by Russia’s actions, might pursue their individual strategies of escalation.

With regards to the nuclear dimension in NATO escalation plans, given the stakes involved, this element would most likely be handled by the three nuclear-weapon members of the Alliance, with the US taking the lead. The existence of three independent centres of nuclear decision-making could be exploited to complicate Russian planning and introduce uncertainty into the Russian strategic calculus, but some degree of “P3” dialogue and coordination would be beneficial. This coordination would not necessarily focus on nuclear targeting, but rather on designing coordinated operations to demonstrate resolve in order to keep the conflict below the nuclear threshold, or bring it back under the threshold after first use.

Relying on concepts of escalation control and on lessons from the Cold War confrontation might be misleading. The circumstances in which a Russia -NATO conflict would play out would be radically different from the 20th century screenplay. Moreover, instead of gradual (linear) escalation or salami tactics escalation, it is possible to imagine surprizing “leap frog” escalation, possibly connected with actions in different domains (e.g. a cyberattack against critical infrastructure). Flexibility, good intelligence and inventiveness in responding to such developments would be crucial.

Conflict termination

Russian and NATO assumptions regarding conflict termination would most likely not survive the first hours of an actual conflict. Both sides are capable of underestimating the resolve of the other side to prevail in a conflict and the other side’s willingness to commit the necessary resources and endure the costs, especially once both sides start committing their political capital and resources and the casualties accumulate.

With regards to Russia, Moscow would most likely be approaching the conflict with a clearer concept of its war aims and thus develop better-formed views on conflict termination. It would seek to establish escalation dominance and confront NATO with a binary choice of either accepting defeat or further intensification of fighting. Such intensification might involve a move to the nuclear level, but Russia would also have conventional escalation options, such as conventional deep strikes.

At the same time, it should be highlighted that Russia is unlikely to start a conflict which involves a high degree of uncertainty about its final outcome and carries a risk of military defeat. Russia cannot safely assume that US-led NATO would act with restraint, nor could it be sure that the Alliance would be ready to surrender and terminate a conflict early. For internal reasons Russia cannot afford to lose a “big war”, so the most prudent option would generally be not to initiate such a conflict in the first place. Such logic could, however, get lost in some of the hybrid scenarios and scenarios of an inadvertent outbreak of a conflict.

#### 2) TRADE-OFF---prioritizing acts of war cannibalizes focus AND resources from broad-based cyber resilience strategies that are more effective.

Jason Blessing 22, Jeane Kirkpatrick Visiting Research Fellow at the American Enterprise Institute, “The Russian Cyber Threat Is Here to Stay and NATO Needs to Understand It,” AEI, 4/25/22, <https://www.aei.org/op-eds/the-russian-cyber-threat-is-here-to-stay-and-nato-needs-to-understand-it/>

Since the Russian invasion of Ukraine, the Biden administration has escalated warnings about likely Russian cyber-attacks on American infrastructure and business. More worrying still, cyber alarmists like Senate Intelligence Committee Chairman Mark Warner, D-Va., have suggested that cyber-attacks from the Kremlin could be acts of war that trigger NATO’s collective defense.

This sky-is-falling delusion, particularly from leaders with access to classified intelligence, is at best counterproductive and at worst dangerous.

Cyber-attacks are rarely acts of war, and treating them as if they are undermines NATO’s ability to deal with real threats short of cyber war.

NATO has only invoked Article 5 – which triggers a collective response – once and that was after the 9/11 attacks.

Cyber-attacks are unlikely to destroy buildings and kill thousands in an instant. While collective defense extends to cyberspace, few operations could realistically be a cause for war.

This would include cyber-attacks resulting in death or damage like traditional military operations or coordinated assaults that take the power grid or entire economic sectors offline. These scenarios are unlikely though: such attacks require far too much time, funding, manpower, and control. Instead, most attacks temporarily overwhelm servers with traffic, deny network access, hold computers hostage, and steal or delete data.

Even if allies wanted to trigger Article 5 over cyber operations, disagreements about the definitions of threats, origins of attacks, and pain thresholds in cyberspace can derail the process.

Collective retaliation requires a unanimous vote across NATO; building unity across these points is nearly impossible for most cyber activity. Unlike missile attacks or tanks in the streets, few “red lines” exist to distinguish cybercrime, cyber espionage, and cyber disruption from digital acts of war.

Beyond the bureaucratic and logistical limitations of elevating cyber to a casus belli, focusing on cyber-attacks as acts of war distracts from the more likely Russian digital assaults below the level of armed conflict. These include ransomware attacks and supply chain infiltrations that look like criminal activity or espionage.

The Kremlin is particularly adept at the latter. In the SolarWinds compromise, Russia hacked one company’s software product to access networks of Fortune 500 companies and U.S. government agencies.

Spillover from operations in Ukraine poses an additional risk. The Russians have already deployed several digital tools to destroy computer data, resulting in corrupted computers for Ukrainian companies with government support roles. The same malicious software has also affected several Latvian and Lithuanian businesses.

The danger is another situation like NotPetya in 2017, where malware self-replicated, spread past Ukrainian targets to cripple networks in over 150 countries, and created $10 billion in damages.

Each of these scenarios are much more likely than a “cyber doomsday” that would justify an Article 5 response from NATO members.

To be fair, policymakers’ fears of cyber war have led to some positive developments for the alliance. For instance, over the last several years, NATO has developed its own framework for combining cyber and conventional military capabilities in warfighting. But allies remain unprepared to deal with “death by 1000 cuts” in cyberspace.

Concentrating only on acts of war comes at the expense of addressing the cumulative costs of low-level cyber threats over time. It leads to an overreliance on cyber deterrence or defensive whack-a-mole strategies, neither of which are sustainable.

Threats of retaliation simply don’t deter most cyber-attacks, and it is unrealistic for defensive measures to stop every hacker.

Policymakers across NATO must acknowledge that security failures are the norm in cyberspace, and that the compounding costs of failure over time are every bit as dangerous as the threat of cyber war.

Building cyber resilience is an important step forward. It acknowledges that, in many cases, the Russians will get the best of us in cyberspace. The focus is on controlling failures to limit damage and quickly get networks back online.

Moving from buzzword to actual strategy requires addressing several questions. Which digital assets are most significant? Where is the alliance most exposed to Russian cyber-attacks? Where should NATO reduce operating risks, and in what areas can it assume more? How can allies track long-term trends and adapt to new technologies?

The Russian cyber threat is here to stay. Collective defense is – and should remain – the cornerstone of NATO. But time is running out for the alliance to protect itself from scenarios that aren’t all-out cyber war.

#### 3) PERCEPTION---ambiguity about NATO’s role in sub-warfare engagements erodes the intelligence norm in cyberspace, which presumes that cyber penetrations are for info gathering rather than achieving offensive effects.

Jeppe T. Jacobsen 21, Ph.D. candidate at the Danish Institute for International Studies and the Center for War Studies at the University of Southern Denmark, worked as cyber coordinator at the Ministry of Foreign Affairs of Denmark where he coordinated Denmark’s cyber diplomacy, “Cyber Offense in NATO: Challenges and Opportunities,” International Affairs, vol. 97, no. 3, 05/01/2021, pp. 703–720

The question then arises: does the lack of capacity to deter non-military hybrid cyber activities suggest that it is time for NATO to renegotiate the scope and substance of its collective defence clause?65 When it comes to cyberspace, the next section expresses scepticism about expanding NATO’s role. It addresses the escalation risk associated with having NATO, an organization that has refocused its attention on a more traditional military threat, become a more active player below the threshold of collective defence. It argues that a more active stance outside military confrontation risks undermining the intelligence norm that currently dominates in cyberspace—a norm whereby state activity in foreign networks is not considered escalatory.

Escalation and the dominant intelligence norm

The large overlap between intelligence collection and attack in cyberspace makes it difficult to send clear signals to adversaries, in terms of either capabilities or intentions. When a foreign entity is moving around in a network, is it then about to start a military operation? Is the activity part of a reconnaissance mission? Is it political or economic espionage? Is it active defence? The difficulty of answering these questions has created much nervousness among cyber-conflict experts. Ben Buchanan, for example, has shown how defensive hacking or intelligence-gathering in cyberspace is easily misinterpreted as aggressive behaviour.66 Why, then, have we not experienced serious misinterpretation and escalation in cyberspace?

One way to explain this is through the existence and dominance of a largely unspoken but widely accepted norm. For decades, the predominant actors in cyberspace have been intelligence agencies; and the norms that characterize interactions between intelligence agencies are not primarily concerned with military concepts such as conflict escalation and deterrence.67 In the world of intelligence agencies, success is not about keeping a distance between oneself and the adversary by signalling one’s intentions and capabilities. It is about being able to outmanoeuvre adversaries in a space of constant contact.68 There are always risks, and the work usually takes place in legal grey zones where a clear distinction between war and peace is not the guiding principle. This is an arena where the opportunity to annoy, cheat and delay opponents is taken when it arises. In short, espionage and counter-espionage do not fit well with the thorough military operational planning that characterizes NATO operations. Intelligence operations, on the other hand, fit perfectly with a dynamic cyberspace where anonymity is easy to achieve and uncertainty a constant condition.69 The states that embrace cyberspace as a domain where the intelligence norm dominates are able to use a broader array of tools to pursue or respond to various foreign political objectives than only those that relate to military operations.

In its 2018 ‘vision’, the US Cyber Command built implicitly on the dominant intelligence norm. Here, the objective is to become more agile and act as close to the adversary as possible (‘defend forward’).70 The United States considers ‘constant contact’ and ‘persistent engagement’ as the necessary guiding principles to achieve superiority in cyberspace and to take full advantage of the broader potential for pursuing its political objectives through cyberspace. During the 2018 US midterm elections, for example, the US Cyber Command worked closely with the NSA to disrupt servers operated by the Russian Internet Research Agency aiming to spread fake news and stir up tension in the United States.71 More recently, the US Cyber Command responded with various cyber effects against Iran after the Iranian Revolutionary Guards apparently placed mines on ships in the Strait of Hormuz.72 These practices illustrate that, for the United States, cyber effects provide political options when one does not want to escalate existing tensions into military confrontation. Defensive coordination between allies through CYOC supports such defensive use of cyber effects, increasing the possibility that US Cyber Command will be allowed to ‘defend forward’ and work persistently through allied networks.73 A more cyber-active NATO, however, risks being counterproductive to the ambition to ‘defend forward’ through allied networks.

Unintended conflict escalation from ongoing cyber activity is mainly a risk if military analysts—in a strategic environment with heightened attention to military confrontation—ignore the dominant intelligence norm. If that happens, it becomes more likely that ‘persistent engagement’ and active cyber defence will be misinterpreted as military preparation, armament or the initial phase of an attack. If NATO, an organization that has publicly returned to its original raison d’être of deterrence and collective defence, becomes the entity that coordinates cyber effects below the threshold of armed conflict, then the likelihood increases that Russia misinterprets these effects as escalatory and acts accordingly. In other words, a more active NATO in the current strategic environment increases the risk that the existing intelligence norm will be undermined and replaced by a more militarized norm.

This does not mean that states that face hostile hybrid activities below the threshold of armed conflict will be left alone. Intelligence cooperation between allied countries does exist, and threat information is occasionally shared. In addition to the current political collaboration facilitated by NATO to improve network security and resilience, the EU is engaging in similar civilian activities, as well as developing and implementing a cyber-diplomatic toolbox to create a common basis for responding to a variety of malicious activities against member states. Further strengthening the political partnership between the EU and NATO is thus the most appropriate way forward to avoid further militarization of cyberspace.

Sustaining the intelligence norm as the dominant norm is not without potential problems. Openly embracing the fact that cyberspace is a domain in which intelligence agencies are constrained only by domestic laws, and where takedowns of servers in foreign countries are not necessarily perceived as serious breaches of sovereignty, is likely to lead to an increase in the exploitation of IT vulnerabilities in commercial software used in both enemy and allied networks. For smaller states, this could increase the risk of retaliation by larger adversaries, and it could increase the risk of divisions between allies—divisions that are not aligned with the United States’ political ambition to use cyber coordination in NATO as part of its attempt to ‘defend forward’.74 More exploitation could also ultimately make cyberspace less free, less open and less secure, rendering civilian populations more susceptible to cybercrime, surveillance and disruptions of everyday services.75 This is why some states, NGOs and private corporations such as Microsoft continue to promote norms that emphasize restraint on the part of states’ intelligence agencies and militaries in cyberspace, and why other states promote more sovereign control of cyberspace.76

Conclusion

This article has pointed to several challenges to the integration of military cyber effects in NATO operations, and has argued that even if the integration is successful, it will not add to the alliance’s deterrence posture. Importantly, the fact that CYOC does not send a strong signal to adversaries such as Russia does not mean that it is a waste of time. Far from it. As both conventional militaries and paramilitary groups are increasingly dependent on civilian networked technologies, the ability of NATO to disrupt, deny, degrade or destroy enemy networks through sovereign cyber effects—even if these amount only to temporary annoyances—will become more relevant in the years to come. This, of course, does not mean that conventional kinetic or electromagnetic capabilities will become redundant. Rather, cyber effects offer a substitute in case the intended target cannot be reached with conventional capabilities, and a supplement that works alongside conventional operations as persistent annoyances of enemy networked devices. The latter, however, demands an agile CYOC that provides member states with broad initial mandates and facilitates quick decision-making and rapid approval when member states stand ready to deliver even minor cyber annoyances.

Furthermore, the article has argued that NATO and its CYOC should not seek to coordinate additional offensive cyber efforts to deter hybrid activities below the threshold of armed conflict. If an organization that is perceived by its main adversary primarily as a military organization engages in active cyber-defence measures and persistent cyber engagements outside of military confrontation, then the risk of escalation increases. This is because every potential NATO-initiated cyber activity in foreign networks is likely to be perceived through a military lens and thus to be (mis-)interpreted as an attack in the making. In fact, active cyber-defence measures in foreign networks and use of cyber means below the threshold of armed conflict to pursue political interests internationally are part of our current reality. Intelligence agencies know this to be a fact, and they live by it every day.

#### The plan solves by reinforcing the cyber-kinetic firebreak---stops cyberattacks from escalating.

Erica D. Lonergan & Sara B. Moller 22, Lonergan is an assistant professor in the Army Cyber Institute and a research scholar at the Saltzman Institute of War and Peace Studies at Columbia University; Moller is a former Eisenhower Fellow at the NATO Defense College and will be joining the Center for Security Studies at Georgetown University later this year, “NATO’s Credibility Is on the Line with its Cyber Defense Pledge. That’s a Bad Idea.,” Politico, 4/27/22, https://www.politico.com/news/magazine/2022/04/27/nato-credibility-cyber-defense-pledge-russia-ukraine-00027829

NATO has achieved some strategic ambiguity with its current cyber policy, which may help to deter high-stakes Russian assaults during the present crisis. However, rather than an all-out Russian cyberattack, a far more plausible scenario is a lower-level attack carried out by the Russian government or a proxy group against one or more allies. In this case, the alliance’s interests — not to mention transatlantic security — would be better served by adopting nationally-tailored responses rather than pulling the Article 5 lever. Additionally, to prevent further escalation and reinforce the implicit firebreak that currently exists between cyber and conventional military operations, NATO allies should also agree to restrict any retaliatory response against Moscow to the cyber realm or non-military instruments of power.

### Cyber Norms ADV

#### Advantage two is CYBER NORMS

#### NATO will overapply article V to any hybrid threat which unravels the international legal order and expands use of force justifications

Aurel Sari 19, Senior Lecturer in Law, University of Exeter; Director, Exeter Centre for International Law; Fellow, Supreme Headquarters Allied Powers Europe; Fellow, Allied Rapid Reaction Corps, “The Mutual Assistance Clauses of the North Atlantic and EU Treaties: The Challenge of Hybrid Threats,” Harvard National Security Journal, Volume 10, <https://harvardnsj.org/wp-content/uploads/sites/13/2019/06/Mutual-Assistance-Clauses-of-the-North-Atlantic-and-EU-Treaties.pdf>

The legal challenges that hybrid threats present for collective security guarantees have been recognized at the highest political level. At their Warsaw summit held in July 2016, NATO’s member states confirmed their readiness to assist each other at any stage of a hybrid campaign and to counter hybrid warfare as part of collective defense.294 They also underscored that the North Atlantic Council “could decide to invoke Article 5 of the Washington Treaty.”295 They repeated these points at their Brussels summit in July 2018.296 By drawing an express link between hybrid warfare and collective defense, NATO leaders signaled their resolve not to allow Article 5 to be hollowed out.297 Still, their declarations of intent strike a rather conservative note. Whilst they accept that NATO may assist an Ally at any stage of a “hybrid campaign,” it is only in cases of “hybrid warfare” that they foresee a potential role for Article 5. This is not an unreasonable position to take. As we saw earlier, recourse to the use of force to counter hybrid threats falling below the threshold of an armed attack is neither permissible nor necessarily appropriate. A pledge to invoke the mutual defense commitment in response to every type of hybrid threat would be a promise to use the proverbial sledgehammer to crack a nut. It would be unrealistic and therefore lack credibility in the eyes of hybrid adversaries.298 By accepting that the role of Article 5 is confined to situations of hybrid warfare, the Warsaw and Brussels Summit Declarations avoid such empty gestures. However, in the same breath they also concede that the application of Article 5 is contingent on the legal threshold between warfare and peace, and thus vulnerable to subversion along the lines discussed in the preceding sections.

It may be tempting to deal with the problem of legal thresholds by attempting to escape them altogether, but this is not a feasible strategy. Even if the contracting parties were to revise Article 5 NAT and Article 42(7) TEU to avoid references to “armed attack” and “armed aggression,”299 they would remain bound by the rules governing the use of force under the UN Charter and customary international law. Although the member states of NATO and the EU make up an influential part of the international community, it is not within their ability to adjust these general rules of international law unilaterally. In any event, lowering the threshold for the use of force in order to facilitate the application of Article 5 and Article 42(7) would come with significant costs, since it would loosen the legal restrictions for all states, including hostile powers. The applicable thresholds therefore cannot be unilaterally modified at will and without the risk of unraveling key elements of the international legal order as it currently stands.

A more promising approach is to strengthen legal interoperability among NATO and EU nations. One line of effort is to reduce legal gray zones,300 for example by narrowing disagreements over the gap that lies between the definition of force and armed attack. This could prepare the ground for developing a shared understanding of what kind of hybrid threats may trigger the applicability of Article 5 NAT and Article 42(7) TEU. Given that the assessment of any security threat depends heavily on its context, it may prove somewhat sterile to build such a consensus in the abstract. Drawing on war-gaming and exercises may offer a more fruitful way forward. Bearing in mind how attractive the use of proxies is to a hybrid state adversary,301 developing a common approach to attribute their activities to the sponsoring state also merits attention. Although many aspects of the rules governing the attribution of wrongful acts are settled, certain questions could benefit from a joint posture.302 NATO and EU nations should also strengthen their collective mechanisms for unmasking attempts at plausible deniability in order to deny its use as a hybrid instrument,303 as illustrated by their united response to the Skripal incident and to Russian cyber operations.304

#### That will be exploited by adversaries to make war more likely in every theater and signals a return to gunboat diplomacy

Patrick C. R. Terry 19, dean of the faculty of law at the University of Public Administration in Kehl, Germany, “The Return of Gunboat Diplomacy: How the West has Undermined the Ban on the Use of Force,” Harvard National Security Journal Volume 10, https://harvardnsj.org/wp-content/uploads/sites/13/2019/02/Return-of-Gunboat-Diplomacy.pdf

This article explores how the “West,” the main creator of modern international law after WWII, is now, nevertheless, steadily undermining it. While purporting to be reemphasizing each state’s right to defend itself and elevating the protection of human rights, the West is, in truth, rendering the far-reaching ban on the use of force envisaged in the U.N. Charter ineffective, thereby paving the ground for a return to 19th century gunboat diplomacy.1 This new age of international law is marked by the use of force no longer being governed by the rule of law, but rather almost exclusively by the raw power of states—a fact western politicians attempt to conceal by issuing dubious, often hypocritical, but wellsounding statements. These states have abandoned the—perhaps utopian—goal of realizing the principle of sovereign equality and are increasingly replacing it with an aggressively hierarchical order of states reminiscent of the colonial era of the 19th century.

Seemingly disparate western forces are eroding the ban on the use of force: right-wing interventionists—predominantly, but not exclusively—to be found in the United States, and so-called liberals spread across the West. Common to both approaches is the argument that international law is steadily and necessarily evolving to adapt to developments in the modern world.

There are supposedly stark differences between right wing and liberal approaches to international law. Right-wing interventionists tend to be quite open about their disdain for international law, sometimes even claiming that law does not and/or has never governed international relations and that outcomes are ultimately the result of the involved states’ relative power.2 Others, such as Michael Glennon, do accept that international law has a role to play in foreign affairs, but argue that its rules should flexibly adjust to the major powers’ relative strength.3 Furthermore, right-wing interventionists tend to focus their arguments on the rules governing the use of force while the liberals’ reforming zeal is generally broader.

The liberal approach tends to emphasize its strict adherence to the rule of law in international affairs. Liberals, however, often argue that international law, especially customary international law, is evolving under the influence of international human rights law. It is no longer the state, but the individual human being that is becoming and should become the focus of international law.4 This has allegedly led to the emergence of a right to intervene abroad on humanitarian grounds. More extreme advocates of the liberal strand of thought have even justified interventions in order to install/reinstate a “democratic” government. At this point, some liberal and right-wing scholars have in fact found limited common ground, as this argument can readily serve to justify the right-wing interventionists’ general “regime change” agenda in “rogue states.”

This article will show both strands of thought to be similarly harmful to the international rule of law. Both necessarily require the acceptance of a hierarchy of states, based on their relative power, and both rely on the United States’ alleged exceptionalism as leader of the Free World and the West’s unparalleled strength following the Eastern Bloc’s collapse in the early 1990s. Since then, the widespread assumption has been that only the United States and its close allies could retain the capabilities to rely on more generous rules permitting the use of force.

As we near the end of the second decade of the 21st century, this blasé attitude towards the rest of the world has turned out to be misplaced. Rather, countries as diverse as Russia, Saudi Arabia, Colombia, and Turkey have increasingly come to rely on ever-expanding exceptions to the ban on the use of force first advocated by the West. Consequently, we are witnessing a return to gunboat diplomacy: states that feel powerful enough to intervene forcefully in another state’s internal affairs will do so and claim justification based on the often ill-defined and ill-advised rules that right-wing interventionists and liberals have tried to impose. The rule of law is thus again being replaced by the Darwinian principle of the “survival of the fittest.” Meanwhile, we are steadily approaching the point Glennon claims we have already passed,5 whereby the jus ad bellum has become indeterminate, meaning that few, if any, constraining rules on the use of force remain.

Recent developments illustrate this: the United States did not even bother to put forward a serious legal argument to justify its attacks on Syrian forces in 2017 and 2018 in retaliation for their alleged use of chemical weapons. The frequent recourse to force irrespective of international law, as practiced by western and, increasingly, other states has led to a widespread increase in spending on defensive and offensive capabilities. States wish to protect both their sovereignty and standing in the new hierarchy of states, and many of them have presumably come to the same conclusion as India already had in 2003, following the United States’ and the U.K.’s unlawful attack on Iraq: disagreement with the United States requires the possession of nuclear weapons.6

The article will focus on the two areas of the law on the use of force where the effect of western thought has contributed to the serious weakening of legal structures. First, I will examine the erosion of the law on self-defense in some detail, before subsequently turning to the attempts to justify the use of force in other cases, notably during humanitarian crises. I will first outline the arguments in support of an expansive view of the right to resort to force before assessing them according to the U.N. Charter, the jurisprudence of the International Court of Justice (hereinafter ICJ) and traditional customary international law. This will be followed by an exposé of state practice and opinio juris. Finally, a brief conclusion will summarize the current state of affairs.

This analysis will demonstrate that successive attempts at “modernizing” international law are in danger of dismantling the safeguards against war and of recreating a world in which a few privileged states can attempt to impose their will on the rest. The logic of an ever-expanding concept of justified military action selfevidently reveals a hierarchal view of the international community: only the wealthy and privileged western states and their close allies should benefit from such generous rules. It was never in the West’s interest that other states, such as Russia, China, or India should invoke an expansive view of the right to use force. However, as recent developments illustrate, the West has miscalculated; its power is no longer sufficient to stop other states from exploiting its dubious precedents.

#### Aggressive China causes miscalculated war

Lyle J. Morris 19, Senior Policy Analyst at RAND, M.A. in international affairs, Columbia University; B.A. in international business administration, Western Washington University, 1/7/19, “Gray Zone Challenges in the East and South China Sea”, http://www.maritimeissues.com/politics/gray-zone-tactics-and-their-challenge-to-maritime-security-in-the-east-and-south-china-sea.html

The United States and Japan have identified the gray zone threat as a major challenge to the international rules-based order. Given the United States’ conventional military superiority and the severe risks associated with regional war, competitors such as Russia and China—who desire to challenge U.S. predominance but remain determined to avoid large-scale conflict if possible—are adopting tactics that undermine U.S. interests but that makes conventional military responses infeasible. By relying largely on non-military capabilities and operating in what has been called a “gray zone,” these competitors confront the United States and its allies with a series of policy and strategy challenges. Thus far, the United States and regional actors have arguably yet to form a coherent policy to address the challenges.

This short policy paper seeks to provide an overview of the challenge posed by gray zone coercion in Asia and propose some principles that should guide the U.S., its allies and partners in countering the threat.

The Gray Zone Challenge in Asia

China’s use of maritime law enforcement and maritime militia to assert administrative control over disputed territory and waters in the East and South China Sea, as well as island-building activities in the South China Sea, have introduced a new doctrine of maritime coercion in Asia. This doctrine puts a premium on non-military assets and subterfuge that puts the onus of military escalation on the recipient of such tactics. China appears to calculate that relying on non-military assets such as coast guard vessels, maritime militia and other civilian maritime actors, while keeping PLA Navy (PLAN) surface ships largely in the background, will enable it to achieve its strategic goals while minimizing the risk of further escalation. Starting in 2014, China also initiated one of the most ambitious island-building campaigns in history – reclaiming over 3,000 acres of land on disputed features in the Paracel and Spratly Island chain – and building civil-military facilities on them. Several of these features now have large airstrips, hangers, radar facilities and military barracks to support military deployments in the naval and air domain. The scale and rapidity with which China achieved these island-building projects was unprecedented and caught the United States, its allies and partners off guard.

By using such tools, platforms and tactics, China has greatly improved its position and administrative control over much of the disputed territory in the East and South China Sea, and done so at minimal material or diplomatic cost. China has also been successful at “civilianizing” the optics of the threat, ensuring that if one of its rivals responds with military assets, such as with its Navy or Air Force, that country will appear to be the party engaging in escalatory behavior, rather than China. Moreover, especially in the case of much weaker rivals like the Philippines, employing naval assets in reaction to provocative Chinese maritime law enforcement or other non-military activities risks creating an opportunity for China to respond in kind, thus escalating the conflict to a level where it enjoys even more overwhelming superiority.

Chinese Gray zone tactics differ in several ways. In East Asia, territorial disputes between China and Japan over the Senkaku Islands have brought about a significant escalation of tensions over the past several years, yet China has not adopted the types of escalatory tactics or maneuvers that might lead to escalation seen in the South China Sea. China’s use of coast guard and maritime militia to change the status of Japan’s administrative control over the Senkakus nonetheless poses new gray zone challenges in the maritime and air domains in Japan’s southwest island chain. Since 2012, China has undertaken near-constant incursions into the Senkaku territorial seas test Japan’s will and resolve to respond. In particular, the recent deployment of armed Chinese coast guard cutters – many of which are decommissioned PLA Navy frigates; and the use of maritime militia fisherman whose vessels are equipped with intelligence gathering capabilities and whose personnel are under the command and control of the Navy – has injected another layer of gray zone challenge for Japan. These moves are calibrated to gauge the timeliness and readiness of the Japanese Coast Guard (JCG) to respond and compel the JCG to maintain continuous presence around the islands. For the most part, however, they follow a predictable pattern of behavior of incursions.

In Southeast Asia, on the other hand, Chinese gray zone tactics inhabit a more materially-threating form and countries in the region have grown increasingly wary of Chinese efforts to deter or in some cases actively deny the use of living and non-living resources in their exclusive economic zone (EEZs) of the South China Sea. To do so, China now actively deploys coast guard and maritime militia to protect the waters and territory within its Nine-Dash Line (NDL) claim, which has been invalidated under international law. In contrast to China’s approach near the Senkakus in the East China Sea, China adopts a much more aggressive posture in the South China Sea, in part due to Beijing’s calculation that is can coerce smaller Southeast Asian countries who in most cases do not counter-deter. The way in which China employs its coast guard, in particular, has upended conventional wisdom on the tactics of how coast guards operate. China’s coast guard is acting as a “blunt defenders of sovereignty” undertaking actions such as ramming other states’ coast guard and fishing vessels, rather than acting as traditional instruments of law enforcement. The use of its coast guard as an instrument to protect claimed territory while conducting peacetime patrols of disputed maritime territory has blurred the line between the platforms and missions associated with “law enforcement” and those associated with “national defense.” In one of the most sweeping rulings on the actions of maritime law enforcement in disputed waters on legal record, the international tribunal found that China’s coast guard had breached several UNCLOS articles governing safety and navigation at sea, striking down China’s claim that it had acted in a legal and professional manner.

#### Escalating Turkey crisis causes WWIII

Matthew Petti 20, national security reporter at the National Interest, “Will Turkey Drag America Into a ‘World War III Scenario’ With Russia?,” National Interest, 2/20/20, https://nationalinterest.org/blog/middle-east-watch/will-turkey-drag-america-%E2%80%98world-war-iii-scenario%E2%80%99-russia-125676

Russia and Turkey are headed towards a Cold War nightmare scenario after fighting between the two major powers in Syria left two Turkish soldiers dead.

Syrian ruler Bashar al-Assad is driving his forces into Idlib, the last rebel-held stronghold in Syria, with Russian support. Turkey faces a humanitarian crisis on its borders as up to two million Syrians fleeing Assad’s rule are left with nowhere else to go, and Turkish forces have entered Idlib to stop the offensive. Now, the United States is mulling over its response to the escalating tensions.

The fresh concerns about America’s role in the region come on the heels of an airstrike by either Russian or pro-Assad forces, which killed two Turkish soldiers during a rebel counter-offensive east of Idlib on Thursday. In response, the Turkish military has reportedly asked the United States to deploy anti-aircraft missiles and launch air patrols in Turkey in order to deter Russia.

“The North Atlantic Treaty Organization [NATO] has never seen fighting of this intensity this close to the border of a member state,” said Amb. Robert Ford, the last U.S. ambassador to Syria, at a Thursday press conference at the U.S. Capitol.

The prospect of a NATO intervention in Syria has exposed fault lines between the State Department and the Defense Department over the U.S. mission in Syria. The State Department has been Turkey’s closest remaining ally in Washington after the Turkish military began using Russian anti-aircraft missiles and attacked U.S.-backed, Kurdish-led forces in northeastern Syria.

But the U.S.-led “military coalition is focused on defeating ISIS in the eastern part of Syria,” Combined Joint Task Force Operation Inherent Resolve spokesman Col. Myles Caggins said in a Sky News interview on Wednesday. Caggins referred to Idlib as a “magnet for terrorist groups” who are “a nuisance, a menace and a threat to civilians.”

“We continue to call on pro-regime forces to halt the offensive and allow for humanitarian efforts in the area,” he added in a later statement.

The U.S. military had earlier called for de-escalation.

“We're seeing the Russians and the Turks have come very close to having more extensive conflict in the area. We're hopeful that they will find a solution to avoid that,” said Department of Defense spokesman Jonathan Hoffman on Wednesday. “There needs to be a political settlement in Syria that will be for the best interests of the Syrian people.”

The State Department has signaled stronger support for Turkey and the Turkish-backed rebels in Idlib since Assad began his offensive in early February.

“We stand by our NATO Ally Turkey . . . and fully support Turkey’s justified self-defense actions,” declared Secretary of State Mike Pompeo after pro-Assad forces killed several Turkish peacekeepers in Idlib on February 2.

Amb. James Jeffrey, the State Department official overseeing Syrian affairs, was in Turkey on February 11, as clashes erupted in Idlib between Turkish and pro-Assad forces, killing five Turkish troops.

“Today, in Idlib, our ally Turkey's soldiers are facing a threat,” Jeffrey declared in Turkish. “We have martyrs on the ground.”

Jeffrey told Turkish television two days later that Russia, Iran, and Assad will come to the table once they “see that they’re not going to make any more [military] progress without coming into conflict with us . . . or the Israeli Air Force or Turkey.”

Additionally, two former State Department officials called for the United States to back Turkey against Russia at a Thursday press conference at the U.S. Capitol.

Wa’el Alzayat, who served under both Ford and Jeffrey, emphasized that Assad’s record of atrocities “makes whatever ISIS did pale in comparison.”

He called for “urgent action to provide political and material support to Turkish forces today who are currently serving as a last line of defense, urgent action for NATO to signal to Russia that what is happening on its border is unacceptable, and we’ll defend an ally.”

“I think it is important that the government of the United States, governments in the North Atlantic Treaty Organization, meet with Turkish officials to discuss how one could establish a safe zone for Syrian civilians on the Syrian side of the Syrian-Turkish border,” Ford himself said. “The Turks can help with the safe zone from inside Turkey, but because they’re facing Russia, they will need help from the United States.”

Ford emphasized to the National Interest that he is not calling for U.S. forces to deploy in Syria itself, adding that a U.S. incursion into Idlib with “combat air patrols” could mean a “World War III scenario.”

U.S. forces are already deployed to northeastern Syria alongside Kurdish-led counterterrorism forces. They reportedly killed a local man during a clash with a pro-Assad militia on February 12, and nearly ran a Russian military vehicle off the road in a confrontation on Wednesday.

#### Failure to cooperatively apply international norms to cyber weapons allows proliferating information warfare

Justin Lynch 19, Associate Editor at Fifth Domain, has written for the New Yorker, the Associated Press, Foreign Policy, the Atlantic, 1/24/19, “Why cyberwar is contributing to a potential doomsday,” https://www.fifthdomain.com/thought-leadership/2019/01/25/why-cyberwar-is-contributing-to-a-potential-doomsday/

A wave of new cyberattacks and an increase in information warfare tactics are helping to create an existential threat to humanity, according to the Bulletin of the Atomic Scientists, who said in their annual report that its Doomsday Clock “is two minutes to midnight.”

The group of top researchers, scientists and thinkers warned Jan. 24 that the world is in a “new abnormal” state of crisis that is comparable when the United States pursued the hydrogen bomb in 1952. Since 1947, the Bulletin of the Atomic Scientists has released a report that uses the clock as an indicator of how close the world is to an existential threat to humanity, or midnight.

As institutions and government agencies face a proliferation of hacking ― attacks that often undercut humanity’s trust in those organizations ― the new fears fuel the state of crisis, said Herb Lin, senior research scholar for cyber policy and security at Stanford University and contributor to the report.

“The lack of cybersecurity for your systems is dangerous because it reduces confidence in the infrastructure,” Lin told Fifth Domain. He gave an example of how fears of election hacking can undermine voting confidence.

Officials from the Department of Homeland Security shared a similar sentiment during the mid-term election season. While the elections went off without acknowledgement of such an incident occurring, Lin cited it as an example of how “the lack of cybersecurity is reducing confidence in democracy.”

He described the threat as an “insidious use of cyber technology and cyber tools to target and exploit weaknesses in human cognition and thinking."

In its annual report, the group warned that “rather than a cyber Armageddon that causes financial meltdown or nationwide electrical blackouts,” a larger risk is the use of cyber-enabled information warfare that erodes “the trust and cohesion on which civilized societies rely.”

Evidence shows, however, that such disinformation campaigns occurred during the 2018 midterm elections.

“Russia, and other foreign countries, including China and Iran, conducted influence activities and messaging campaigns targeted at the United States to promote their strategic interests,” Director of National Intelligence Dan Coats said in a review of the mid-term election’s security.

To stem the tide of cyber and information warfare, the Bulletin of the Atomic Scientists suggested a collaborative approach between countries.

“The international community should begin multilateral discussions that aim to discourage cyber-enabled information warfare,” the group said in its annual report.

However, rallying major powers around an agreed upon set of norms has so far been unsuccessful in cyberspace. The prospects for future cohesion appear to be slim.

#### Information warfare’s the most dangerous existential threat humanity has ever faced---massive threat multiplier

John Mecklin 20, Editor, Science and Security Board, Bulletin of the Atomic Scientists, 1/23/20, “Closer than ever: It is 100 seconds to midnight,” https://thebulletin.org/doomsday-clock/current-time/

To: Leaders and citizens of the world

Re: Closer than ever: It is 100 seconds to midnight

Date: January 23, 2020

Humanity continues to face two simultaneous existential dangers—nuclear war and climate change—that are compounded by a threat multiplier, cyber-enabled information warfare, that undercuts society’s ability to respond. The international security situation is dire, not just because these threats exist, but because world leaders have allowed the international political infrastructure for managing them to erode.

In the nuclear realm, national leaders have ended or undermined several major arms control treaties and negotiations during the last year, creating an environment conducive to a renewed nuclear arms race, to the proliferation of nuclear weapons, and to lowered barriers to nuclear war. Political conflicts regarding nuclear programs in Iran and North Korea remain unresolved and are, if anything, worsening. US-Russia cooperation on arms control and disarmament is all but nonexistent.

Public awareness of the climate crisis grew over the course of 2019, largely because of mass protests by young people around the world. Just the same, governmental action on climate change still falls far short of meeting the challenge at hand. At UN climate meetings last year, national delegates made fine speeches but put forward few concrete plans to further limit the carbon dioxide emissions that are disrupting Earth’s climate. This limited political response came during a year when the effects of manmade climate change were manifested by one of the warmest years on record, extensive wildfires, and quicker-than-expected melting of glacial ice.

Continued corruption of the information ecosphere on which democracy and public decision making depend has heightened the nuclear and climate threats. In the last year, many governments used cyber-enabled disinformation campaigns to sow distrust in institutions and among nations, undermining domestic and international efforts to foster peace and protect the planet.

This situation—two major threats to human civilization, amplified by sophisticated, technology-propelled propaganda—would be serious enough if leaders around the world were focused on managing the danger and reducing the risk of catastrophe. Instead, over the last two years, we have seen influential leaders denigrate and discard the most effective methods for addressing complex threats—international agreements with strong verification regimes—in favor of their own narrow interests and domestic political gain. By undermining cooperative, science- and law-based approaches to managing the most urgent threats to humanity, these leaders have helped to create a situation that will, if unaddressed, lead to catastrophe, sooner rather than later.

Faced with this daunting threat landscape and a new willingness of political leaders to reject the negotiations and institutions that can protect civilization over the long term, the Bulletin of the Atomic Scientists Science and Security Board today moves the Doomsday Clock 20 seconds closer to midnight—closer to apocalypse than ever. In so doing, board members are explicitly warning leaders and citizens around the world that the international security situation is now more dangerous than it has ever been, even at the height of the Cold War.

Civilization-ending nuclear war—whether started by design, blunder, or simple miscommunication—is a genuine possibility. Climate change that could devastate the planet is undeniably happening. And for a variety of reasons that include a corrupted and manipulated media environment, democratic governments and other institutions that should be working to address these threats have failed to rise to the challenge.

The Bulletin believes that human beings can manage the dangers posed by the technology that humans create. Indeed, in the 1990s leaders in the United States and the Soviet Union took bold actions that made nuclear war markedly less likely—and as a result the Bulletin moved the minute hand of the Doomsday Clock the farthest it has been from midnight.

### Plan

#### The United States federal government should increase its security cooperation with the North Atlantic Treaty Organization to clarify the conditions under which Article V of the North Atlantic Treaty can be activated in response to cyber threats.

### Solvency

#### Internal clarification of article V is key

David H. Ucko 10, adjunct fellow at the Department of War Studies, King's College London"Resetting Article 5: Toward a New Understanding of NATO's Security Guarantees", World Politics Review, https://www.worldpoliticsreview.com/articles/6838/resetting-article-5-toward-a-new-understanding-of-natos-security-guarantees

For all this, the alliance badly needs a clarification of its collective security mechanism, for, though its current ambiguity may fool prospective adversaries, it really should not fool NATO itself. There is a need, in other words, to chart a middle path between traditionalists and revolutionaries, whereby NATO maintains a solidarity clause but comes to a new, narrower and shared understanding of its meaning and implications. The point would be to downgrade the expectations that come with NATO membership by talking more honestly, within NATO, about what the alliance is likely and able to commit to.

First, it would be necessary to convey, in private, to members that an Article 5 response is not automatic, but is rather the product of intensely political processes within each NATO state, and that even if a response is forthcoming, there is no way of guaranteeing that it will be timely or particularly effective. The language of an unflinching, immediate, collective and effective response may be appropriate for audiences outside of NATO, but not for internal discussion. Within the alliance, less grandstanding rhetoric and greater transparency would reduce the scope for obfuscation. The language of collective security would remain -- for symbolic reasons, for the deterrent role that Article 5 still plays and for the foundation it provides for retaliatory action. But the point would be to re-emphasize within the alliance the oft-forgotten provision of Article 5 whereby each member takes only "such action as it deems necessary" when fulfilling its security obligations.

Second, NATO would need to delineate much more clearly what types of threats it is capable of countering. No doubt a nontraditional attack can be as devastating as a military strike, but it does not follow that NATO is equally prepared to handle both. The decision regarding NATO's role in any incident must be based not only on the severity of a potential attack, but also on NATO's ability to mount an effective response. Whereas the language of solidarity following the Sept. 11 attacks was certainly appropriate, a case can be made that NATO ultimately overextended itself in invoking Article 5. The invocation established a dangerous precedent for the kinds of threats that the article might cover, many of which NATO lacks the expertise to deter, to forestall or to counter. Talking loudly about collective defense against non-traditional attacks without a concomitant ability to deliver when they occur is likely to provoke a crisis of credibility for the alliance.

Similar gaps between expectations and capabilities surround the issue of cybersecurity, which Secretary-General Rasmussen recently suggested should be covered by Article 5, as well as energy-security threats and economic warfare: NATO undoubtedly has a role to play in protecting its members from these potentially very harmful forms of attack, yet until the capability is created, it may want to interpret its security guarantees more narrowly. This also raises the question of how serious an attack in a nontraditional domain would need to be to trigger Article 5 considerations. Some informal criteria would need to be agreed upon to inform expectation, yet clearly this is also something that would need to be settled behind closed doors, so as not to invite attack and provocation under the established threshold or precisely where NATO's guarantees are the weakest.

Naturally, the prospect of agreeing within NATO to a more honest but weaker Article 5 regime will elicit much support among those who rely most on NATO's security guarantees. Nonetheless, greater transparency is preferable to false hope. A hardnosed stocktaking of what NATO can and cannot do would also provide for a more promising foundation on which progress could be made: a common appraisal of problems faced and a framework for finding limited solutions, where possible. This would also allow those nations that feel most vulnerable to make their own security arrangements, even if that means seeking relationships outside the alliance structure. In the event that such arrangements are inimical to NATO's interests, the onus would then be on the alliance itself to provide a preferable alternative. In that sense, greater transparency would make the self-interest of individual members the foundation of NATO's collective defense mechanism, rather than the need to ensure the alliance's solidarity or prove its relevance, the reasons most often used to justify Article 5 security guarantees today but whose rhetorical appeal rarely translates into action.

Upholding a security regime that is limited, patchy and short on substance is far from ideal, yet it would accurately reflect the alliance's current intentions, capabilities and political will. So long as both those making the promise of collective defense and those hoping to take it up are mutually aware of its true possibilities and very real limitations, it may be the least-bad and most-viable way out of an awkward situation.

#### Internal honesty exerts pressure on allies to fill capability gaps

Łukasz Kulesa 19, Łukasz Kulesa is the deputy head of research at the Polish Institute of International Affairs (PISM), “The Future of Deterrence: Effectiveness and Limitations of Conventional and Nuclear Postures,” Carnegie Europe, 11/28/19, https://carnegieeurope.eu/2019/11/28/future-of-deterrence-effectiveness-and-limitations-of-conventional-and-nuclear-postures-pub-80440

Two recent events have forced the alliance to tailor deterrence to specific actors. The first was Moscow’s aggression toward Ukraine from 2014 onward, along with its military exercises that rehearsed a war with NATO. The second was the deterioration of the situation in the Middle East and North Africa: civil wars in Syria and Libya and the emergence of the self-proclaimed Islamic State in Iraq and Syria, which helped spawn the 2015 migration crisis. Since then, Russia has remained the focus of NATO’s deterrence, but a reflection is under way on how to best deter nonstate and state threats from the Middle East and North Africa.

Going forward, NATO will need to consider three dimensions of deterrence: who, what, and how. First, the alliance knows that it may be called on to deter other actors in addition to Russia, but it needs to spell out which ones, because each requires a different mix of means and strategies. Second, NATO needs to consider what types of action, beyond armed attacks, it needs to deter. This applies to the full spectrum of threats, including those from Russia. And third, the allies have to constantly review the effectiveness of their current deterrence approaches in all areas of focus, as modern conflict has come to be dominated by unconventional and hybrid tactics used by state and nonstate actors.

ISSUES AT STAKE

THE WHO

On NATO’s Eastern flank, the focus is on Russia. Moscow seeks to achieve its strategic aims—a sphere of influence in the neighborhood and the prevention of NATO’s expansion—without a war but seems ready to engage in brinkmanship and is working on creating favorable conditions to prevail in a conflict. This makes it necessary for the allies to develop a credible deterrence strategy.

However, NATO also has to deter the threats from states and nonstate entities in the Middle East and North Africa. The effects of conflicts in the region are already being felt on NATO territory, and governments in the most affected member states are asking how they can prevent further spillover of existing and potential crises. The discussions have been light on specifics, though not for lack of options. The allies are already fielding missile defenses in Turkey to defend against missile attacks from Syria; deterring conventional attacks on NATO territory could be the next step, depending on developments in Syria itself. Other actors of concern include Iran, with its growing missile arsenal, and nonstate groups operating in Lebanon, Libya, and Syria.

Farther afield, given the U.S. and other allies’ engagement in the Asia Pacific and NATO’s close links with Australia, Japan, New Zealand, and South Korea, the alliance may have to consider the feasibility of deterring China and North Korea from threatening or harming member states. This would be a new task with significant resource implications and should not be undertaken lightly.

THE WHAT

Internally, NATO members need to be clear about specific actions they can reasonably expect the alliance to deter. Clearly, an armed attack—from whatever direction—is one course of action to be deterred, but other actions are not so simple.1

In the case of Russia (and other state actors), the focus is also on deterring coercion: the act of adversaries imposing their will on NATO allies through a combination of military threats and nonmilitary means. For now, the thinking at NATO has emphasized deterrence of a territorial grab or blockade in the Baltic region. However, the characteristics of the Russian approach to warfare mean that the alliance has to look beyond the Baltic Sea and beyond the physical domain, mainly to the cyber realm.2 More and more of the critical systems running hospitals, carrying electricity, or patrolling the skies are now connected to the internet and therefore vulnerable. NATO’s adversaries can, in theory, block allied governments from coming to each other’s aid by threatening devastating cyber attacks that will cause populations to panic and cripple economies.

NATO has already declared that a cyber attack could lead the alliance to invoke its Article 5 collective defense clause, a statement that aims to have a deterrent effect—though there is little evidence that it has stopped adversaries from trying.3 This is mainly because most cyber attacks are designed to stay below the level that would trigger a response of the whole alliance. The allies need a clearer policy on what to do if the line is crossed one day. That policy must also address the thorny issue of credible attribution and should be rehearsed rigorously.

THE HOW

NATO does not need to mirror the activities of its adversaries to deter effectively. The idea is to signal that the alliance will not be intimidated or coerced, but that can be done in multiple ways.

With regard to Russia and the threat of a land incursion, NATO has decided to rely on limited forward deployments along its Eastern flank and on the ability to reinforce quickly those small contingents in times of crisis. The shortcoming of this posture is that if Russia overwhelms the first line of defense, it may be able to use the strength of its conventional forces, as well as the threat of nuclear weapon use, to thwart allied reinforcement.

NATO, as a whole, is adapting its posture to respond, and the United States is strengthening its military presence in Europe to address these potential weak points. The mix of U.S. troops and stored equipment and supplies in Europe is being expanded, including in Poland. And NATO has taken steps to improve its ability to deploy units from North America and move them around Europe by creating a Joint Force Command for the Atlantic and a Joint Support and Enabling Command. Other means of strengthening deterrence include implicit or explicit threats of political or economic sanctions or threats of countermeasures in cyberspace.

Regarding the South, the exact form of deterrence has to match the threat that NATO chooses to deter. With regard to potential state adversaries, NATO’s existing deterrence tools and military capabilities can be utilized against threats from that direction. The creation of the Strategic Direction South Hub—a consultation and coordination body for allies and partners—at the NATO command in Naples, Italy, also contributes to the deterrence mission. However, these measures alone will not deter the main challenge in the South: terrorist groups, with the potential to strike in Europe, operate in lawless spaces.

RECOMMENDATIONS

NATO may be back to its traditional mission of deterrence, but deterrence itself has evolved. A new approach must be adapted to today’s environment, in which a number of deterrence challenges need to be tackled simultaneously and sophisticated nonconventional means can be used jointly with traditional military tools to test the alliance.

MAINTAIN ALLIANCE COHESION

While the allies’ initial response to deterrence challenges has been impressive, in the long run, deterrence fatigue may present problems. NATO needs to keep all allies committed to the deterrence mission and continue to secure sufficient contributions of committed forces, capabilities, and resources. The risk is that allies’ unity and cohesion—the indispensable foundations of NATO—will weaken as memories of the Islamic State’s caliphate and of Russia’s aggression against Ukraine fade. Adversaries will do their part to sow or exploit divisions or doubts about the strength of solidarity among alliance members.

To keep cohesion from fraying, NATO’s leadership should continuously engage every ally in dialogue about the rationale for the posture, the threat assessment, and members’ views on, and concerns over, the implementation of the deterrence mission. National governments have the same essential responsibility toward their parliaments and publics. NATO must also make sure that discussions do not focus only on one strategic direction but rather address both defense and crisis-management tasks.

Engagement with partners should include a dedicated dialogue on deterrence issues. In some cases, based on mutual consent, NATO should be ready to explore coordinated deterrence signaling or mutually reinforced deterrence activities, such as joint statements, deployments, or exercises.

Engagement with adversaries must be seen as an inseparable companion to deterrence. Dialogue and multiple contact channels remain crucial to convey and receive deterrence signals, avoid accidental or inadvertent escalation, and explore risk-reduction and arms control opportunities.

DETER RUSSIA’S ADVENTURISM

In the foreseeable future, specific challenges connected with deterring Russia will continue to dominate the practical agenda. As a priority, the allies should fully implement the 2018 decisions to adapt NATO’s command and force structure.4 The military credibility of the current deterrence posture depends, to a large extent, on the alliance’s ability to speedily augment its forward-deployed units with follow-on forces.

The allies should look for new ways of stimulating the development of necessary capabilities and interoperability. A more transparent discussion of the major gaps in allied capabilities could help exert pressure on members to make relevant investments. The NATO Military Committee should play a more active role in the alliance’s adaptation by more visibly highlighting the military requirements for credible deterrence to civilian authorities and—via individual military leaders—to NATO populations.

#### Establishing internal limits to the collective defense is key to a credible cyber policy for NATO

Jarno Limnéll 16, Professor of Cybersecurity, Aalto University, Finland, Charly Salonius-Pasternak, Senior Research Fellow, The Finnish Institute of International Affairs, Challenge for NATO – Cyber Article 5, Briefing Paper, Published by the Center for Asymmetric Threat Studies, June 2016, Swedish Defence University, https://www.diva-portal.org/smash/get/diva2:1119569/FULLTEXT01.pdf

What then might lead to cyber-attack causing Article 5 to be invoked? No one knows, as it is situationally dependent. The old way of thinking is that a ‘severe cyber-attack’ has to involve physical destruction – people have to die, and physical damage must be seen in the critical infrastructure. However, as we become ever more dependent on data and ‘non-kinetic assets’, could for example the manipulation of health records lead to Article 5 being invoked? Moreover, is there a difference between banking data and health-care data being manipulated, with one potentially leading to severe economic disruptions and the other in extremis to death.

Formulating clear doctrines is frequently preferred by militaries, while politicians and diplomats prefer flexibility in message and response. The Alliance has two paths it can chose in creating the doctrine regarding cyber. It can either chose a public approach, rather similar to its approach when creating its most recent strategic concept. In such a document it could generally describe what constitutes an attack that would qualify for the invocation of Article 5, and what would be an accepted retaliatory action. The other path is to maintain strategic ambiguity, recognizing that formulating clear redlines would invite potential adversaries to push up to the red line. In this case developing the doctrine is still important, but would then be for internal use only. This non-public approach may reduce the objective of improving the Alliance´s cyber deterrence. The pace of development in the field would argue against an overly specific set of guidelines or doctrine, lest it require too frequent and politically challenging updates.

The current ‘cyber warfare playbook’ is still a slim volume - but it is growing by the day. In order to remain a credible defence alliance, NATO must possess a credible cyber policy, including cyber deterrence. Credibility comes from a largely similar set of actions as NATO has engaged in regarding conventional military. Doing it in the cyber domain is, however, harder at the moment. For example, what is the equivalent of standing up in practice permanent battalions in member states? How do you exercise, publicly message determination to defend and counter aggression, in a serious but non-threatening way?

NATO has to find a clear way to deal with a ‘Cyber Article 5’ event. It may be necessary to reinterpret what Article 5 and an armed attack constitute in today´s world. The biggest challenges is to reach a shared understanding of the limits (physical and cyber) which could lead a member state to invoke Article 5 and delineate what proportionality in response means. The decisions are political by their nature and requires strong understanding on strategic cyber domain and its development by the political actors involved. Ultimately, success will depend on how the cyber is blended with traditional political and military power.

## Russia ADV

### Cyber Impact---AT: Defense

#### Cyberattacks on critical infrastructure cause nuclear retal

Michael T. Klare 19, professor emeritus of peace and world security studies at Hampshire College, “Cyber Battles, Nuclear Outcomes? Dangerous New Pathways to Escalation,” Arms Control Association, November 2019, armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation

Yet another pathway to escalation could arise from a cascading series of cyberstrikes and counterstrikes against vital national infrastructure rather than on military targets. All major powers, along with Iran and North Korea, have developed and deployed cyberweapons designed to disrupt and destroy major elements of an adversary’s key economic systems, such as power grids, financial systems, and transportation networks. As noted, Russia has infiltrated the U.S. electrical grid, and it is widely believed that the United States has done the same in Russia.12 The Pentagon has also devised a plan known as “Nitro Zeus,” intended to immobilize the entire Iranian economy and so force it to capitulate to U.S. demands or, if that approach failed, to pave the way for a crippling air and missile attack.13

The danger here is that economic attacks of this sort, if undertaken during a period of tension and crisis, could lead to an escalating series of tit-for-tat attacks against ever more vital elements of an adversary’s critical infrastructure, producing widespread chaos and harm and eventually leading one side to initiate kinetic attacks on critical military targets, risking the slippery slope to nuclear conflict. For example, a Russian cyberattack on the U.S. power grid could trigger U.S. attacks on Russian energy and financial systems, causing widespread disorder in both countries and generating an impulse for even more devastating attacks. At some point, such attacks “could lead to major conflict and possibly nuclear war.”14

These are by no means the only pathways to escalation resulting from the offensive use of cyberweapons. Others include efforts by third parties, such as proxy states or terrorist organizations, to provoke a global nuclear crisis by causing early-warning systems to generate false readings (“spoofing”) of missile launches. Yet, they do provide a clear indication of the severity of the threat. As states’ reliance on cyberspace grows and cyberweapons become more powerful, the dangers of unintended or accidental escalation can only grow more severe.

#### Causes existential nuclear risks

Martin **Rees 18**, Astronomer Royal, founded the Centre for the Study of Existential Risk, Fellow of Trinity College and Emeritus Professor of Cosmology and Astrophysics at the University of Cambridge, “1. Deep in the Anthropocene,” in On the Future: Prospects for Humanity, 10/16/2018, Princeton University Press, pp 11-60

Nuclear annihilation still looms over us: the only consolation is that, thanks to arms control efforts between the superpowers, there are about five times fewer weapons than during the Cold War— Russia and the United States each have about seven thousand—and fewer are on ‘hair trigger’ alert. However, there are now nine nuclear powers, and a higher chance than ever before that smaller nuclear arsenals might be used regionally, or even by terrorists. Moreover, we can’t rule out, later in the century, a geopolitical realignment leading to a standoff between new superpowers. A new generation may face its own ‘Cuba’—and one that could be handled less well (or less luckily) than the 1962 crisis was. A near-existential nuclear threat is merely in abeyance.

Chapter 2 will address the twenty-first-century sciences—bio, cyber, and AI—and what they might portend. Their misuse looms as an increasing risk. The techniques and expertise for bio- or cyberattacks will be accessible to millions—they do not require large special-purpose facilities like nuclear weapons do. Cybersabotage efforts like ‘Stuxnet’ (which destroyed the centrifuges used in the Iranian nuclear weapons programme), and frequent hacking of financial institutions, have already bumped these concerns up the political agenda. A report from the Pentagon’s Science Board claimed that the impact of cyberattack (shutting down, for instance, the US electricity grid) could be catastrophic enough to justify a nuclear response.4

#### Causes nuclear retaliation

Robert **Tilford 12**, Writer for The Examiner, “Cyber Attackers Could Easily Shut Down the Electric Grid for the Entire East Coast,” Examiner, 07/27/12, http://www.examiner.com/article/cyber-attackers-could-easily-shut-down-the-electric-grid-for-the-entire-east-coa

“Cyber attackers could all too easily shut down the electric grid for the entire east coast, the west coast, and the middle part of our country”, said Senator Grassley on July 26, 2012. “Any one attack could leave dozens of major cities and tens of millions of Americans without power. We know, because we were shown in a room here in the Capitol, how an attack could take place and what damage it would do, so we know this is not just make believe”, he said. So what would a cyber attack look like anyway? The Senator explained: “Without ATMs or debit card readers, commerce would immediately grind to a halt. My daughter, who lives here in the DC area, lost power when the storm hit. They waited for a number of hours, and then they took all the food out of their freezer, they gave away what they could, and they threw the rest away. And that was the way it was all over. Their power was out for about a week, and it made it very difficult. They are fortunate enough to have a basement, and the heat wasn’t oppressive down there. Without refrigeration, food would rot on the shelves, the freezers would have to be emptied, and people could actually go hungry. Without gas pumps, transportation arteries would clog with abandoned vehicles. Without cell phones or computers, whole regions of the country would be cut off from communication and families would be unable to reach each other. Without air conditioning and without lifesaving technology and the service of hospitals and nursing homes, the elderly and sick would become much sicker and die. Most major hospitals have backup power, but it is only for a limited amount of time. It depends on how much fuel they can store, and that is very limited”, Senator Grassley said. The devastation that the Senator describes is truly unimaginable. To make matters worse a cyber attack that can take out a civilian power grid, for example could also ~~cripple~~ harm the U.S. military. The senator notes that is that the same power grids that supply cities and towns, stores and gas stations, cell towers and heart monitors also power “every military base in our country.” “Although bases would be prepared to weather a short power outage with backup diesel generators, within hours, not days, fuel supplies would run out”, he said. Which means military command and control centers could go dark. Radar systems that detect air threats to our country would shut Down completely. “Communication between commanders and their troops would also go silent. And many weapons systems would be left without either fuel or electric power”, said Senator Grassley. “So in a few short hours or days, the mightiest military in the world would be left scrambling to maintain base functions”, he said. We contacted the Pentagon and officials confirmed the threat of a cyber attack is something very real. Top national security officials—including the Chairman of the Joint Chiefs, the Director of the National Security Agency, the Secretary of Defense, and the CIA Director— have said, “preventing a cyber attack and improving the nation’s electric grids is among the most urgent priorities of our country” (source: Congressional Record). So how serious is the Pentagon taking all this? Enough to start, or end a war over it, for sure (see video: Pentagon declares war on cyber attacks http://www.youtube.com/watch?v=\_kVQrp\_D0kY&feature=relmfu ). A cyber attack today against the US could very well be seen as an “Act of War” and could be met with a “full scale” US military response. That could include the use of “nuclear weapons”, if authorized by the President.

### Cyber Impact---AT: No Escalation

#### Large-scale cyber certainly escalates---laundry list of scenarios

Stephen Cimbala 22, professor in the Political Science department at Pennsylvania State University Brandywine, “Nuclear-Crisis Management and Cyber War—A Dangerous Crossroads,” Naval War College Review, vol. 75, no. 1, 04/27/2022, https://digital-commons.usnwc.edu/nwc-review/vol75/iss1/5

POTENTIAL DISRUPTERS

Information or cyber warfare has the potential to attack or to disrupt successful crisis management with regard to each of the preceding attributes.24 First, infowar can muddy the signals being sent from one side to the other in a crisis. This can be done deliberately or inadvertently. Suppose one side plants a virus or worm in the other’s communications networks.25 The virus or worm becomes activated during the crisis and destroys or alters information. The missing or altered information may make it more difficult for the cyber victim to arrange a military attack; however, destroyed or altered information also may mislead either side into thinking that its signal has been interpreted correctly when it has not. Thus, side A may intend to signal “resolve” instead of “yield” to its opponent on a particular issue; side B, misperceiving what it has received as a “yield” message, may decide to continue its aggression, but then meets unexpected resistance, causing a much more dangerous situation to develop. There is also the possibility of cyber-enabled preemption to disable enemy nuclear missiles before they reach the launchpad or during the launch itself. Apparently, the United States has used such “left-of-launch” techniques against North Korea.26 During a nuclear crisis, would such a move be accepted by the attacked party as one of intimidation and deterrence or, to the contrary, would offensive cyber war against missile launches prompt a nuclear first use or first strike by the defender for fear of losing its retaliatory capability?

Infowar also can destroy or disrupt communication channels necessary for successful crisis management. One way it can do this is by disrupting communication links between policy makers and military commanders during a period of high threat and severe time pressure. Unanticipated problems, from the standpoint of civil-military relations, may arise under these conditions. For example, political leaders may have predelegated limited authority for nuclear release or launch under restrictive conditions; only when these few conditions obtain, according to the protocols of predelegation, would military commanders be authorized to employ nuclear weapons distributed within their commands.27 Clogged, destroyed, or disrupted communications could prevent top leaders from knowing that military commanders perceive a situation to be far more desperate, and thus permissive of nuclear initiative, than it really is. For example, during the Cold War, disrupted communications between the U.S. national command authority and ballistic-missile submarines, once the latter came under attack, could have resulted in a joint decision by submarine officers and crew, in the absence of contrary instructions, to launch.

Second, infowar during a crisis almost certainly will increase the time pressure under which political leaders operate. It may do this literally, or it may affect the perceived timelines within which the policy-making process yields its decisions. Once either side sees parts of its command, control, and communications (C3) system being subverted by phony information or extraneous cyber noise, its sense of panic at the possible loss of military options will be enormous. In the case of American Cold War nuclear war plans, for example, disruption of even portions of the strategic C3 system could have prevented competent execution of parts of the Single Integrated Operational Plan (SIOP), the nation’s strategic nuclear war plan. The Cold War SIOP depended on finely orchestrated time-on-target estimates and precise damage expectancies against various classes of targets.28 Partly misinformed or disinformed networks and communications centers would have led to redundant attacks against the same target sets and, quite possibly, unplanned attacks on friendly military or civilian installations. Even in the post–Cold War world of flexible nuclear-response plans, the potential slide toward preemption, on the basis of mistaken or exaggerated fears of C2 vulnerability, casts a shadow over deterrence stability. As Blair has warned, “There are no widely accepted methods for calculating command and control performance under wartime conditions, and empirical validation of such an assessment cannot be done. Compared with the tight and tidy standard calculations of force vulnerability, any objective assessment of command and control systems would raise more questions than it answered.”29

A third potentially disruptive effect of infowar on nuclear-crisis management is that it may reduce the search for available alternatives to the few and desperate. Policy makers seeking escapes from crisis denouements need flexible options and creative problem-solving. Victims of infowar may have a diminished ability to solve problems routinely, let alone creatively, once information networks are filled with flotsam and jetsam. Questions to operators will be posed poorly, and responses (if available at all) will be driven toward the least common denominator of previously programmed SOPs. Retaliatory systems that depend on launchon-warning dynamics instead of survival after riding out an attack are especially vulnerable to reduced time cycles and restricted alternatives. “A well-designed warning system cannot save commanders from misjudging the situation under the constraints of time and information imposed by a posture of launch on warning. Such a posture truncates the decision process too early for iterative estimates to converge on reality. Rapid reaction is inherently unstable because it cuts short the learning time needed to match perception with reality.”30

The propensity to search for the first available alternative that meets minimum satisfactory conditions of goal attainment is strong enough under normal conditions in nonmilitary bureaucratic organizations.31 In civil-military C2 systems under the stress of nuclear-crisis decision-making, the first available alternative quite literally may be the last—or so policy makers and their military advisers may persuade themselves. Accordingly, the bias toward prompt and adequate solutions is strong. During the Cuban missile crisis, for example, a number of members of the presidential advisory group continued to propound an air strike and invasion of Cuba during the entire thirteen days of crisis deliberation. Had less time been available for debate and had President Kennedy not deliberately structured the discussion in a way that forced alternatives to the surface, the air strike and invasion might well have been the chosen course of action.32 Paul K. Davis and coauthors have noted the following:

Usual discussions of crisis stability assume that leaders are in control of their nuclear capabilities. Again, history is sobering. President Kennedy became worried in 1961 about possible unilateral actions by military leaders to prepare a preemptive strike against the Soviet Union. He instigated efforts to tighten the President’s personal control. Soviet leadership worried about survivability of its forces and developed capability for launch on warning and automatic response. Such systems could be the source of accidental war.33

Fourth and finally on the issue of crisis management, infowar can cause flawed images of each side’s intentions and capabilities to be conveyed to the other, with potentially disastrous results. Another example from the Cuban missile crisis demonstrates the possible side effects on U.S. crisis management of simple misunderstanding and noncommunication. At the most tense period of the crisis, a U-2 reconnaissance aircraft got off course and strayed into Soviet airspace. U.S. and Soviet fighters scrambled, and a possible Arctic confrontation of air forces loomed. Khrushchev later told Kennedy that Soviet air defenses might have interpreted the U-2 flight as a prestrike reconnaissance mission or as a bomber, calling for a compensatory response by Moscow.34 Fortunately, Moscow chose to give Washington the benefit of the doubt in this instance and to permit U.S. fighters to escort the wayward U-2 back to Alaska. Why this scheduled U-2 mission was not aborted once the crisis began never has been revealed fully; the answer may be as simple as bureaucratic inertia compounded by noncommunication down the chain of command by policy makers who failed to appreciate the risk of “normal” reconnaissance under these extraordinary conditions.

The significance of the preceding discussion and examples is underscored by the assessment of expert analyst Martin C. Libicki about the relationship between cyber war and crisis management.

To generalize, a situation in which there is little pressure to respond quickly, in which a temporary disadvantage or loss is tolerable, and in which there are grounds for giving the other side some benefit of the doubt is one in which there is time for crisis management to work. Conversely, if the failure to respond quickly causes a state’s position to erode, a temporary disadvantage or degree of loss is intolerable, and there are no grounds for disputing what happened, who did it, and why—then states may conclude that they must bring matters to a head quickly.35

SCENARIOS AND RISKS

The outcome of a nuclear-crisis-management scenario influenced by information operations may not be a favorable one. Despite the best efforts of crisis participants, the dispute may degenerate into a nuclear first use or first strike by one side and retaliation by the other. In that situation, information operations by either side or both might make it more difficult to limit the war and bring it to a conclusion before catastrophic destruction and loss of life has taken place. Although there are no such things as “small” nuclear wars compared with conventional wars, there can be different kinds of “nuclear” wars, in terms of their proximate causes and consequences.36 Possibilities include a nuclear attack from an unknown source; an ambiguous case of possible, but not proved, nuclear first use; a nuclear “test” detonation intended to intimidate, but with no immediate destruction; or a conventional strike mistaken, at least initially, for a nuclear one.

With regard to the last-mentioned case, George H. Quester has noted that the “United States and other powers have developed some very large and powerful conventional warheads, intended for destroying the hardened underground bunkers that may house an enemy command post or a hard-sheltered weapons system. Such ‘bunker-buster’ bombs radiate a sound signal when they are used and an underground seismic signal that could be mistaken from a distance for the signature of a small nuclear warhead.”37 In such an instance, the adversary may question why its command posts or strategic assets are being targeted and assume the actions are the prelude to an all-out strategic strike.

The dominant scenario of a general nuclear war between the United States and the Soviet Union preoccupied Cold War policy makers, so concerns about escalation control and war termination were swamped by apocalyptic visions of the end of days. The second nuclear age, coinciding roughly with the end of the Cold War and the demise of the Soviet Union, offers a more complicated menu of nuclear possibilities and responses.38 Interest in the threat or use of nuclear weapons by rogue states, aspiring regional hegemons, or terrorists, abetted by the possible spread of nuclear weapons among currently non-nuclear-weapons states, stretches the ingenuity of military planners and fiction writers.

In addition to the possibility of the world’s worst characters engaging in nuclear threat or first use, there also may be backsliding in political conditions, such as between the United States and Russia, or Russia and China, or China and India (among current nuclear-weapons states). Arguments assuming the continuation of stable deterrence among major powers depend on the continuation of favorable political auguries in regional or global politics. Conflicts that are politically unthinkable in one decade have a way of evolving into wars that are politically unavoidable in another; World War I is instructive in this regard. The war between Russia and Georgia in August 2008 was a reminder that local conflicts on regional fault lines between blocs or major powers have the potential to expand into worse. So, too, were the Balkan wars of Yugoslav succession in the 1990s. In these cases, Russia’s one-sided military advantage relative to Georgia in 2008 and NATO’s military power relative to that of Bosnians of all stripes in 1995 and Serbia in 1999 contributed to war termination without further international escalation.

Escalation of a conventional war into nuclear first use remains possible where operational or tactical nuclear weapons have been deployed with national or coalition armed forces. In allied NATO territory, the United States deploys several hundred substrategic, air-delivered nuclear weapons among bases in Belgium, Germany, Italy, the Netherlands, and Turkey.39 Russia probably retains several thousand operational or tactical nuclear weapons, including significant numbers deployed in western Russia.40 The New Strategic Arms Reduction Talks (New START) agreement establishes a notional parity between the United States and Russia in nuclear systems of intercontinental range.41 But U.S. and allied NATO superiority in advanced-technology, information-based conventional military power leaves Russia heavily reliant on tactical nukes as compensation for comparative weakness in nonnuclear forces. NATO’s members breathed a sigh of relief when Russia’s officially approved Military Doctrine of 2010 did not seem to lower the bar for nuclear first use compared with previous editions.42

However, Russia’s military doctrine does indicate a willingness to engage in nuclear first use in situations of extreme urgency for Russia, as defined by its political leadership.43 And, despite NATO’s evident superiority in conventional forces relative to those of Russia, neither the United States nor the rest of NATO is necessarily eager to get rid of its remaining substrategic nukes deployed among America’s NATO allies. An expert panel that NATO convened to set the stage for its 2010 review of the alliance’s military doctrine was carefully ambivalent on the issue of the alliance’s forward-deployed nuclear weapons. The possibility of negotiating away these weapons in return for parallel concessions from Russia was left open for further discussion. On the other hand, the NATO expert report underscored the present majority sentiment of governments that these weapons provided a necessary link in the chain of alliance deterrence options.44

Imagine now the unfolding of a nuclear crisis or the making of a decision for nuclear first use, under the conditions of both NATO and Russian campaigns employing strategic disinformation and information operations intended to disrupt enemy C3 and warning systems. Disruptive information operations against enemy systems on the threshold of nuclear first use, or shortly thereafter, could increase the already substantial difficulty of bringing fighting to a halt before a Europe-wide theater conflict or a strategic nuclear war ensues. All the previously cited difficulties in crisis management under the shadow of nuclear deterrence pending a decision for first use would be compounded by additional uncertainty and friction after the nuclear threshold had been crossed.

In addition, three new kinds of frictions would be posed for NATO. First, the cohesion of allied governments would be tested under conditions of unprecedented stress and danger, doubtless aided by a confused situation on the field of battle. Second, reliable intelligence about Russian intentions following Russian or NATO first use would be essential but challenging to nail down. Third, the first use of a nuclear weapon in anger since Nagasaki would establish a new psychological, political, and moral universe within which negotiators for de-escalation and war termination would have to maintain somehow their sangfroid, obtain agreed stand-downs from their militaries, and return nuclear-capable launchers and weapons to secured but transparent locations. All this would be taking place within the panic-spreading capabilities of 24/7 news networks and the Internet.

Theoretically, one might finesse the issue by eliminating cyber operations that potentially conflict with de-escalation. But the political desire to do so conflicts with the military need for timely information gathering, assessment, and penetration of enemy networks to accomplish two necessary, but somewhat opposed, missions. First, each side would want to anticipate correctly the timing and character of the other’s decision for nuclear first use—and, if possible, to throw logic bombs, Trojan horses, electronic warfare, and other impediments in the way. (Or, if methods of finesse are not available, bombing the relevant installations is always an option, although obviously a provocative one.) The second, and somewhat opposed, mission is to communicate reliably to the other side one’s preference for de-escalation, one’s willingness to de-escalate if reciprocity can be obtained, and one’s awareness of the possibility that the situation shortly will get out of hand. Consider the Russian General Staff and the president’s office filtering this hydra-headed group of messages while their forces are grappling in Georgia or Ukraine, with the smaller country having been taken into NATO membership, say, a year earlier, over Russia’s objections.

The problem of nuanced messages and the management of de-escalation, even short of war, is illustrated by the 1983 iteration of NATO’s command-post exercise ABLE ARCHER, held 7–11 November that year. An annual exercise, ABLE ARCHER was intended to practice nuclear-release procedures. Soviet intelligence routinely monitored these exercises. However, the 1983 version took place against a background of rising U.S.-Soviet political tensions and heightened suspicions within the Soviet political leadership and military high command that the United States and NATO might be preparing for a nuclear first strike. One reason that Russian sensitivities to the possibility of U.S. or NATO nuclear first use or first strike were high at this time was NATO’s decision to begin deploying Pershing II ballistic missiles and ground-launched cruise missiles of intermediate range in Europe, beginning in the fall of 1983. Soviet and Warsaw Pact reactions to ABLE ARCHER 83 included an unprecedented surge of Warsaw Pact technical collection, a significant increase in reconnaissance by Soviet strategic and naval aviation, and other unusual Soviet moves that indicated increased concern about NATO and U.S. intentions.45 The case illustrates how mistaken interpretations of “normal” events can overvalue pessimistic assessment at just the wrong time.46 As the President’s Foreign Intelligence Advisory Board concluded in 1990, “We believe that the Soviets perceived that the correlation of forces had turned against the USSR, that the US was seeking military superiority, and that the chances of the US launching a nuclear first strike—perhaps under cover of a routine training exercise—were growing. We also believe that the US intelligence community did not at the time, and for several years afterwards, attach sufficient weight to the possibility that the war scare was real.”47

The possibility of nuclear war by inadvertent escalation did not disappear with the end of the Cold War. The Russian General Staff remained alert to the possibility of a U.S. nuclear attack even as political relations between the two early post–Cold War states were officially nonhostile. In one instance, a U.S.- Norwegian Black Brant research rocket was launched from an island off the coast of Norway on 25 January 1995 to study the northern lights. This triggered a reaction from Russia’s missile-early-warning system, which alerted senior Russian defense officials, including then-President Boris Yeltsin, who for the first time activated his nuclear briefcase until confirmation was received that no attack was in progress.48

Avoiding mistaken nuclear preemption in a complex information environment is one kind of challenge; the problems in coordinating the management of de-escalation and conflict termination with the conduct of information operations offer another. Two examples follow. The first, already alluded to, is the use of a bunker-busting or other advanced-technology conventional weapon that the other side, during the fog of crisis or war, confuses with a nuclear first use or first strike. Russia expressed this concern specifically during New START negotiations in 2010, with regard to American plans to deploy some conventionally armed ballistic missiles on nuclear-capable intercontinental or transoceanic launchers.49 New START counting rules regard conventionally armed ballistic missiles as being nuclear-capable launchers, and therefore subject to overall restrictions on the numbers of deployed launchers and weapons. U.S. plans for Prompt Global Strike systems to include missiles or future space planes were approved first during the George W. Bush administration and carried forward under the Obama administration.

A second illustration of the problem of managing escalation control and conflict termination alongside information operations, one separate from the issue of escalation in Europe, is provided by the proposal for a joint NATO-Russian theater-missile-defense (possibly including air defenses) system. The idea had expert and highly visible political proponents on both sides of the Atlantic, and official Russian commentators have not closed the door to the possibility of some cooperation on ballistic-missile defenses (BMDs). Here, NATO and Russia are facing in two political directions: toward each other, displaying wariness but also openness; but regarding Iranian or other Middle Eastern leaders who may get their hands on nuclear weapons in the future, and who may be beyond deterrence based on the credible threat of nuclear (or other) retaliation, displaying concern.

However, the problems of achieving missile-defense cooperation between NATO and Russia are not only political. Even with the best of intentions among U.S., NATO, and Russian negotiators, the military-technical difficulties involved in coordinating BMD C3 systems are considerable. Indeed, they are not strictly “military-technical” but also heavily embedded with issues of political sovereignty; classified intelligence; and trust, among both governments and militaries. Even among NATO members, militaries differ in their national traditions, military-service identities, experiences in nuclear arms control, and willingness to share online information in real time with temporary partners who may be future enemies. For example, if a European theater-wide system of intelligence and missile-attack warning is established, how many capitals will host relevant servers and receive timely output? Who will decide that a missile warning is now a threat requiring activation of the European BMD system—can a single nation do so if a missile is headed its way, or must NATO (including the United States) and Russia agree before any action is taken in response?

If a political crisis between NATO and Russia erupts, and both sides already have deployed missile defenses, will Russian or American cyber warriors attempt to spoof or otherwise negate the other’s missile-defense component? Would it be better to reassure Russia regarding the surety of its own missile defenses, as against the possibility of a conventional or nuclear preemption? Neither Russia nor the United States will want to relinquish sovereign control over its part of any cooperative missile defenses. However, would it be more prudent to announce a withdrawal from the cooperative aspect of the regional BMD system during a crisis or to maintain the fiction of cooperation while attacking the other side’s cyber systems with Trojan horses, logic bombs, and trapdoors—just in case? Perhaps, in future nuclear or other crises, the U.S. and Russian cyber commands should have their own direct “hotline,” or in this case an encrypted digital link.

### Grid Impact---AT: Defense

#### It cascades globally AND it’s irreversible---extinction

Martin Rees 18, Astronomer Royal, founded the Centre for the Study of Existential Risk, Fellow of Trinity College and Emeritus Professor of Cosmology and Astrophysics at the University of Cambridge, “2. Humanity’s Future on Earth,” in On the Future: Prospects for Humanity, 10/16/2018, Princeton University Press, pp 61-119

2.5. TRULY EXISTENTIAL RISKS?

Our world increasingly depends on elaborate networks: electricity power grids, air traffic control, international finance, globally dispersed manufacturing, and so forth. Unless these networks are highly resilient, their benefits could be outweighed by catastrophic (albeit rare) breakdowns— realworld analogues of what happened in the 2008 global financial crisis. Cities would be ~~paralysed~~ [gridlocked] without electricity— the lights would go out, but that would be far from the most serious consequence. Within a few days our cities would be uninhabitable and anarchic. Air travel can spread a pandemic worldwide within days, wreaking havoc on the disorganised megacities of the developing world. And social media can spread panic and rumour, and economic contagion, literally at the speed of light.

When we realise the power of biotech, robotics, cybertechnology, and AI— and, still more, their potential in the coming decades— we can’t avoid anxieties about how this empowerment could be misused. The historical record reveals episodes when ‘civilisations’ have crumbled and even been extinguished. Our world is so interconnected it’s unlikely a catastrophe could hit any region without its consequences cascading globally. For the first time, we need to contemplate a collapse— societal or ecological— that would be a truly global setback to civilisation. The setback could be temporary. On the other hand, it could be so devastating (and could have entailed so much environmental or genetic degradation) that the survivors could never regenerate a civilisation at the present level.

#### Ends humanity

Kai **Kupferschmidt 18**. Contributing correspondent for Science magazine. 1-11-2018. "Could science destroy the world? These scholars want to save us from a modern-day Frankenstein." Science | AAAS. http://www.sciencemag.org/news/2018/01/could-science-destroy-world-these-scholars-want-save-us-modern-day-frankenstein

Church says a "crunch," in which a large part of the world population dies, is more likely than a complete wipe-out. "You don't have to turn the entire planet into atoms," he says. Disrupting electrical grids and other services on a huge scale or releasing a deadly pathogen could create chaos, topple governments, and send humanity into a downward spiral. "You end up with a medieval level of culture," Church says. "To me that is the end of humanity."

### Grid Impact---AT: Defense---AT: No Retal

#### Yes nuclear retal

Martin Rees 18. Astronomer Royal, founded the Centre for the Study of Existential Risk, Fellow of Trinity College and Emeritus Professor of Cosmology and Astrophysics at the University of Cambridge. 10/16/2018. On the Future: Prospects for Humanity. Princeton University Press.

Chapter 2 will address the twenty- first- century sciences— bio, cyber, and AI— and what they might portend. Their misuse looms as an increasing risk. The techniques and expertise for bio- or cyberattacks will be accessible to millions— they do not require large special- purpose facilities like nuclear weapons do. Cybersabotage efforts like ‘Stuxnet’ (which destroyed the centrifuges used in the Iranian nuclear weapons programme), and frequent hacking of financial institutions, have already bumped these concerns up the political agenda. A report from the Pentagon’s Science Board claimed that the impact of cyberattack (shutting down, for instance, the US electricity grid) could be catastrophic enough to justify a nuclear response.4

### Grid Impact---AT: Defense---CI Cascade

#### CI is interdependent---individual failures cascade

David Manheim 20, lead researcher at 1Day Sooner Inc., former contract researcher at the Future of Humanity Institute at Oxford University, “The Fragile World Hypothesis: Complexity, Fragility, and Systemic Existential Risk,” Futures, vol. 122, 09/01/2020, p. 102570

3. Fragility and Systemic Risk

As technologies develop, they often build on one another, so that the continued operation of the system depends on a growing set of other systems. The way that failure occurs and propagates in such systems is non-obvious, but it is largely dependent on the topology of the interdependence between components. Pastor-Satorras, Castellano, Van Mieghem, and Vespignani (2015) Simple dependencies, where a system requires the functioning of every component, can make the resulting system of systems more fragile than the components. A very basic model of this shows that given a system-of-systems with N components, each of which independently can fail at the rate Fi the failure rate is Text

Description automatically generated. While this grows more slowly than the sum of the individual failure rates as new systems are added, it is also far higher than the average failure rate of those individual systems.

As a concrete example, the peak of efficient farming once required family farms to depend on a family to manage the farm, a blacksmith to make horseshoes and plows, and draft animals to pull them. Losing any one of these would be enough to (eventually) make the system unable to continue, and there was some risk that this would occur. Still, the limited number of inputs and the substitutability of other inputs made such systems fairly stable - especially because many risks were uncorrelated across farms, and could often be addressed by borrowing from other farms nearby.

The farms of today, of course, are not nearly as simple. They require everything from satellite GPS systems to pinpoint locations, to the semiconductors and fabrication plants used to make specific integrated chips used in the farm equipment, to internet connectivity to run machine learning algorithms using collected data and satellite imagery on remote servers. Zubarev, Fomin, and Zubarev (2019) Modern agribusiness depends on everything from finding and hiring skilled laborers to manage complex machinery, to managing regulatory, financial, and other factors critical to farm operation. Kingwell (2011) These are often more tightly correlated across an economy, increasing risk. Beyond that, managing these farms requires understanding “human, technical, economic, financial, risk, institutional and social” issues, as Lewis et al. noted more than a decade ago. Lewis, Malcolm, and Steed (2006)

The risk is likely not yet critical, but it seems clear that dependence is growing, and the ability to use backup systems can be lost. For example, if remote servers become unavailable, local corn farms may lack the information needed to decide where to increase and decrease watering levels, or even lose the ability to run their computer-controlled irrigation systems. Similarly, decades ago supplies and ordering were managed on paper, and now, without the servers running Software-as-a-Service supply-chain-management software, the dairy farm down the road may not have access to an inventory of their supplies or know what amounts of products are needed or what they have historically ordered, and end up unable to feed their cows.

The inter-dependencies in such systems are more complex than the above model allows, but more complex analyses, such as those employing percolation analysis to understand mutual interdependency of multiple networks, Buldyrev, Parshani, Gerald Paul, Stanley, and Havlin (2010) show the same trend. That is, interdependent systems where failures can propagate can be far more likely to fail than the average rate at which the individual systems’ components fail. Worse, analysis of “high–value, technology– and engineering–intensive products or systems…used to produce consumer goods and services” has shown that the failure rates are nearly-additive, and worse, are hard to identify. Yeo and Ren (2009)

It should be noted that modern computer networks do not display such fragility, but this is a function of intentional design. Metcalfe and Boggs (1976) Simple network structures, such as lines or rings, are far more prone to failure Clark, Pogran, and Reed (1978). That is, unless a system was designed for resilience, resilience should not be expected. And when technological systems are made efficient and complex, they tend to be tightly coupled - meaning that failure in one place spreads Bookstaber (2007).

3.1. Inevitable Technological Fragility Hypothesis

The proposal of this paper, to provide an addendum to Bostrom's hypothesis, is that if technological development continues indefinitely, systemic fragility will increase to the point that the possibility of a shock sufficient for complete collapse approaches certainty.

This hypothesis rests on a number of assumptions, but there are also a variety of reasons to find it plausible and concerning. To lay these out clearly, we will first consider the question of how and why individual systems are fragile, then make an argument that it is at least plausible that the multiple interconnected systems and systems-of-systems which are necessary for much of modern civilization not only fail to address this risk, but multiply it.

4. Single-System Complexity and Fragility

The key question so far is whether fragility increases over time as systems are built. The answer to that question depends on a combination of factors that can push in either direction. These include increasing complexity of systems, the economic incentives for efficiency over robustness and the resulting levels of investment in resilience, the failure rates of individual components and systems, as well as the way in which systems-of-systems (and systems-of-systems-of-systems) are interrelated, and the extent to which systems and their interdependencies are designed to be robust.

Even the claim of inevitable fragility in individual systems makes several assumptions about how fragility increases. Before looking at the systemic question of how fragility could lead to collapse, we will outline these assumptions. Note that these are in fact assumptions, rather than claims - if any one of them is false in ways that are outlined, it would refute the hypothesis. The third assumption is particularly critical, and will be explored further in the next subsection.

First, for fragility to matter, the current trend of efficiency-increasing and resilience-decreasing technologies must continue to apply to at least one critical system, such as agriculture, communication, or transport. If this is wrong, and future white-ball / safe exploration technologies are ones that favor robustness over efficiency in all such critical domains, the trend would reverse. For instance, distributed fault tolerant computing arguably increases both efficiency and robustness. Most new technologies move in the opposite direction, but if enough resilience increasing technology is found, the balance could shift.

Second, the argument for increasing fragility assumes that economic growth continues to absorb human effort in a way that does not lead to overabundant resources. In Eric Drexler's ’Paretotopia‘ scenario, increased resources are unmatched by increased demand. Drexler (2019) In that future case, resources are abundant enough that robustness is easy to achieve. This second scenario also assumes the absence of supercharged competition that uses the newly abundant resources. This would not occur, for example, in Hanson's proposed default “Em” scenario, where human-based intelligences are simulated computationally, leading to a reduction rather than an increase in surplus that could be redirected to robustness for lack of other needs. Hanson (2016)

Third, it assumes that fragility is relatively hard to identify, such that at least some failures will be unanticipated. This has been true historically, but it is possible that future developments would reverse this trend, making the search for increased robustness itself efficient enough to counterbalance the more general and destabilizing increased fragility that new technology allows. If failures do become easy to anticipate, more expensive general resilience can be replaced with more specific redundancies targeted to the exact failure modes identified.

4.1. Non-Obvious Fragility

As mentioned, hard-to-identify fragility is a key assumption. Broadly speaking, non-obvious fragility is the result of planning for efficiency, instead of designing for redundancy, fault tolerance, or even provable safety. This is a fairly general fact about any control system. Paattilammi and Makila (2000) The concrete result of the current optimization shows clear signs of producing fragile results. One example is the proliferation of disposable technology, such as fragile smartphones designed to be replaced rather than fixed or upgraded. Failure of these optimized devices is normal, and while mitigating failure is important, it is often the case that risk must be accepted, rather than avoided. Perrow (2011) This type of fragility is obvious and anticipated, rather than non-obvious and worrying. For example, individual computers are fragile, and components fail frequently. For this reason, in high-reliability computer systems, a variety of mechanisms are in place to compensate, including redundant online systems for data storage, Chen, Lee, Gibson, Katz, and Patterson (1994) or methods to address other hardware failures. Wang, Zhang, and Xu (2017)

The fact that computer networks are not fragile, and the fragility that does exist is well understood, seems to be a counterexample. But the resilience itself is planned, in contrast to ecological systems where it is emergent - as we will discuss in detail below. This means that fault-tolerant designs are built to be tolerant of expected faults. Not only that, but resilience itself is optimized, for example, to minimize the number of backups or other costs needed to have a planned level of reliability. Rodrigues-da Silva and Crispim (2014) This creates fragility to unexpected faults, and allows the systems to operate through anticipated contingencies, but not to anything beyond that point.

4.2. Sociotechnical Resilience

Fragility of systems is not based purely on the lack of resilience of technical systems. In fact, fragility of optimized technical systems is compensated for by the greater robustness of sociological systems. The combined sociotechnical system, then, is the level at which fragility should be considered.

To reduce the fragility of sociotechnical systems, organizations can attempt to build more resilience at the organizational level. This can involve information sharing, distributed decision making, and better risk assessment. If done well, these attempts provide a sociotechnical system that compensates for technical and operation risk, but is again very different from emergent resilience. Langeland, Manheim, Mcleod, and Nacouzi (2016) Unfortunately, the interaction between humans and technology can often multiply risks, rather than mitigate them. Yeo and Ren (2009)

Another reason to think that sociotechnical resilience will not fully compensate for technological fragility is the reduced human involvement in technical systems. As automation increases, Danzig notes that humans are increasingly necessarily out-of-the-loop. Danzig (2018) He further argues that when there is competition, this dynamic is a necessary result of continued optimization.

To conclude the discussion of single-system fragility, we note that inevitable fragility of systems is not actually required for the hypothesis presented. As this section argued, it does seem plausible that in expectation, new technologies will be more fragile than those they replace. However, systemic risk can exist given the much weaker claim that specific critical systems are relied upon, and technological improvements relevant to those systems alone exhibit sufficient fragility to cause a cascading collapse. Before discussing the interaction between systems, however, it is worth considering how these human, technical, or sociotechnical systems differ from naturally resilient biological systems.

### Grid Impact---AT: Defense---Kills Millions

#### Especially from cyberattacks---best case kills millions because of failure cascades.

William Arthur **Conklin &** Anne **Kohnke 18**. Conklin is at the College of Technology, Houston; Kohnke is at the College of Management, Lawrence Technological University. 03/09/2018. “Cyber Resilience: An Essential New Paradigm for Ensuring National Survival.” Proceedings of the 13th International Conference on Cyber Warfare and Security: National Defense University Washington DC, USA.

Cyberspace is full of adversaries with potential actors ranging from state-sponsored groups to criminal enterprises, to anyone with an Internet connection who wishes to do harm. Cyberattacks on the various elements of the U.S. critical infrastructure occur on a daily basis. For instance, the Industrial Control Systems- Computer Emergency Response Team (ICS-CERT) reports that U.S. industrial control systems were attacked at least 245 times over a 12-month period (OAS, 2015). "While China, the U.S. and Russia lead the world in cyberattacks, virtually every government engages in such attacks, and nearly every country has its share of computer hackers" (Wagner, 2017). The ability to launch a successful cyber-attack makes every nation- state, into a potential super power (Wagner, 2017). Perhaps the most egregious example comes from the Ukraine. In December 2015, a presumed Russian cyberattacker successfully seized control of the Prykarpattyaoblenergo Control Center (PCC) in the Ivano-Frankivsk region of Western Ukraine (Wagner, 2017). This attack marked the first time that a concerted cyber-attack was successfully launched against a nation's power grid (Wagner, 2017). However Stuxnet, in 2010, might be the first instance of a nation enforcing policy through other means (Howard & Parot, 1976). The perpetrators of the Ukrainian attack were observed conducting similar exploits against the U.S. energy sector (Brasso, 2016). Although there was never any actual disruption, many experts believe that those activities were a probe for future moves on the U.S. infrastructure (Brasso, 2016). One key question is, "Could a catastrophic cyberattack in the United States Infrastructure ever occur? The National Security Agency's former Director, Mike Rodgers, made his own evaluation of the possibility of a successful attack against critical infrastructure when he said; "It's a matter of, when, not if' (Smith, 2014). Power grids are the most frequently mentioned target (Wagner,2016; Brasso, 2016; Smith, 2014) due to the interconnectedness of power grids which opens them up to "cascading failures". As nearby grids take up the slack for a failed grid system, they overload and fail themselves, causing a chain reaction. Rogers says that such attacks are part of "coming trends" in which so-called zero-day vulnerabilities in U.S. cyber systems are exploited (Smith, 2014). The reason why the protection of our national infrastructure is so critically important is that a major exploit, like a successful cyberattack on the electrical grid could leave the U.S. cloaked in darkness, unable to communicate and without any form of twenty-first century transport. It would likely kill many thousands of citizens, perhaps millions either through civil unrest, failure of public systems, or mass starvation (Brasso, 2016; Maynor, 2006). Many experts believe that the cyberwar began in 2003 (Wagner, 2017) when the Northeast (U.S.) blackout occurred. That blackout caused 11 deaths and an estimated $6 billion in economic damages (Wagner, 2017). After the attack, SCADA attacks occurred in the UK, Italy and Malta, among others. According to Dell's 2015 Annual Security Report, cyber-attacks against infrastructure systems doubled in 2014 to more than 160,000. (Wagner, 2017) Infrastructure systems are diverse and coupled with the criticality of the sensors and controllers that comprise a typical infrastructure system, make them tempting targets for attack. Therefore, there have been long-standing concerns about the overall digital infrastructure being vulnerable to cyberwarfare and cyberterrorism attacks (Eisenhauer, 2006, Nat-Geo, 2017). Notwithstanding the disastrous nature of cyberattacks on digital targets, none of the industries in our current national infrastructure have developed coherent plans, or effective strategies, to protect themselves (Brasso, 2016). This has caused an increasing interest in a coherent model for defending the critical infrastructure against cyberattack (Symantec, 2014; E-Y, 2014).

### Grid Impact---AT: Alt Cause---EMP

#### No EMP alt cause

Jeffrey Lewis 13, Director of the East Asia Nonproliferation Program for the James Martin Center for Nonproliferation Studies at the Middlebury Institute of International Studies at Monterey, “The EMPire Strikes Back”, Foreign Policy, 5/24/2013, https://foreignpolicy.com/2013/05/24/the-empire-strikes-back/

Jim Woolsey, a former director of central intelligence and noted Oklahoma City conspiracy theorist, and Peter Pry had an op-ed in the Wall Street Journal on Tuesday warning that North Korea might attack United States with a nuclear weapon. But instead of vaporizing Washington, Woolsey and Pry warn that North Korea would use just one bomb to create a massive electromagnetic pulse (EMP) that would fry our iPhones and end "modern civilization."

It will be like The Hunger Games meets Red Dawn!

If you aren’t familiar with the crowd of cranks and threat inflators banging the EMP drum, this scenario might seem a little far-fetched. It does seem like the sort of overcomplicated plot dreamed up by a Bond villain, one that only works in the movies. Bad movies.

Well, bad movies and terrible books — like Newt Gingrich and William Forstchen’s potboiler One Second After, about life in the United States after an EMP attack. Yes, that’s right. Newt Gingrich wrote dime-store pulp fiction about the aftermath of an EMP attack. I am just going to give you a minute here to compose yourself.

All better? Okay, as I said, Newt Gingrich wrote a book about EMP. EMP advocates get a little cranky when you make fun of it. An indignant Peter Pry once responded to mockery of the book by comparing One Second After to Uncle Tom’s Cabin. Really.

That’s because the EMP crowd is about raising "awareness." The Heritage Foundation even promotes "EMP Awareness Day." And Congress empanelled a Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack in 2001 (and reauthorized it in 2006) and even has an "EMP Caucus." No, I don’t know if they wear little tinfoil hats at their caucus meetings. Why would you ask something like that?

The possibility of an electromagnetic pulse wiping out Western civilization — or at least our local varietal — is a hardy perennial of a particular worldview espoused by types like the John Birch Society. EMP "awareness" basically occupies the space vacated by activism in the 1950s for civil defense. For a flavor of the old civil defense paranoia, I recommend a slim volume from 1968 entitled "Who Speaks for Civil Defense?" — particularly a chapter by the late Steuart Pittman that perfectly captures the paranoia of the movement.

Sharon Weinberger, author of the excellent Imaginary Weapons, has already written a readable account of the craziness of this view in these very electronic pages ("The Boogeyman Bomb"), which elicited a letter from Pry that took itself very, very seriously. The humorlessness of the EMP movement is not surprising. This is about scaring people. Any mirth is entirely unintentional.

For such a dry, serious subject, the amount of actual data on the threat from electromagnetic pulse attack is pretty thin. Electromagnetic pulse is, of course, a real phenomenon produced by a nuclear explosion. The EMP Commission likes to point to its "years" of research based on "decades" of data on the effects of nuclear weapons. But at the end of the day, even if we understand the physics of electromagnetism, there is no credible way to model the mass effect of a pulse on a complex system like our power grid or our communications infrastructure.

The United States and the Soviet Union did engage in high-altitude nuclear testing before realizing this might not be the greatest idea, eventually banning tests in the atmosphere and outer space. The most famous event was called Starfish Prime — a 1.4 megaton nuclear explosion conducted by the United States in the Pacific in July 1962. By contrast, North Korea’s 2013 nuclear test — its largest and most successful — was on the order of 10 kilotons, or more than a hundred-times smaller.

EMP threat-mongers sometimes dramatically exaggerate the effects of Starfish Prime. For example, Lowell Wood, later a member of the EMP Commission, described the impact of Starfish Prime to Congress in plainly apocalyptic terms. Starfish Prime, he said, "very unexpectedly turned off the lights over a few million square miles in the mid-Pacific. This EMP also shut down radio stations, turned off cars, burned out telephone systems, and wreaked other mischief throughout the Hawaiian Islands, nearly 1,000 miles distant from ground zero."

All of which was terrible — or would have been, had it happened. It did not.

Starfish Prime was bad, but it was not nearly so dramatic as Wood claimed. In fact, lots of people turned out to watch the explosion from hotels and beaches in Hawaii, including reporters sent to cover it.

Take a gander at the coverage in Life Magazine, which has some really beautiful images of the event. My favorite account comes from Dick Stolley. He’s famous, by the way. He would later buy the Zapruder film. Stolley reported on Starfish Prime from the beach at Waikiki:

There were coeds in muumuus, college boys in swimsuits, tourists in newly purchased resort wear, sleepy kids…. [The blast was] white and hot, like the flash of a breaking electrical circuit. It turned almost instantly to a bright bilious green, a color so unexpected that watchers gasped.

Tough assignment, huh? Life doesn’t mention what Stolley did next, but given his fond recollection of the drinks cart after putting an issue of Life to bed, I like to think he slipped back to the Royal Hawaiian for a Mai Tai and to interview any coeds in muumuus who happened to be around.

Now, as I say, Starfish Prime did do some damage, even if Waikiki’s luau schedule was uninterrupted. The electromagnetic pulse and other effects probably killed off two or three satellites in orbit, which was bad enough. The explosion may also have damaged some telephone equipment, but there were no telephone outages. (Military communications and test instrumentation all worked fine.) Some street lights on Ferdinand Street in Manoa and Kawainui Street in Kailua also went out. Of course, street lights and telephone systems experience everyday failures, too. You’d be surprised at how hard it is to demonstrate that street light failures are the result of an electromagnetic pulse rather than, say, faulty fuses. (Apparently, the answer turns on fascinating questions like "How many clear plastic washers were in transformer cutouts that failed?") Contemporary reports mention continuous radio coverage of the event with no outages.

So let’s be clear: Starfish Prime did not “turn off the lights over a few million square miles in the mid-Pacific." It did not shut down any radio stations or cars or burn out the telephone system. The biggest problem that Dick Stolley and other reporters had filing their stories the next day was probably a hangover.

Even if we understand how an electromagnetic pulse works and have data about the vulnerability of equipment, a modern system like a power grid or communications network presents just too complex a set of resiliencies and vulnerabilities.

The solution of the EMP Commission was simply to collect more data, essentially creating laundry lists of things that might go wrong. For example, the EMP Commission exposed 37 cars and 18 trucks to EMP effects in a laboratory environment. While EMP advocates claim the results of an EMP attack would be "planes falling from the sky, cars stalling on the roadways, electrical networks failing, food rotting," the actual results were much more modest. Of the 55 vehicles exposed to EMP, six at the highest levels of exposure needed to be restarted. A few more showed "nuisance" damage to electronics, such as blinking dashboard displays.

This kind of experiment is better than nothing, of course, but it doesn’t model the effect of an EMP event on urban transportation networks. Would the result be massive pile-ups on expressways? Carmaggedon? Friday afternoon on the Beltway? The experiment raises as many questions as it answers, including, "How did they get enough money to purchase 55 vehicles?" I can’t help but wonder if they just rented them one by one. "How was your car, Mr. Graham?" "Oh, yeah, uh, the dash display is blinking." "We’re sorry to hear that, we hope it wasn’t an inconvenience." "What? Oh, well, never mind. All’s well that end’s well, that’s what I say."

The bottom line is that there simply isn’t enough evidence to support the wild claim that a single nuclear weapon, or even a few, detonated at high altitudes would pose an "existential threat" to "modern civilization," as Woolsey and Pry claim. It would be a nuisance, but preferable to having the bomb detonate in a major city.

### Grid Impact---Vulnerable Now---2AC

#### Vulnerability AND motive are real---but even if not, threat magnitude justifies prevention.

John J. **Klein 18**. Senior Fellow at Falcon Research in Northern Virginia. Spring/2018. “Deterring and Dissuading Cyberterrorism.” Air & Space Power Journal: Afrique et Francophonie, vol. 9, no. 1, pp. 21–34.

Security experts have argued for some time that the energy sector has become a potential target for cyber attack through the creation of Internet links—both physical and wireless—that interfere with the supervisory control and data acquisition (SCADA) systems used by electrical and power distribution networks.16 SCADA systems manage the flow of electricity and natural gas, while also being used to control the industrial systems and facilities used by chemical processing plants, water purification and water delivery operations, wastewater management facilities, and a host of manufacturing firms.17 Studies have indicated that critical infrastructures that include SCADA systems may be vulnerable to a cyberterrorist attack because the infrastructure and the computer systems used are highly complex, making it effectively impossible to eliminate all potential weaknesses.18 It is believed by many security professionals that a terrorist’s ability to control, disrupt, or alter the command and monitoring functions performed by SCADA systems could threaten regional or national security.19 Cyberterrorism, when considered generally, may be conducted by either state or non-state actors, but the calculus and implications can be quite different for each category. Of note, the U.S. Department of State lists three designated state sponsors of terrorism in 2015: Iran, Sudan, and Syria.20 State sponsored cyberterrorism would most likely be conducted to achieve the goals as defined by the state’s political leadership and any actions would tend to support long-term national security goals. Even though the cyber domain offers a bit of anonymity, if a cyber attack is traced back to its network source or Internet address, then the physical location of those perpetrating the attack could be determined within the boundaries of the state authorizing the cyber attack. Because states have geographic boundaries and the initiating computer networks potentially have a physical location, there is increased likelihood, when compared to non-state actors, that those responsible for initiating a state-sponsored cyber attack would be identified. In contrast, non-state actors—to include many terrorist organizations—do not necessarily act uniformly or according to the same underlying beliefs, and many of the most aggressive organizations are motivated by an ideology that embraces martyrdom and an apocalyptic vision.21 This ideology may be based on religion or a desire to overthrow a government. Terrorists who are motivated by ideology and intend to conduct cyber attacks against the United States or its interests may not care about the repercussions following an act of cyberterrorism, whether military in scope or not. In such a scenario, some strategists think a terrorist organization’s leadership may prove undeterrable by traditional military means.22 Despite the disparate motivators of terrorists, many terrorist organizations, to include al-Qaida and the self-proclaimed Islamic State, are said by some security experts to function strategically and rationally.23 Because a terrorist organization’s leadership may be inclined to make rational decisions, deterrence may at times be a suitable method of influencing future actions. Consequently, deterrence should be considered a critical element in a successful national strategy to prevent cyberterrorism. The Advantages of Cyberterrorism There are several advantages to using the cyber domain to conduct acts of terrorism. First, cyberterrorism can be far less expensive than traditional terrorist methods.24 Potentially, all that is needed is a personal computer and an Internet connection, instead of needing to buy weapons, like guns or explosives, or acquire transportation.25 Second, cyberterrorism has the potential for being more anonymous than traditional, kinetic methods.26 It can be difficult for security and police agencies to track down the identity of terrorists when they use online “screen names” or are an unidentified “guest user.”27 Third, the number of potential targets is enormous when compared to the number of targets typically used in kinetic actions.The cyberterrorist could target the computer networks of governments, individuals, public utilities, private airlines, SCADA systems, and other critical networks. The sheer number of potential cyber targets is thought to increase the likelihood that an adversary can find a weakness or vulnerability in one of the different networks to exploit. Finally, cyberterrorism can be conducted remotely, a feature that may be especially appealing to some would-be attackers. Exaggerated Threat? Many critics have noted, however, that while the potential threat of cyberterrorism is alarming and despite all the dire predictions of impending attack, no single instance of real cyberterrorism has been recorded.28 To date, there has been no recorded instance of cyberterrorism on U.S. public facilities, transportation systems, nuclear power plants, power grids, or other key components of the national infrastructure. While cyber attacks on critical components of the national infrastructure are not uncommon, such attacks have not been conducted in a manner to cause the kind of damage or severity of effects that would qualify as cyberterrorism.29 The 2007 widespread denial of service cyber attack in Estonia, which brought down the banking system for three weeks, did not cause catastrophic damage, injury, or death.30 Even in the case of the Stuxnet malware, discovered in June 2010 and called “world’s first digital weapon” because of its capability of causing physical destruction to computers and other equipment, did not cause widespread, severe destructive effects.31 This begs the question: Just how real is the cyberterrorism threat? While cyberterrorism may be an attractive option for modern terrorists who value its remote access, anonymity, potential to inflict massive damage, and psychological impact, some critics say that cyber fears have been exaggerated.32 Furthermore, there is disagreement among some cyber experts about whether critical infrastructure computers, to include SCADA systems, offer an effective target for furthering terrorists’ goals.33 Many computer security experts do not believe that it is possible to use the Internet to inflict damage, injury, or death on a large scale.34 Some of these experts note that critical computer systems are resilient to attack through the investments of time, money, and expertise during the design and development of these critical systems. For example, the U.S. Department of Defense, Central Intelligence Agency, and Federal Bureau of Investigation are reported to protect their most critical systems by isolating —also called air-gapping—them from the Internet and other internal computer networks.35 Despite the ongoing debate about whether the cyberterrorism threat is exaggerated or if the potential destructive effects can be sufficiently achieved to warrant concern, both the news media and government reporting indicate that some terrorist organizations now use the Internet to communicate, recruit people, raise funds, and coordinate future attacks.36 Even though there is no publically available information that terrorist organizations have directly and successfully attacked Internet servers or major computer networks, reporting does suggest that many terrorist organizations would employ cyber means to achieve their goals if the opportunity presented itself.37 Because there appears to be a persistent desire by some terrorist organizations to use any and all means, including cyber attacks, to achieve their desired goals, it is paramount for policy makers and military planners to take preparatory actions to prevent such acts and mitigate any effects should such an attack occur. These preparatory actions include deterrence efforts.

### Grid Impact---Vulnerable Now---1AR

#### Multiple weak points now

**Maglaras et al. 18**. School of Computer Science and Informatics, De Montfort University. 03/01/2018. “Cyber Security of Critical Infrastructures.” ICT Express, vol. 4, no. 1, pp. 42–45.

4. Real-world attacks Among others, the STUXNET worm infection [17] perfectly represents the frailty of the regulatory systems devoted to control critical infrastructures. First isolated in mid-June 2010, STUXNET was a computer virus specifically designed for attacking Windows based industrial computers and taking control of Programmable Logic Controller (PLCs), influencing the behaviour of remote actuators and leading to instability phenomena or even worse. The paradox is that critical infrastructures massively rely on newest interconnected (and vulnerable) Information and Communication Technology (ICT) technologies, while the control equipment is typically old, legacy software/hardware. Such a combination of factors may lead to very dangerous situations, exposing the systems to a wide variety of attacks. The lesson the CIIP (Critical Information Infrastructure Protection) community has learned from the spread of the STUXNET worm is that, in order to effectively react to a specific low level menace, there is the need to consider both the global and local perspectives. In fact, besides obtaining a wider perspective on the state of the System of Systems, there is the need to increase the intelligence of equipments and devices that are used to influence the behaviour of the system, such as RTUs, valves, etc. Moreover, as emphasised by several episodes [18], another effective way to paralyse a SCADA system via cyber attack is to saturate the bandwidth of the carrier used for the communication (this was, for example, the way in which the SLAMMER worm operated in 2003 to affect the SCADA of two United States (US) utilities and a nuclear power plant). Indeed, as emphasised also by the ANSI/ISA.99 (American National Standards Institute/International Society of Automation), availability is the most crucial attribute of information security. The lack of timely information to/from the field may cause dramatic consequences because the field is unable to receive the adequate command, hence even trivial episodes may provoke dramatic impact, as shown by the US black-out. In an evaluation of the Mariposa botnet infection in an ICS organisation, the US Department of Homeland Security [19] explained that they found that the infection occurred when an employee used a USB drive to download presentation materials to a corporate laptop. When the user connected the laptop to the corporate network upon returning to work, the virus spread to over 100 hosts. The security of SCADA communications is becoming more complicated because the decision has been taken to link the SCADA networks with IT networks to allow better and faster communications. But these new features have increased the threats and risks on SCADA communications. There are presently no convinced solutions to enforce the security of SCADA communications in that perspective. The idea to add intelligence to the field is not new; electro-valves for gas pipelines are available on the market that, in the case they receive a rapid sequence of open-close commands, do not perform them in order to avoid the consequence of the mechanical shock. A number of EU (European Union) projects such as the FP6 SAFEGUARD and FP7 CRUTIAL (CRitical UTility InfrastructurAL Resilience) have explored the technical feasibility to improve cyber security of SCADA system by improving the smartness of the field devices. 5. Discussion Further complication arises because it is known that a large percentage of attacks are induced by inside attackers. Thus perimeter defense alone cannot defend the system. In such cases, the question that one is confronted with is whether there is enough indication of an ongoing attack in the dynamics of the system itself [20]. Despite this range of activities, it has been proven that half of these have human error at their core [21]. Therefore, there should be increased empirical and theoretical research in to human aspects of cyber security based on the volumes of human error related incidents in order to establish ways in which mainstream cyber security practice can benefit. Security measures tend to neglect that persistent attackers will eventually gain access whatever that perimeter protection may be. One main objective from modern security solutions would be to develop novel methods that could detect and disturb the activities of the attackers once they have gained access inside the system. Special care should be given to the implementation of new strategies that can detect, prevent and mitigate data exfiltration attacks, since intrusion detection/prevention strategies are now deemed to be inadequate for data protection [22]. In order to strengthen the security of SCADA systems, one solution is to deliver defence in depth [23] by layering security controls so as to reduce the risk to the assets being protected. By applying multiple controls on top of the information asset (in this case the SCADA and ICS configuration and management data) the architect introduces further barriers, which a threat actor has to overcome. For the more competent threat actors this will slow them down. Within the time it takes to get through some of the controls, the protective monitoring service should have alerted someone to the attack, which will allow further action to be taken (such as dropping the threat actors connection). Defence in depth ensures there is no single point of failure from threats to assets by providing differing barriers (controls) in a layered approach. 6. Conclusions The synergy between the ICS and the IoT has emerged largely bringing new security challenges. We have identified key security issues for ICS and current solutions. Future work should primarily focus on the balance between holistic approaches that can deal with a wide variety of attacks, real time identification of intruders with high accuracy and solutions that impose low overhead to the communication and performance of SCADA/ICS systems.

#### Empirics prove---despite countermeasures

Julia E. **Sullivan &** Dmitriy **Kamensky 17**. Sullivan is a U.S. attorney based in Annapolis, Maryland, who advises energy companies, investors, and public institutions in connection with market formation, risk management, mergers and acquisitions, and regulatory compliance, Visiting Professor at Berdyansk State Pedagogical University; Kamensky is a Professor of Law at Berdyansk State Pedagogical University. 04/2017. “How Cyber-Attacks in Ukraine Show the Vulnerability of the U.S. Power Grid.” The Electricity Journal, vol. 30, no. 3, pp. 30–35.

Critical infrastructure owners and operators “continue to experience increasingly sophisticated cyber intrusions, which provide malicious actors the ability to disrupt the delivery of essential services, cause physical damage to critical infrastructure assets, and potentially produce severe cascading effects.” 28 According to one estimate, between 2000 and 2015, there were 15 suspected cyber-attacks or events against the U.S. electricity grid.29 Reported cybersecurity incursions into industrial control systems (ICS) within the U.S./Canadian energy sector have decreased slightly in the past two years (see Table 1), despite an overall increase in the number of reported ICS incidents across the broader economy. So far, these incursions have been unsuccessful at inhibiting or disrupting power system operations, but the continued rollout of smart grid technologies makes us increasingly vulnerable.30 Public and private resources have been hard at work for many years to identify critical energy infrastructure and implement robust action plans to prevent, detect, respond to, and mitigate the potential effects of malicious cyber-attacks. The U.S. bulk power system has been subject to mandatory and enforceable cybersecurity standards since 2008.31 These standards are continuously updated, most recently in 2016.32 Critical assets such as control centers, transmission substations, and generators must receive a full panoply of protections, including cyber protections, physical protections, cyber and physical access limitations, security training for appropriate personnel, and the development and implementation of incident response and asset recovery plans. Violations are punishable by civil penalties of more than $1,000,000 per violation per day.33 And yet a recent simulation by Lloyds and the University of Cambridge's Centre for Risk Studies, called Business Blackout, found that an extreme event, while unlikely, remained plausible.34 Business Blackout simulated a fictionalized scenario that was designed by subject matter experts and subjected to peer review “to ensure that the effects could plausibly be achieved.” The simulation assumed that the U.S. was targeted by a significantteam of personnel with a high level of skill who spent many months on careful research, preparation, and operational implementation.35 In the Project Blackout scenario, intruders planted malicious code that took control of 50 generators and caused them to overload or even catch fire. As a result, 15 U.S. states were plunged into darkness, leaving 93 million people without power. The scenario showed a rise in mortality rates as health and safety systems failed, a decline in trade as ports shut down, disruption to water supplies as electric pumps failed, and chaos to transport networks as infrastructure collapsed. The estimated impact to the U.S. economy ranged from $243 billion to more than $1 trillion.36 The Business Blackout researchers found that this scenario, “while improbable, is technologically possible.” 37

#### Consensus

Emily O. **Goldman &** Michael **Warner 17**. Goldman is the senior adviser to the commander, US Cyber Command, and the director, National Security Agency; Warner is the command historian of US Cyber Command and an adjunct faculty member at American University and Johns Hopkins University. 10-16-17. “Why a Digital Pearl Harbor Makes Sense . . . and Is Possible.” Carnegie Endowment for International Peace. <https://carnegieendowment.org/2017/10/16/why-digital-pearl-harbor-makes-sense-.-.-.-and-is-possible-pub-73405>

US adversaries have also shown an increasing capability and intent to target its industrial control systems recently. Since 2011 known or suspected hackers in several countries have run supervisory control and data acquisition (SCADA) exploitation attempts against US critical infrastructure. In September 2015 in testimony before the House Permanent Select Committee on Intelligence, Director of National Intelligence James Clapper revealed that unknown Russian cyber actors had compromised the supply chains of at least three industrial control system vendors. He warned, “Politically motivated cyber-attacks are now a growing reality, and foreign actors are reconnoitering and developing access to U.S. critical infrastructure systems.”6 Cyberspace threats also headlined Clapper’s February 2016 testimony to the Senate Select Committee on Intelligence on worldwide threats. In subsequent hearings before the House Armed Services Subcommittee on Emerging Threats and Capabilities in March 2016, Adm. Mike Rogers, commander of US Cyber Command and director of the National Security Agency (NSA), testified that “industrial control systems and SCADA probably is the next big area for us because we’ve got to transition from a focus purely on the network structure.”7 He noted that the Department of Defense (DOD) has already begun looking at data concentrations and focusing more on industrial control systems and SCADA. Rob Joyce, chief of the NSA’s Tailored Access Operations unit, complains that SCADA security keeps him up at night. Joyce understands how to exploit such systems;8 he also appreciates how vulnerable the United States is, in turn, and that the “Internet of things” will multiply those vulnerabilities exponentially.9 Supply chain vulnerability, another dimension of the problem, was raised during Admiral Rogers’s hearings before the Senate Armed Services Committee in April 2016. Specific processes exist in the US government to address these issues for some components of DOD infrastructure, particularly nuclear systems, but not for other major systems or components. The DOD’s focus on network security is now expanding to focus on the risks to individual combat platforms, weapons systems, and individual data concentrations. In the National Defense Authorization Act of 2016, Congress directed the secretary of defense to complete an evaluation of the cyber vulnerabilities of every major weapons system by December 2019.

#### Ukraine proves

Emily O. **Goldman &** Michael **Warner 17**. Goldman is the senior adviser to the commander, US Cyber Command, and the director, National Security Agency; Warner is the command historian of US Cyber Command and an adjunct faculty member at American University and Johns Hopkins University. 10-16-17. “Why a Digital Pearl Harbor Makes Sense . . . and Is Possible.” Carnegie Endowment for International Peace. <https://carnegieendowment.org/2017/10/16/why-digital-pearl-harbor-makes-sense-.-.-.-and-is-possible-pub-73405>

The December 2015 events in Ukraine, where multiple electric companies were hacked—the first power outage known to be caused by a cyber attack—should serve as a wake-up call. Hackers used malware to gain access to the Ukrainian utilities’ business networks and, from there, maneuvered to their production networks and on to operator stations. The hackers then remotely disconnected the breakers of thirty substations. According to Robert M. Lee of Dragos Security, “Every bit of this is doable in the U.S. grid.” Although the US grid is more hardened than Ukraine’s, the former’s recovery would be more difficult because if the SCADA systems are lost, the fully automated US systems cannot switch to manual control as the Ukrainians’ system did.11

### Grid Impact---Vunlerable Now---AT: Airgapping

#### Airgapping doesn’t solve.

Davidson et al. 18. University of South Alabama. 03/09/2018. “On SCADA PLC and Fieldbus Cyber-Security.” Proceedings of the 13th International Conference on Cyber Warfare and Security: National Defense University Washington DC, USA.

Air gapped systems attempt to achieve security by completely segmenting networks and disallowing any connections to external networks. This generally required any data access to be performed from within a secure facility with physical security assets in place. Stuxnet (Failliere, Murchu and Chien 2011) has shown us that even facilities such as these can be compromised through the introduction of unauthorized code walked in on USB sticks and/or disgruntled employees/contractors with direct network access. Once the network has been breached, an attack on the PLC's and the local fieldbus network become possible. However, physical separation of disparate networks may make an attack more difficult to execute in that some sort of physical presence is required. Many control systems that purport to have physical network separation do so only in a virtual manner. Firewalls, virtual local area networks (VLAN), virtual private networks (VPN), demilitarized zones (DMZ), and other tools are used to logically segment networks such that, theoretically, networks are effectively, if not literally, airgapped (Knapp 2011; Stouffer, Pillitteri, Lightman et al. 2015). This allows for convenience in that authorized communications can be allowed without requiring a physical presence. This requires that all software and hardware systems be correctly setup and kept current which is often a complex and time-consuming task. Errors may create vulnerabilities that could be exploited. The more complex the software and configuration, the more room for error.

### Grid Impact---Vulnerable Now---AT: Encryption

#### Not encrypted

Davidson et al. 18. University of South Alabama. 03/09/2018. “On SCADA PLC and Fieldbus Cyber-Security.” Proceedings of the 13th International Conference on Cyber Warfare and Security: National Defense University Washington DC, USA.

As shown, If the control center can be breeched and access gained to the network, then the lack of security features in many common fieldbus protocols may be exploited. These protocols often lack even simple password capabilities and those that do, often transmit in clear text. Encryption is not common. It is not unusual for ОТ staff to use shared passwords or for device vendors to have hard-coded passwords into their products (Krutz 2005;Knapp 2011). Strong security policies that are enforced can help to mitigate some of the risk, but an unsecure protocol remains unsecure. Rush, Kinast, and Shaw (Rush 2006) with the American Gas Association (AGA) noted that encryption is uncommon in many control system protocols and championed the development of a device to sit on each end of the communications path between the control center and a remote PLC/RTU. This device would encrypt/decrypt network traffic between the endpoints thus providing secure communications of even unsecure protocols. Though this device was designed over ten years ago, it has not been heavily deployed.

### Grid Impact---Vulnerable Now---AT: Microgrids

#### Not coming AND don’t solve

Julia E. Sullivan & Dmitriy Kamensky 17. Sullivan is a U.S. attorney based in Annapolis, Maryland, who advises energy companies, investors, and public institutions in connection with market formation, risk management, mergers and acquisitions, and regulatory compliance, Visiting Professor at Berdyansk State Pedagogical University; Kamensky is a Professor of Law at Berdyansk State Pedagogical University. 04/2017. “How Cyber-Attacks in Ukraine Show the Vulnerability of the U.S. Power Grid.” The Electricity Journal, vol. 30, no. 3, pp. 30–35.

Some industry analysts predict enormous growth of microgrids in the next five years, but technical, economic, and regulatory barriers remain. Technical barriers. Most distributed energy resources as currently installed are incapable of providing backup power during a grid outage, because they weren’t designed with resiliency in mind. For a distributed energy resource to provide electricity during a grid outage, it must be designed to function as a standalone system that can isolate itself from the grid and continue power production in island mode. For safety reasons, current operating standards require that grid-connected resources automatically disconnect from the grid during a power outage. Most of these systems are currently designed to cease power production once they disconnect from the grid, leaving customers in the dark.61 Thus, for example, the majority of New Jersey's distributed energy resource systems, including solar, combined heat and power, fuel cells, and other renewables, did not operate during or after Superstorm Sandy when the distribution grid went down.62 In order to provide resilience and security of supply benefits to consumers, these systems need to be designed – and in some cases reconfigured – so that they can operate in island mode when they are disconnected from the grid. Economic barriers. Microgrids are cost-prohibitive for many customers, particularly in the residential sector. Federally funded research63 and tax incentives64 have been essential in making distributed solar PV technology available to an increasing number of Americans. However, there is real concern that these federal programs may be reduced or even eliminated as part of President Trump's announced intention to cut spending on initiatives linked to climate change. In the current political environment, it may become increasingly important to focus the debate on alternative justifications for decentralized power resources, such as resilience and security of supply. Regulatory barriers. Regulatory barriers complicate and even prohibit the deployment of microgrids in some areas. Microgrids typically require the use of existing power distribution lines or the construction of new power lines within a defined zone, which may infringe on traditional utility franchise rights. Microgrid operation may involve the exchange of power between parties or the distribution of power across streets or public areas, which could make operators subject to comprehensive public utility regulation. The lack of clarity regarding interconnection rules and who pays for necessary equipment and network upgrades is another major barrier. New financing models are also needed to overcome the barrier of high upfront costs and make microgrids more accessible to a broader number of customers.65

### Grid Impact---Vulnerable Now---AT: Repairs

#### Can’t be rebuilt due to weak supply chains

Justin Van Dunk 20, Liberty University, “The Threat of Terrorism to Power Grids: Effects of Electromagnetic Pulses to the United States,” Liberty University Journal of Statesmanship & Public Policy, vol. 1, no. 1, 07/25/2020, https://digitalcommons.liberty.edu/jspp/vol1/iss1/7

Transformers

Transformers and their substations are the backbone of the United States’ electrical grid. The purpose of a transformer is to convert electricity into higher or lower voltages rendering the electricity usable for everyday life.29 This vital component of society is not immune to the consequences of a successful EMP strike against the United States. The Federal Energy Regulatory Commission (FERC) holds that there are 30 high voltage transformers throughout the United States. These transformers are weak links throughout the entire system. If an EMP were able to successfully target only nine of these transformers, a coast-to-coast blackout throughout the contingent United States could happen.30 While the destruction of transformers would be devastating, replacing these transformers would prove to be even more costly. Overseas manufacturers account for 85% of the United States’ transformer inventory.31 Manufacturing and shipping of these custom-built transformers would take approximately 12 to 18 months.32 In addition, shipment and installation of these transformers within the United States would take several months’ time.33

#### Repairs take forever.

Bill White 15. 3-17-2015, "6 Ways The Power Grid Could Collapse," Survivopedia. http://www.survivopedia.com/the-power-grid-could-collapse/

Of all our infrastructure, the electrical power grid is the most fragile. In the 2013 Infrastructure Report Card, prepared by the American Society of Civil Engineers, Energy received a grade of D. The only reason it was that high, was that the energy category includes all classes of energy, not just electrical energy. However, in the narrative, the ASCE described the true condition of the electrical grid, declaring that it needed over one trillion dollars of investment to survive the next ten years. The problem is that our electrical grid, like much of our infrastructure, was designed for a 50 year lifespan. If you look at the average age of our power plants and distribution network, it’s clear that way too much of it is over well over the halfway point in its lifespan. In fact, there is a considerable amount of it that is still in use, even though it is past its programmed life. It doesn’t take much to leave us without electrical power. A good snowstorm or thunderstorm will knock down power lines, leaving people without electrical power. Larger storms, like hurricanes can do enough damage to the electrical grid to leave people without electrical power for weeks. However, that’s a little misleading. The only reason that the damage to the grid is fixed so rapidly in cases like a hurricane is that that [because] power companies send in teams from outside the area to help with repairs. If there was a nationwide event that caused the loss of electrical power, it would take much longer to repair the damage; both due to a lack of crews and a lack of necessary equipment. When we talk about the grid, we are actually talking about three independent, but interconnected grids. There is an eastern grid, a western grid and the Texas grid. So, taking the grid down actually requires taking three separate grids. {adinserter emp}Destruction of the grid, regardless of whether it is by intent or by accident is actually not all that hard to accomplish. The entire grid is interconnected and to some extent automated. When one part of the grid becomes overloaded by demand or by loss of power production capability, it automatically compensates, bringing in resources from farther away to provide the needed power. Were that to happen enough times, the whole system would become overloaded.

### Grid Impact---Vulnerable Now---AT: Resilient

#### Supply/demand mismatches collapse the grid in seconds.

Steven Ferrey 14. Professor of Law at Suffolk University Law School and served as a Visiting Professor of Law at Harvard Law School in 2003. 2014. “Broken at Both Ends: The Need to Reconnect Energy and Environment.” 65 Syracuse L. Rev. 53. Lexis.

Reliable electricity supply requires a constant, second-by-second simultaneous balancing of power generation supply to meet demand on the utility grid. 3 The United States electric grid will collapse within approximately four seconds if sufficient generation of power is not constantly supplied to meet fluctuating consumer demand. 4 Either too [\*55] much or too little power causes system instability, 5 and a loss of power would disrupt communication, transportation, heating and water supplies, hospitals, and emergency rooms. 6 According to Kirchoff's Law, 7 power moves almost at the speed of light on an energized grid. 8 If power supply does not constantly balance instantaneous demand, the grid can blackout large areas, 9 as happened to the Northeast United States population on August 14, 2003, 10 and subsequently with rolling blackouts in Texas. 11 The 2003 blackout affected fifty million people and caused a loss of six billion dollars. 12 During this blackout, production was lost at approximately half of the Chrysler plants, a Ford plant was lost for a week of repairs, oil refineries shut down, one chain of 237 drugstores in New York City was forced to close, major urban airports closed causing more than a thousand flights to be cancelled, and frozen and perishable foods were lost. 13

## Norms ADV

### Environment Addon---2AC

#### Adapting international law to new forms of warfare solves Bio-d and pollution

Ted **Piccone 17**, Nonresident Senior Fellow, Security and Strategy - Foreign Policy, 4/12/17, “Why international law serves U.S. national interests”, https://www.brookings.edu/research/why-international-law-serves-u-s-national-interests/

Now, with over 560 major multilateral instruments deposited with the United Nations alone, citizens around the world benefit every day from rules their governments have adopted conjointly with each other. These agreements, as the American Society of International Law has documented, enable worldwide telecommunications and postal networks; universal recognition of time standards; improved weather forecasting; stronger safety standards for automobiles, airplanes, and ships; sharing of information about the origin of our food and other products; protection of software, literary, and artistic works; and preservation of cultural heritage sites and endangered species, to name a few.[1] With the adoption of international human rights treaties after World War II, these rules expanded to protect people from torture and other forms of inhumane treatment; promote equal protection for women and children, including for adopted children and those caught in custody disputes; and facilitate pursuit of war criminals, terrorists, human smugglers, and drug traffickers. Agreements to protect the public and the environment from chlorofluorocarbons (CFCs) and other harmful pollutants are among some of the more effective binding instruments of modern international law.¶ Despite these and many other obvious benefits from international law, the political culture of the United States has turned markedly sour when it comes to ratifying treaties that demonstrably serve its national interests. Two recent examples immediately come to mind: The U.N. Convention on the Rights of Persons with Disabilities, which is modeled on the Americans with Disabilities Act of 1990 and would protect disabled Americans when traveling overseas, was denied Senate ratification in 2012 based on spurious charges it would impinge on home schooling.[2] Similarly, the U.N. Convention on the Law of the Sea, endorsed by senior U.S. military, defense, business, and environmental leaders as a key instrument for protecting U.S. interests in safe passage for its vessels and in its 200-nautical-mile exclusive economic zone, was blocked by 34 Republican senators in 2012 on grounds it would, inter alia, bind the United States to third party arbitration.[3] Meanwhile, China and others are shaping the rules and practices of the treaty body that regulates exploitation of seabed resources without Washington having a seat at the table. ¶ Such pro-sovereignty sentiments are now the dominant view in the White House and most of the Republican-controlled Congress. That is likely to spell further trouble for preserving U.S. leadership of an international order which has overwhelmingly served U.S. interests in a coherent system of rules and customs that has given us 70 years free of direct major power conflict and impressive economic prosperity.¶ The Justice Stephen Breyer Lecture series on international law, formally established in 2014 in partnership with the Netherlands Foreign Ministry, the mayor of The Hague, and The Hague Institute for Global Justice, was created to help policymakers on both sides of the Atlantic think about new challenges to international law and order. It would be fair to say that when our cooperation on this initiative began in 2013, we did not imagine that the pendulum swing against the underpinnings of the international order would advance as far and as fast as it has in the last year. Core beliefs and lessons learned from the 20th century are up for grabs around the world, including on both sides of the Atlantic, at least judging from current political discourse favoring nationalism over “globalism.” A trans-Atlantic approach, therefore, is particularly timely and relevant.¶ A trans-Atlantic perspective is also valuable as an intellectual endeavor because Europeans and Americans come from different historical perspectives, a point James Madison made in 1792: “The [U.S.] Constitution is a charter of power granted by liberty,” not, as in Europe, “a charter of liberty…granted by power.”[4] The Declaration of Independence’s reference to “a decent respect to the opinions of mankind” was an early indication, however, that America’s founding fathers felt an obligation to consider the views of others, even its former colonial masters, in matters of law and justice. Justice Breyer, “the great transnationalist judge of our age,” has taken up that charge in the modern era, following in the tradition of Chief Justices John Marshall and John Jay.[5]¶ Since then, trans-Atlantic jurisprudence has largely converged around some fundamental principles based on national constitutions, the United Nations Charter, and institutions founded after World War II—“shared public norms with similar meanings in every national system of the world,” as Professor Harold Koh puts it. But meaningful differences remain and often revolve around the limits to which citizens and their representatives are prepared to cede traditional sovereignty to an international body. The European Union, for example, is wrestling mightily with both the benefits and costs of “pooled sovereignty.” While the United States may be a laggard when it comes to adopting certain treaties, it is not immune from the judicial and legislative decisions of other countries, as Justice Breyer himself explained so well in his inaugural lecture at Brookings. In a quickly changing world, he said, “we better learn what is going on elsewhere because that affects directly what we do at the Supreme Court. In a word, understanding and referring to what is happening abroad is often the best way to preserve our American values,”[6] particularly our faith in the rule of law for ourselves and in our relations with others.¶ Justice Breyer’s analysis of five areas in which the development of law in other parts of the world has a direct effect on U.S. judicial decisionmaking includes matters highly relevant to public debates today, from protecting civil liberties from executive overreach to determining the application of World Trade Organization rules and decisions to U.S. domestic law. Under a Trump White House and Republican-controlled Congress clamoring to put America first, these issues are bound to be fiercely contested in the months ahead.

One area of international law that is not contested, at least not by the United States, is the strict prohibition against the production, stockpiling, and use of chemical weapons and their precursors, as set forth in the U.N. Chemical Weapons Convention (CWC).[7] Ratified in 1997 by the U.S. Senate after intense debate, the CWC and its implementation arm, the Organization for the Prohibition of Chemical Weapons (OPCW), headquartered in The Hague, is the only legally binding instrument to ban comprehensively an entire class of weapons of mass destruction under international verification. More importantly, it has established a process in which the vast majority of states have declared their chemical weapons stockpiles for the purpose of their destruction under international monitoring. The United States and Russia, which hold the largest amount of such weapons, have committed to destroy their holdings completely by December 2020 and September 2023, respectively. The task of ridding the world of these reprehensible weapons will not be complete, however, until states outside the convention, like North Korea, are brought to heel. Even more challenging, as OPCW Director General Ahmet Üzümcü warned in his remarks at Brookings in April 2015, is stopping terrorists and other rogue actors from using chemical weapons to attack U.S. troops and innocent civilians, as seen in Iraq and Syria in 2016.[8]

In addition to the overwhelming international consensus to stop the use of chemical weapons, recent events in Syria have demonstrated the operational value of such binding commitments. After reports of chemical weapons attacks against Syrians were tragically confirmed in August 2013 when an estimated 1,500 people died from a sarin nerve gas attack in Ghouta, the treaty was quickly put to work. In short order, a U.N. investigation confirmed the use of chemical weapons, Syria submitted its instrument of accession to the CWC, and Russia and the United States agreed on a framework for the elimination of the Bashar Assad regime’s chemical weapons program. The OPCW then fast-tracked approval of a plan to eliminate the weapons, which the Security Council endorsed the same day.[9] Three days later, OPCW experts were on the ground in Damascus to help verify Syria’s stockpile of approximately 1,300 metric tons of chemical weapons and oversee their destruction. As further elaborated by Director General Üzümcüin his speech at Brookings, a remarkable multilateral response involving contributions from 35 OPCW member states led ultimately to the removal and destruction of all of Syria’s declared chemical weapons by January 2016.

Unfortunately, the story does not end there. Reports of new attacks in Syria, this time with chlorine agents, emerged in 2015 and led to further U.N. investigations, spurring additional U.N. Security Council proposals by the United States and others to hold perpetrators accountable. This time, however, U.S.-Russia cooperation had evaporated, leading to a joint Russia-China veto of a U.N. Security Council resolution in February 2017 that would have imposed sanctions under Chapter VII of the U.N. Charter on Syrian government officials and entities linked to chemical weapons attacks; placed an embargo on arms sales and chemicals intended to be used as weapons; and established a mechanism to monitor implementation.[10]

The lessons learned from the Syria case about the realities of international law and politics are manifold: (1) establish clear rules of the road and mechanisms for implementation before a crisis hits; (2) move quickly on windows of opportunity when they arise; and (3) fortify the political will among major powers to ensure concrete action.[11] The CWC worked well when all three factors were present, and fell short when the third element dried up. Consensus broke down in part because of the demand for punishment of specific government officials and agencies, a step apparently too far for Syria’s chief defenders on the Security Council. On balance, the CWC and its quick implementation in the Syria case certainly advanced U.S. national security interests in containing the spread of chemical weapons in a volatile part of the world. But the current lack of accountability for blatant violations raises serious questions about the deterrent value of the instrument.

While chemical weapons were prevalent over a century ago, new forms of warfare are emerging that test the boundaries of national and international laws rooted in core principles of necessity, proportionality, reciprocity, and human rights. The absence of specific rules that govern the use of new technologies like armed drones and offensive cyber weapons requires policymakers and lawyers, in Harold Koh’s view, to “translate what Montesquieu called ‘the spirit of the laws’ to present day situations,” at least until paralyzed legislatures are able to write new laws.[12] Under the administration of President Obama, decisionmakers looked both to international and U.S. law for proper authority and guidance on how to engage in non-traditional armed conflict between a state and a transnational terrorist network like al-Qaida. These rules included humane treatment of combatants and noncombatants,[13] as well as the strict prohibition of torture in all places and at all times with no exceptions.[14] Targeted killings were considered permissible if in accordance with international humanitarian law (e.g., in situations of imminent threat, an act of self-defense, or an armed conflict where a combatant has no immunity), if the action was authorized under domestic and international law, and if the target’s rights have been considered and sovereignty of the relevant nation respected.

#### Biod loss causes human extinction

Joe McCarthy 18, a Staff Writer at Global Citizen, Nov 8 2018, "Humans Could Face Extinction if We Don't Protect Biodiversity: UN", Global Citizen, https://www.globalcitizen.org/en/content/biodiversity-loss-human-extinction/

As the sixth mass extinction event accelerates around the world, engulfing thousands of animal and plant species, humans risk facing a similar fate unless drastic interventions are made, according to Cristiana Pașca Palmer, the United Nations biodiversity chief, who recently spoke with the Guardian.

Palmer said that within the next two years, countries have to develop an ambitious plan to conserve land, protect animals, and stop practices that are harming wildlife. This effort is equally as urgent as the Paris climate agreement’s goal of mitigating climate change, she said.

“The loss of biodiversity is a silent killer,” she told the Guardian. “It’s different from climate change, where people feel the impact in everyday life. With biodiversity, it is not so clear but by the time you feel what is happening, it may be too late.”

Next month, countries will meet in Sharm el Sheikh, Egypt, to begin mapping out what such a plan would like. Palmer hopes that a final version will be formalized in Beijing in 2020.

If a binding global treaty fails to materialize, then humanity faces an uncertain future, she said. Past efforts to stop the loss of biodiversity have not proved successful, according to the Guardian.

In recent years, evidence of this staggering loss has begun accumulating.

Wild animal populations have declined by 60% since 1970, more than 26,000 plants and animals are close to extinction, nearly two-thirds of the world’s wetlands and half of all rainforests have been destroyed, more than 87% of the world’s ocean area is dying, and the planet needs an estimated 5 million years to recover from the biodiversity loss it has already sustained.

“We are sleepwalking towards the edge of a cliff,” Mike Barrett, executive director of science and conservation at WWF, recently told the Guardian. “If there was a 60% decline in the human population, that would be equivalent to emptying North America, South America, Africa, Europe, China, and Oceania. That is the scale of what we have done.”

“This is far more than just being about losing the wonders of nature, desperately sad though that is,” he said. “This is actually now jeopardising the future of people. Nature is not a ‘nice to have’ — it is our life-support system.”

The benefits of biodiversity are hard to overstate. The food chain, climate systems, atmospheric conditions, natural resources, and much more depend on the delicately structured interactions of ecosystems around the world.

The truly wild places in the world, meanwhile, are crucial to generating, cleaning, and distributing water around the world, and could help to mitigate the looming water crisis. These landscapes and marine environments also clean the air and act as carbon sinks, stabilize the global environment, and protect countries from natural disasters.

In addition to climate change, the biggest threats to biodiversity are deforestation, agriculture, over-development, and industrial pollution.

While Palmer sounded an urgent alarm bell while speaking with the Guardian, she’s hopeful that countries will recognize the threat of biodiversity loss and begin to take action.

The UN is calling for at least 30% of all land and 15% of all marine environments to be protected by 2030 and for targets to be lifted in the following years.

“Things are moving. There is a lot of goodwill,” Palmer said. “We should be aware of the dangers but not paralysed by inaction. It’s still in our hands but the window for action is narrowing. We need higher levels of political and citizen will to support nature.”

#### Pollution causes extinction

Baskut Tuncak 19, Special Rapporteur on the implications for human rights of the environmentally sound management and disposal of hazardous substances and wastes, “Toxic pollution: Another extinction crisis looms, warns UN expert”, https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25201&LangID=E

NEW YORK (24 October 2019) – Under the shadow of the existential threats of climate change and biodiversity collapse lies another, insidious extinction crisis: the toxification of our planet and our bodies, a UN human rights expert told the General Assembly today.

“Our incessant exposure to pollution and other sources of toxic substances poses a global threat to human rights, including to our right to reproductive health,” said the UN Special Rapporteur on hazardous substances and wastes, Baskut Tuncak, as he called on States to recognise and uphold their duty to prevent exposure to hazardous substances.

He said that when viewed through the lens of children’s and reproductive health, the importance and gravity of preventing exposure to toxic substances at the outset sharpens further into focus. Declining fertility, including declining sperm quality and quantity, is only one of many worrying health trends linked to toxic exposure that persist because States have not truly prioritised exposure prevention.

“Every State has binding human rights obligations that create a duty to take active measures to prevent the exposure of individuals and communities to toxic substances. Nonetheless, people and peoples are knowingly exposed to a multitude of hazardous substances that could be prevented. Relief and remedy, to the limited extent it materialises, is often insufficient and too late for those who are exposed.”

Tuncak’s report reminds States of their duty to prevent exposure to toxics in the context of the rights to life, health, dignity and bodily integrity. It is increasingly demonstrated that “safe” levels of exposure for many toxic substances are presumed, and for many there is no safe level of exposure.

“There is a danger that the human rights to safe water, adequate food and housing, clean air, a healthy environment and safe and healthy work, among others, will be a false promise and never truly realised without concerted efforts to make exposure prevention an urgent priority,” said Tuncak.

Tuncak stressed that this “toxic cocktail” of pollution is conservatively calculated as the single largest source of premature death in the world, and it causes and contributes to a “silent pandemic” of diseases and disabilities. “We can no longer see the problem substance-by-substance – but rather must address the combined effect of a multitude of chronic exposures, particularly on those that are most vulnerable, such as children, workers, different genders and people living in poverty,” he said.

### AT: SQ Solves

#### Squo doesn’t solve norms---AFF key

Charlie Dunlap 17, former deputy judge advocate general of the United States Air Force, joined the Duke Law faculty in July 2010 where he is a professor of the practice of law and Executive Director of the Center on Law, Ethics and National Security, “Are cyber norms as to what constitutes an “act of war” developing as we would want?,” Lawfire, 9/15/17, https://sites.duke.edu/lawfire/2017/09/15/are-cyber-norms-as-to-what-constitutes-an-act-of-war-developing-as-we-would-want/

Ironically, there has been a lot of work done to help nations work through the law regarding cyber incidents. For example, the NATO-sponsored Tallinn 2.0 Manual provides superb guidance as to the current state of the law vis-à-vis cyber operatiions (albeit it is not an official NATO document.) Chapter XVI of the DoD Law of War Manual also provides – at least for DoD – some broad guidance as to the law applicable to cyber operations.

The devil, of course, is in the details – and those details involve determining what facts are appropriately applied to the law. It is here where uncertainty frequently exists. For example, last June, NATO Chief Jan Stoltenberg announced that a “severe” cyber-attack might trigger NATO’s Article 5 “collective self-defense” authority, but it still isn’t clear what “severe” would mean to decision-makers in a particular factual circumstance.

Given the importance of state practice in the development of norms, VADM Tighe’s comments are apropos. In speaking to some National Security Council experts yesterday afternoon, I argued (along the lines of my prior Lawfire blog) that it is extremely important for the U.S. to characterize cyber incidents for what they really are (at least from the U.S. perspective. If they amount to unlawful uses of force that violate the UN Charter and permit a self-defense response under Article 51 of the Charter, we should say so. (N.B. The U.S. takes an expansive view of what would trigger self-defense authority – see Chapter XVII of the DoD Law of War Manual and former Legal Advisor to the State Department Harold Koh’s 2012 remarks, and the critique of them here ).

Importantly, an official characterization of a particular cyber incident as a “use of force” or “armed attack” (UN Charter terms) – or even the colloquial “act of war” (again, a political term, not legal one) – does not mandate a particular response, but doing so would nevertheless serve to help advance international norms. Of course, like everything else, there are potential downsides. In a very thoughtful article, Hofstra professor Julian Ku discusses the “restrictivist” view that China takes with respect to the use of force generally, and opines that it may not be in the U.S.’s interest to force China to accept the U.S. interpretations of international law restrictions as to cyber warfare because of the potential of China applying them pejoratively to U.S. actions in other contexts.

### Yes Model---China

#### NATO’s failure to respond to Russia’s hybrid warfare legitimizes China

Sascha Dominik (Dov) Bachmann et al 19, Professor, Canberra Law School, “Competition short of war – how Russia’s hybrid and grey-zone warfare are a blueprint for China’s global power ambitions ,” Australian Journal of Defence and Strategic Studies Vol. 1 No. 1, November 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract\_id=3483981

Russia and China have been working hard to end the unipolar order of the US, which has dominated global politics since the end of the Cold War and the implosion of the Soviet Union and the Warsaw Pact in 1991. It has to be acknowledged that a multi-polar world order, with China and Russia competing with the US for global influence and power, is the reality of today’s global world affairs. Australia has to recognise this reality in order to not fall into the trap of blindly following the US’s present attempts to counter and/or reverse the threats to its waning unipolar status as sole superpower without too much concern regarding its allies.

China and Russia have acted illegally in violation of international law and aggressively in both instances: China in regard to the South China Sea and Russia in regard to Crimea and Ukraine. Both actors seem to have identified the unwillingness and inability of the West to counter their actions effectively. In Europe, no one wants to risk war over Russia’s aggression in Ukraine. In the Asia–Pacific context, ASEAN countries, wedged between the giants India and China, in the South China Sea, are in much the same situation. Neither China nor Russia expect any military response from NATO or an ASEAN country, and so continue to use hybrid warfare and greyzone tactics to erode further the international systems of comity and the rule of law. This leads to erosion within the affected societies and political systems, as the indecisiveness within the EU to continue with sanctions against Russia highlights.79

There is growing Sino-Russian cooperation across nearly all domains and sectors of interest and potential risk for Australia. From economic ties (China is Russia’s second largest trading partner) to technical collaborations in respect to the internet of things including 5G infrastructure, and now the explicit expression of the intent to ‘develop bilateral cooperation, in the spirit of comprehensive partnership and strategic interaction’,80 Sino-Russian cooperation increases.

It seems only logical that China is following Russia’s successful use of hybrid warfare as ‘it reduces the need for using classical military resources, providing them with a shield of plausible deniability’.81 With the backdrop of Europe’s failure to call out Russia for its aggression in Ukraine, Russia’s hybrid warfare strategy seems to have worked so far. Arguably, China’s strategy in the South China Sea also seems to be working. Terraforming the maritime environment as undertaken by Russia and China is illegal under international law and constitutes the use of force or the threat of such. The fact that Russia and China successfully managed to get away with such illegal and aggressive behaviour is reprehensible and constitutes a clear and present threat to international comity and security.

The threats posed by contemporary adversaries (both state and nonstate actors) in employing hybrid and grey-zone tactics poses an increasing threat to Australia’s security and global stability in the years to come; accordingly the identification of such threats and the planning of countermeasures and contingencies to meet these threats is paramount. Whether such an approach is based on a doctrinal approach of hybrid warfare as understood in the NATO and Western context, the use of greyzone counter-tactics or a yet-to-be developed doctrine is academic, so long as the response is comprehensive and multimodal, drawing from the full spectrum of military and civil resilience.

### Yes Model---Turkey

#### Turkey’s actions are symptomatic of a turn to gunboat diplomacy

İlhan Uzgel 20, professor in the department of international relations at Ankara University, “The rise of Turkey’s gunboat diplomacy,” Duvar English, 1/6/20, https://www.duvarenglish.com/columns/2020/01/06/the-rise-of-turkeys-gunboat-diplomacy/

The Erdoğan government has been taking Turkey from one crisis to another, opening up new military and diplomatic fronts. The government’s decision to send troops to support the Government of National Accord in Libya, and its prior acceptance that these forces can be engaged in actual conflicts, is the most risky military adventure the AKP has ever taken. It seems that both the government and the pro-AKP circles do not seem to be aware of the risks they have taken in such an overseas military engagement which would be conducted in a hostile environment, against a multitude of adversaries and two thousand km away from the mainland.

Putting aside the risks it contains, the decision to engage militarily directly in the Libyan civil conflict is also symptomatic of a trend in recent Turkish foreign policy which has become militarized to a great extent. Currently, Turkish air force is pondering the PKK sites in northern Iraq, Turkish land forces made three incursions in northern Syria and controlling the Idlib area with its observation posts, and has been engaged in the not so secret arms procurement to the radical Islamist groups in Libya which turned into a deeper engagement in armed drone war over the Libyan airspace. This last authorization of dispatching Turkish troops to Libya would cover air, land forces and the navy which means a full-scale military engagement that is unprecedented in Turkey’s history except the military operation in Cyprus in 1974. It is important to examine the reasons behind this evolving militarization of Turkish foreign policy in regional issues and crises. There seems to be three intertwined reasons which forced the AKP government to resort to the military force in dealing with the security issues, many of which it directly contributed to emerge.

### IW Impact---AT: Defense

#### The threats it causes are systemic and can’t be addressed without targeting the pollution of the information space

Herbert Lin 19, senior research scholar for cyber policy and security at the Center for International Security and Cooperation and Hank J. Holland Fellow in Cyber Policy and Security at the Hoover Institution, both at Stanford University, “The Existential Threat from Cyber-Enabled Information Warfare,” Bulletin of the Atomic Scientists, vol. 75, no. 4, Routledge, 07/04/2019, pp. 187–196

The infrastructure for human civilization is undeniably tangible (that is, physical, chemical, and biological), but it is increasingly virtual as well, and the virtual aspects of that infrastructure – the information ecosystem (or, equivalently, environment) – in many ways has become central and often critical to the way people now live all over the world.

As Balkin (2012) describes, “it is not an exaggeration to say that modern states are informational states: states that recognize and solve problems of governance by collecting, analyzing, and distributing information.” Consider that nations require good information to allocate benefits and social services to the populace; to administer mechanisms for public safety (e.g. law enforcement, court systems, fire-fighting); to provide for national security; to gather revenue to support national expenditures; and to engage with other nations in ways that support national interests.

Businesses and nonprofit entities in turn are also highly dependent on information. They use it to develop products and services for customers and clients; to understand markets and audiences for their products and services; to inform customers and clients about their products and services; to comply with laws and regulations applicable to their products and services; and to maintain their accounting and finances. Construction and manufacturing projects entail the coordination of dozens, hundreds, or thousands of parties – all of whom must have a justifiable confidence in the information they are sharing and relying upon.

Contextualized, reliable, trustworthy information is as important to the thinking of human beings as clean air is to human breathing. Human beings depend on good information for making informed decisions about political candidates standing in elections; to know as consumers which specific products and services will best serve their needs; for managing their finances; in making health-related decisions about themselves and their loved ones; in learning to perform their jobs more effectively or efficiently; and in truly countless other ways.

Nations also engage extensively in information production. They provide education for young people; support scientific research that undergirds economic growth and prosperity; and collect, curate, and disseminate large-scale statistical data that influence decisions at every level of society.

Imagine what life would be like if citizens could not count on the validity and trustworthiness of the information underlying any of these activities. In some cases, the result would be no more than minor annoyance. In others, however, the result could be life-threatening. Nations could be crippled, as they could and likely would make bad or at least sub-optimal decisions about war and peace, the economy, law enforcement, housing, food production, energy, and the many other important matters for which governments have some responsibility.

On the existential threat from cyber-enabled information warfare

Corruption of the information ecosystem has become an existential threat to civilization as we know it because prosperity and advancement depend on a secure information infrastructure and environment that provides human beings with contextualized, reliable, trustworthy information when and where it is needed. Information is as much a part of human ecology and the essence of being human as DNA (itself a form of information!) is a part of the evolutionary processes in biological systems.

Today, chaos reigns in much of the information ecosystem on which societies depend. In many forums for political and societal discourse, national leaders shout about fake news, by which they mean information they do not like. These same leaders lie shamelessly, calling their lies truth, or perhaps “truthful hyperbole.” Acting across national boundaries, these leaders and their surrogates exacerbate existing divisions, creating rage and diminishing confidence in elections and democratic institutions. Using unsupported anecdotes and sketchy rhetoric, denialists undermine well-established science about climate change and other urgent issues. Established institutions of the government, journalism, and education – institutions that have traditionally provided stability – are under attack precisely because they have provided stability.

The founding of the Bulletin predates by several decades the widespread availability of computers, the Internet, smart phones, search engines, and social media. Few could imagine in 1945 a technological environment that affords today’s high-speed and widespread connectivity, high degrees of anonymity, insensitivity to distance and national borders, easy and customized information searches, democratized access to publishing capabilities, inexpensive production and consumption of information content (including and increasingly importantly emotionally evocative video and audio content), disintermediation of established information sources, and ubiquitous, always-on, always-available access to information sources through mobile devices.

Such advances in information technology have heralded the arrival of the information age, a world in which taking near-immediate advantage of information opens up enormous opportunities in both the private and public sectors for improved delivery of existing products and services and, perhaps more important, the creation of entirely new products and services. Products and services can be customized to individual needs and preferences on a large scale and at more affordable costs. Transactional friction can be tremendously reduced. Through the Internet of Things, actuators and sensors can be connected to process control computers to optimize the behavior and function of physical systems. Everywhere that information can be used to create and improve new and existing functionality (that is, essentially everywhere), one can find or imagine new information technologies to do so.

At the same time, advances in information technology have a dark side. The same increases in the volume and velocity of information have created a louder and more chaotic information environment that stimulates fast, angry, reflexive, intuitive, and visceral thinking, reaction, and action in people and thus displaces more complex, reflective, and rational thought. In a chaotic environment of information overload, people are more likely to use mental shortcuts as a way to reduce the cognitive burden that such an environment places on their thinking.

In recent years, we have seen how the Internet, social media, and mobile devices (and other technologies) can be used by foreign adversaries to interfere in elections and to disrupt the democratic process. We have seen:

Social media exploitation of cognitive biases to increase their impact and reach – short messages of 280 characters and emotionally evocative video/audio clips are nearly ubiquitous and much more the norm than they ever were two decades ago.

Disintermediation of established information sources that reduces the role and influence of those previously responsible for providing factual information and proliferates information sources. The US Supreme Court noted in Associated Press v. US (1945) that “the widest possible dissemination of information from diverse and antagonistic sources is essential to the welfare of the public, that a free press is a condition of a free society.” Today, modern information technology has enabled the creation of a larger number of information sources than the 1945 US Supreme Court could possibly have imagined.

Search engines that return highly visible results for queries based in large part on the popularity of those results and the inferred desires of the user for specific information rather than their actual importance to those queries. Such functionality also makes it easier than ever for people to find information online “by doing their own research,” thus indulging in their confirmation biases by selectively finding and attending only to information that confirms one’s beliefs. Search engine optimization techniques enable gaming of search algorithms to promote the visibility of false, misleading, or worthless information.

Many-to-many connectivity that enables the formation of echo chambers and media bubbles that reinforce pre-existing beliefs.

Large-scale data mining that allows adversaries to sift huge amounts of personal data on individuals to identify and target those most susceptible to customized, inflammatory, false, malign, or misleading messages – and also to keep such messages away from public view.

Near-immediate data transfer, which enables propaganda and other malign information to spread far and wide quickly, while efforts to correct false information are more expensive, often fall short, and frequently fail altogether.

Inauthentic voices that are largely indistinguishable from authentic ones. Macedonian entrepreneurs discovered ways to monetize an affinity of Trump voters for fake news (Subramanian 2017). Paid human employees of the Internet Research Agency created and spread false information on behalf of the Russian government prior to the 2016 U.S. election (MacFarquhar 2018). And automated “bots”–accounts purportedly associated with human users but in fact managed entirely or mostly by machines – add further chaos to the information environment.

Is this state of information affairs really new? Haven’t adversaries of all stripes always employed propaganda and lies – otherwise known as information warfare (or at least a big part of it) – to advance their interests?

Yes. Information warfare indeed has a long pedigree that reaches into the past for at least the three millennia since the Trojan Horse enabled Greek warriors to breach the walls around the city of Troy. Much more recently, the rise of the Nazi regime in Germany relied on propaganda. As Hitler (1925, 155–56) wrote:

[I]ts purpose must be … to attract the attention of the masses and not by any means to dispense individual instructions to those who already have an educated opinion on things or who wish to form such an opinion on grounds of objective study – because that is not the purpose of propaganda, it must appeal to the feelings of the public rather than to their reasoning powers. … The art of propaganda consists precisely in being able to awaken the imagination of the public through an appeal to their feelings, in finding the appropriate psychological form that will arrest the attention and appeal to the hearts of the national masses. … The receptive powers of the masses are very restricted, and their understanding is feeble.

But more so today than at any earlier point in human history, human beings are vulnerable to information warfare. At the same time that new information technologies have led to an increase in the volume and velocity of information available on Earth by many orders of magnitude in the past few decades, the cognitive architecture of the human mind is more or less unchanged on the time scale of centuries or even millennia.

On human cognition

Research in the fields of cognitive and social psychology has formalized what Hitler knew intuitively. We now understand that human cognitive processing capability is not unlimited; humans have finite cognitive resources that can be “used up” under mentally stressful circumstances. Findings from the same cognitive psychology that has transformed neoclassical economics into behavioral economics (and resulted in three Nobel Prizes in economics) have made clear the “bounded rationality” of human thought and the simultaneous existence in every individual of the capability to engage in two types of cognitive processing.

Specifically, heuristic dual-system cognitive theory posits that human beings have two systems for cognitive processing – an intuitive, reflexive, and emotionally driven mode of thought (often designated as System 1) and a slower, more deliberate, analytical mode of thought (often designated as System 2). Kahneman (2011) provides a primer on System 1 and System 2 thinking. (See Petty and Cacioppo 1986; Chaiken 1987 for other variants of dual-system cognitive theory; see Kruglanski and Thompson 1999 for a contrary view on dual-system cognitive theory.)

System 1 is designed to operate rapidly, but it can do so because it does not take account of all available information and is thus more prone to error (also called bias). System 2 operates more slowly but is more likely to take into account the available information and is less prone to error. People engaging in System 1 information processing respond more emotionally and less rationally or critically than in System 2 processing.

Most important, System 1 thinking is the default mode of thought for human beings – it uses smaller amounts of cognitive resources, relies on simple gut-based judgments, and is used more often when humans are under stress. For most situations encountered in everyday life, System 1 thinking is adequate and produces mostly valid and useful outcomes, but it often fails when a situation requires complex inferences for understanding. For such situations, System 2 thinking, which is effortful and consumptive of cognitive resources, is more often appropriate – and when individuals fail to use System 2 when it is appropriate to do so, they are easily misled.

Most individuals are capable of both System 1 and System 2 thinking; thus, the important operative question is the circumstances under which they select one or the other type of thinking. Psychology has accumulated considerable evidence relevant to this question.

For example, Taber and Lodge (2006) show that an individual tends to be less critical of information that is favorable to his or her position than of information that is not favorable – that is, he or she is more likely to engage in System 1 thinking for favorable information. People have a confirmation bias in their information seeking and processing behavior – they preferentially seek out information that is consistent with their beliefs and they are highly critical of (or ignore) information that contradicts their beliefs. In a meta-analysis of 91 studies, Hart et al. (2009) considered two motivations for how an individual might select information to consume – the desire to gain an accurate understanding of reality and the desire to feel validated in his or her beliefs. These two motivations conflict when an accurate understanding of reality does not validate one’s beliefs, and such a situation motivates the question of which of these motivations is more powerful. Hart et al. concluded that both motivations drive human information-seeking behavior, thus moderating each other to a certain extent, but that on balance, humans do exhibit a tendency towards the validation of their beliefs. People are also subject to belief perseverance (a.k.a. a continuing influence effect) – a cognitive bias through which individuals do not revise beliefs based on erroneous information even when they know for sure that such information is erroneous (Lewandowsky et al. 2012).

Maintenance of an individual’s social identity is an important influence on his or her invocation of System 1 or System 2 thinking. Evidence suggests that individuals tend to adopt the views of the peer groups that are most salient to them, even if the “objective” or “factual” information available to them contradicts those views. (Asch 1951 performed the classic “conformity experiments” that demonstrated this phenomenon in the early 1950s.) Uncritical System 1 thinking is active in processing information that is consonant with the beliefs and attitudes of those peer groups. Critical and skeptical System 2 thinking is active in processing information that is dissonant to those groups’ beliefs. These effects (that individuals tend to accept salient group norms) are even more pronounced in an anonymous environment, such as that which characterizes much online interaction (Postmes et al. 2001).

Lastly, there is evidence that emotion and motivation affect cognition. For example, people who are angry tend to rely more heavily on simple heuristic cues (suggestive of System 1 thinking) than those who are not angry (Bodenhausen, Sheppard, and Kramer 1994). Individuals are more likely to stereotype people (a form of System 1 thinking) when that stereotype is consistent with their desired impression of those people; conversely, when the stereotype is inconsistent with their desired impression, individuals tend to inhibit the use of this stereotype (Kunda and Sinclair 1999). Negative emotions (such as those induced by the receipt of information incongruent with a person’s prior beliefs) can improve the ability of a person to reason logically, thus enabling him or her to negate or discount that information (Goel and Vartanian 2011).

In the new information environment, exploitation of human cognitive architecture and capabilities – which are largely unchanged from what existed millennia ago – provides the 21st century information warrior with cyber-enabled capabilities that Hitler, Stalin, Goebbels, and McCarthy could have only imagined. By exploiting cognitive limitations, the perpetrators of cyber-enabled information warfare have learned to exacerbate prejudices, biases, and ideological differences; to add heat but no light to political discourse; and to spread widely believed “alternative facts” in advancing their political positions.

Russian interference in the 2016 US presidential election has dominated news headlines ever since. But interference by authoritarian countries in the elections of democratic states – as undesirable and threatening as it may be – is hardly the only negative consequence of cyber-enabled information warfare. The problems of nuclear war and climate change are hard enough to solve even when well-intentioned, well-informed parties on all sides share a basic understanding and knowledge of the relevant facts. Yes, they may have different values and different priorities, may act under different constraints, and be able to bring to bear different levels of resources to these problems.

But without shared, fact-based understandings of the blast, thermal, and radiation effects of nuclear explosions, what hope is there for national leaders to reach agreements to reduce the threat of nuclear holocaust or to make good decisions about nuclear weapons use in times of crisis? Without shared, fact-based understandings that rising atmospheric carbon dioxide concentrations caused by human beings result in corresponding increases in global temperature and climatic disruption, what hope is there for national leaders to reach agreements to begin serious efforts at decarbonizing their economies?

Climate change denialism

Climate change denialism can be fairly characterized as cyber-enabled information warfare against the reality of large-scale anthropogenically-induced climate change. In the responses of people resistant to taking action to mitigate climate change, we see a number of psychological factors at work (Zaval and Cornwell 2016). For example, one key element of System 1 thinking is the availability heuristic, with which individuals tend to associate the likelihood of an event with the ease with which they can remember similar events in the past. But the long-term consequences of climate change are unprecedented in recorded human history and obviously people have no personal memories of unprecedented events.

Moreover, climate change is a long-term process whose inexorable progression is easily masked by short-term fluctuations in local weather conditions. For example, public concerns about climate changes correlate with local weather conditions (Krosnick et al. 2006). Climate change deniers are also quick to flag for public attention days that are particularly cold as “evidence” that global warming is not occurring and thus, they claim, discrediting theories of climate change. This illustrates a bias known as attribute substitution, as Kahneman and Frederick (2002) describe, through which individuals substitute salient information (such as the cold temperature today) for information that is more relevant but harder to understand (such as information about global climate change).

People are also subject to a loss-aversion bias, in which they place greater weight on losses than gains of equal value. In 1992, the United States committed itself to the United Nations Framework Convention on Climate Change, although President George HW Bush also stated that “the American way of life is not up for negotiation” – and in 2018, the United States withdrew from the Paris Agreement (which was based on the convention). The argument? That the United States would have to give up too much if it kept to the agreement.

To close this (merely illustrative) exploration of biases relevant to climate change denialism, the optimism bias suggests that people consider themselves exceptions when considering the likelihood of a negative event occurring. That is, bad things may happen to other people, but they won’t happen to me, even though I and those other people are similar in important and relevant ways. In a climate context, the bad things may involve sea level rise or heat waves – and the misperception that “others may suffer from such problems but I won’t” diminishes the power of personal concern as a driver for rational decision making.

Connecting the operation of these cognitive biases to the affordances of modern information technologies is not difficult. For example, Roxburgh et al. (2019) demonstrate how the characteristics of specific weather events (e.g. hurricanes or snowstorms) and “short-term socio-political context can play a critical role in determining the lenses through which climate change is viewed.” Note especially the importance of “short-term socio-political context” – precisely the context that social media shapes.

Elsasser and Dunlap (2013) noted the influential role of a variety of newspaper columnists in advancing denialist arguments and thus amplifying these arguments to a broad segment of the American public. Fewer in number then, essentially all columnists today (of all political leanings) have a social media presence that they use to publicize their work, and in many instances their online presence is driven in significant part by social media and reach many more readers online than in print. Furthermore, subtleties and nuances in their extended written pieces are likely to be lost when they are represented in social media.

Another important element of climate change denialism is the easy accessibility of seemingly-authoritative information that casts doubt on the well-established science of climate change. As reported by The Guardian, a variety of largely secret funding sources distributed $118 million to 102 denialist organizations (Goldenberg 2013). Oreskes and Conway (2011) provide the definitive work on deliberate information campaigns to obscure the scientific truth on a range of issues from smoking to climate change. These denialist organizations have generated a variety of products for public and policy consumption (but – unsurprisingly – not many peer-reviewed scientific articles) that are easily accessible to the public, mainstream media outlets, and policy makers. Their products are broadly disseminated through social media and easily found through customized search, and they are sought by reporters who seeking to cover “both sides” of a controversy that is intellectually equivalent to a “controversy” about whether the earth is round or flat.

Nuclear conflict

On the risks of nuclear conflict, theories and approaches to nuclear deterrence and strategic stability developed prior to the collapse of the Soviet Union in the late 1980’s and early 1990’s rest on the presumption of rationality in national decision makers. In particular, they assume that adversaries are deterred from attacking by a threat of retaliation that would impose costs on the adversary that would outweigh any conceivable benefits that it would gain from an attack (Morgan 2003). Central to this assumption is a rational adversary that can and does make a calculation of expected costs and benefits, compares them, and then acts accordingly.

But the psychologically informed understanding of real-world decision making described above was not accepted widely in the scientific literature until approximately the same time as the collapse of the Soviet Union, and the seminal work in such understanding occurred only in the decade previous to that. What a psychologically-informed understanding of real-world decision making tells us is that the rationality assumption at the base of much traditional thinking on deterrence and strategic stability is untenable, given that humans have evolved to rely on intuitive, reflexive, heuristic System 1 thinking to make decisions, particularly when faced with time pressures, surprise and other obstacles to the deliberate calculation implied by System 2 thinking (Kahneman 2011). Psychology tells us that – more often than not – the fast, intuitive judgements of System 1 often take precedence over the slower, more analytical thinking of System 2.

The challenges posed by reflexive reliance on System 1 thinking are greatly accentuated by characteristics of today’s information environment. Social media networks in particular are optimally designed to stimulate System 1 thinking – emotional, reflexive, immediate – and they rapidly transmit content among like-minded individuals, creating the ideal conditions for public polarization and divisiveness to occur (Pfeffer, Zorbach, and Carley 2014). Multiple narratives rapidly emerge around complex events; citizens splinter into their own informational universes and are unable to agree on an underlying reality. Political leaders themselves are subject to these conflicting narratives and may even be active and influential participants in one or another of them.

It is thus easy to posit that in this information environment, manipulated information – either artificially constructed or adopted by a strong grassroots base – could be used by interested parties to generate pressure on leaders to act. At the same time, leaders themselves are likely to be facing information overload and less able to distinguish analyzed information from their own intelligence sources and other, unvetted information originating from their constituencies.

The coming information dystopia

Nuclear war and climate change are arguably the most important existential challenges today that are compounded by the corruption of the information ecosystem. But even if a single miraculous stroke the laws of physics were changed to make nuclear weapons impossible to build and operate and to immediately eliminate anthropogenic emissions at zero cost, cyber-enabled information warfare could still can lead to an information dystopia. Here are some possible elements:

Adversaries manufacture numerous graphic videos of American soldiers (complete with sound effects) committing battlefield atrocities, and spread them widely through the Internet. Once upon a time, high-quality video forgeries were difficult and expensive to make. AI-based technologies will bring this so-called deepfake capability to the masses, and anyone with imagination, a modicum of technical skill, and a personal computer will be able to distribute reasonably realistic forgeries. Denials will be issued but of course will also not be believed by large fractions of viewers. Even if proof of inauthenticity can be provided, such evidence will not affect the responses of many viewers.

Political campaigns conduct similar efforts to discredit political opponents (e.g. “showing” an opponent making controversial or disqualifying remarks before an election). But they also use the existence of deepfake technologies to deflect attention from authentic and real evidence of their own political and personal misdeeds. For example, a real video of a candidate punching an old lady who supports his opponent will be dismissed as “one of those deepfakes that anyone could have produced.”

Financial markets are disrupted by falsified videos of CEOs making announcements regarding company prospects that are much more pessimistic than expected. Attempts to correct the record are drowned out in a subsequent flood of contradictory information, all of which appear at first glance to be authentic.

Public safety is compromised by reports of local disasters (e.g. explosions of chemical plants that result in the release large amounts of toxic gases). These reports, along with “authentic” video of people choking amidst locally familiar locations (e.g. well-known fields or sport stadiums), cause spontaneous mass evacuations. Contradictory directions for evacuation broadcast using social media result in chaos on the streets and highways.

Public health is placed at risk when the safety and efficacy of medical treatments known to be safe and effective are publicly questioned through active disinformation campaigns conducted on the Internet and in bookstores. Attempts to provide valid information are met with responses such as “that’s what the pharmaceutical companies and medical establishment want you to think, but just look at what’s happened to our children.”

Children in schools are threatened by online campaigns to spread rumor, innuendo, and positive or negative information about various students. Conducting such campaigns for pay becomes the business model of entrepreneurs who advertise that they can guarantee admission to selective colleges, boost the social standing of the children of their clients, or take revenge on those who have harmed such children, all in anonymous and untraceable ways.

Journalists, political leaders, and judges are compromised by artfully forged emails and alterations to other documents that are mixed with entirely authentic leaked emails and documents and are indistinguishable from them.

A world with these elements – and many more comparable ones – will be the inevitable result if and when deployment and use of the tools of cyber-enabled information warfare become widespread. And even more troubling is the fact that not every bit of information needs to be corrupted for this dystopian outcome to occur – it will require only a fraction of it to be corrupted for people to lose faith entirely in “objective” and “trustworthy” sources of information, the result of which will be that people will fractionate into their own information realities.

Fearing the end of the enlightenment

The Enlightenment established reason and reality as the foundational pillars of civilized discourse. In such discourse, logic matters, and a logical contradiction between statement A and statement B means that at least one of those statements is false. The truth of a statement about the world is tested by its correspondence to objective reality rather than by how many people believe it; that is, empirical data are influential. Furthermore, statements known to be wrong or false do not affect conclusions or choices between alternative courses of action.

Cyber-enabled information warfare provides the tactics, tools, and procedures – in short, the means – to replace the pillars of logic, truth, and reality with fantasy, rage, and fear. In a world of ubiquitous cyber-enabled information warfare, communication and information inflame passions rather than informing reason, play to the worst in people’s cognitive architectures rather than the best, and divide rather than unify. Deliberate corruption of the information ecosystem could be seen as an analog of poisoning water supplies that can be done remotely, inexpensively, and anonymously. All of this is just another way of saying that today it is possible to see glimmerings of an anti-Enlightenment that can possibly take root and that would indeed be the end of civilization as we know it.

Adversaries foreign and domestic that make use cyber-enabled information warfare turn our internal cognitive processes and our external institutional and legal processes against us. Under the cover of “fair play” rubrics and the First Amendment, they have turned us against ourselves. Desperately needed are ways of countering the insidious tactics of cyber-enabled information warfare for ourselves.

How might we proceed? We need action to develop better ways of identifying adversary cyber-enabled information warfare campaigns in progress; good countermeasures to help human beings resist the use of cyber-enabled information warfare operations targeted against them; and good measures to degrade, disrupt, or expose the adversary’s use of cyber-enabled information warfare operations. All of this is easier said than done, however, as cyber-enabled capabilities for information warfare increase while human cognitive limitations remain the same. Our work is cut out for us. If we fail, the world is at increasing risk of large-scale and long-term societal fracture, the end of the Enlightenment, and the start of an informational Dark Age.

#### It's the highest magnitude issue.

Cees J. Hamelink 20, Emeritus Professor of International Communication at the University of Amsterdam, “A Polarized Planet,” Communication and Peace: Celebrating Moments of Sheer Human Togetherness, edited by Cees J. Hamelink, Palgrave Macmillan UK, 2020, pp. 37–66 Springer Link, doi:10.1057/978-1-137-50354-1\_2

Polarization

The Greek philosopher Herakleitos coined the phrase: “From differences results the most beautiful harmony”. Maybe he should have been somewhat more cautious because we are biologically, psychologically and linguistically wired to think in fragments as in most modern sciences where we are still haunted by Cartesian divisions. We understand the notion of “parts” better than the concept of “wholeness” because we tend to think in fragments and not in coherent patterns. Once we have fractured the world into stand-alone pieces, it is an illusion that simply connecting us through advanced technologies will create coherence. Through social media we connect but do not create togetherness. Common to all the forms of fragmentation—that I described—is a mode of thinking that William Isaacs (1999) called “thinking alone” which means being defensive about our positions, clinging to certainties and imposing judgements upon others. It reflects a binary discourse that categorizes people against each other. Men versus women, black versus white, impaired versus non-impaired, religious versus non-religious. Binary thinking fosters exclusion and discrimination. We have no shared discourse to converse about the fractures of humanity. Against this Isaacs argues that we need to “think together” which means listening, respecting, suspending assumptions and letting our inner voices speak up. “Thinking alone” fosters and feeds polarized fragmentation. The opposite poles are immobile and entrenched in their singular identities. Once people lose the capacity to think about themselves in terms of multiple identities, they are ready to believe that the others deserve to be dehumanized and eventually to be eliminated. The belief in singular identities tends to see violence as only way to protect your own identity. When fragmentation gets polarized, conflicting parties tend to forget that all have multiple identities and that identities are not static but dynamic lest we become each others’ enemies. Our identities and those of others are permanently in flow. We are “flaneurs” as Walter Benjamin phrased it. Especially in global cities there is a constant interaction between multiple identities and we need to reclaim the capacity to celebrate this. The city can only survive if we dance in the streets! There are no fixed identities; they are constructed labels for convenient purposes such as domination. Identities are fluid. As Kwame Appiah says in an interview with the Financial Times (31 August 2018) “Still, whatever their religion, sexuality, racial identity, or nationality, people should have a lighter hand with their use of these identity categories in a way that would mean that moments in our cultures where conflicts arise might be somewhat defused”. Essential identities do not exist however much many people care about them and get angry when what see as their identity is not taken sufficiently seriously. Identity can only develop in interaction with others. Appiah, “Beginning in infancy, it is in dialogue with other people’s understandings of who I am that I develop a conception of my own identity” (Appiah 2007, 20). As Appiah argues identity is not an authentic inner essence but it is—in the words of Charles Taylor—dialogically constituted. “Individuality presupposes sociability” (ibidem, 20) since we are social beings as Aristotle already knew. In Appiah’s felicitous phrasing “so much we care about is collectively created” (ibidem, 20). We should understand that our individual identities have strong collective dimensions… “because they are constituted in part by socially transmitted conceptions of how a person of that identity properly behaves” (ibidem, 21). In processes of polarization, the narratives about who we are tend to be narrowed down to the stories of others who think like us and behave like we do. The collective dimension impoverishes and the dialogical construction of our identity allows the input of a limited set of voices only. There is grave danger in the frozen identities to which the so-called nationalist/populist identity politicians greatly contribute. We need to answer this polarization of dividedness with creativity and flexibility, with storytelling, theatre, music and dance. Once dividedness polarizes, it paralyzes communities and stands in the way of their resilience. With polarization, the de-escalation of conflicts becomes practically impossible because conversation is no longer possible. Polarization confronts us with the most dangerous of all fractures. Humans have managed to create a formidable enemy—Mother Gaia—and we need protection against her devastating anger. A deeply polarized human species is unable to provide this protection that needs to be based upon togetherness, thinking together and conversing together.

Existential Risk

The accumulation of the fractures into polarization causes the human species—in the beginning of the twenty-first century—to face once again deep existential risks. Those are the risks where humankind as a whole is imperilled as they imply major adverse consequences for the course of human civilization for all time to come. Risks in this category are a recent phenomenon. This is part of the reason why it is useful to distinguish them from other risks. We have not evolved mechanisms, either biologically or culturally, for managing the present risks (Bostrom 2002) that are largely “unintended consequences of radicalized modernity” (Beck 1999, 3). The concern about the extinction of the species we belong to is based on carcinogenic ingredients in food supplies, organized (cyber-)crime, pollution by poisonous materials (acid rains, chemical products), series of natural disasters (asteroids, comets, volcanoes), genetic experiments, collapse of financial markets, the scarcity of water and energy sources, infectious pandemic diseases, the consequences of genetic engineering, artificial intelligence or molecular manufacturing, or on increasing global inequalities that endanger economies and politics (Stiglitz 2013). There is the persistent risk of nuclear, chemical and biological warfare with the observation that for the first time in history weapons of mass destruction and the knowledge of how to manufacture them are available for individuals and small groups. There is also climate change, the loss of biological diversity and the largely underrated issue of overpopulation.2 The human species has survived over centuries many risks but contemporary risks have a planetary scale and “In the charged reflexive settings of high modernity, living on ‘automatic pilot’ becomes more and more difficult to do, and it becomes less and less possible to protect any lifestyle, no matter how firmly pre-established, from the generalised risk climate” (Giddens 1991, 126). As Ulrich Beck writes in the world risk society we cannot be privately insured against the risks of modernity (Beck 1999, 4) and their global interdependence. Unprecedented technological progress that provided the conditions under which the mass murders organized on an industrial scale and made possible by an efficiently organized and managed modern bureaucratic state by the Nazi’s could take place. Technical skills and organizational talent is crucial to organize massive genocide and massive addiction to industrially produced goods such as mobile telephones. Under conditions of modernity Auschwitz could happen again. The need for highly efficient coordination makes modern society very vulnerable to disruptions and on a level of global interdependence such disruptions may have global consequences. Technological advances make humans ever more dangerous, and at the same time, humanity is incapacitated to deal with such unprecedented risks as it outsources its moral responsibilities increasingly to medical, psychotherapeutic, scientific, nutrition and technical-engineering experts. Whereas the Enlightenment promised to liberate humans from the selfimposed inability to use their minds independently of others (Kant), modern life is handed over to coaches and counsellors. As “the most likely global catastropic risks all seem to arise from human activities, especially industrial civilization and advanced technologies” (Bostrom and Cirkovi´ ´ c 2008, 27) humanity has the responsibility to reflect on the unintended and unforeseen consequences of its actions. Most urgent in terms of human survival are the fractures between humans and the Earth System. In the planet’s history humanity finds itself now in a new phase: the “anthropocene”. This means that humans are with their immense and unprecedented power the most influential force in the evolutionary process. Interestingly enough the social sciences largely have refused to accept that the Earth sciences can contribute to our understanding of the world as no longer a “humans among themselves affair” (Hamilton 2017). The “humans only” focus that prevails in the social sciences leads to humans watching their own extinction as a televised spectacle that takes place outside the cubicle of their daily lives. Humans may—as the most powerful species—be at the centre of the planet but are increasingly unable to control the planet. “Our understanding of the Earth we inhabit is undergoing a radical change. The modern ideas of the Earth as the environment in which humans make their home, or as a knowable collection of ecosystems more or less disturbed by humans, is being replaced by the conception of an inscrutable and unpredictable entity with a violent history and volatile ‘mood swing’” (ibidem, 47). It is debatable whether as Pope Francis states in Laudation Si: On Care for our Common Home (Encyclical published by the Vatican, May 24, 2015) nature “is the sister that cries out to us” and “a beautiful mother who opens her arms to embrace us”. As Clive Hamilton notes “Now when Mother Earth opens her arms it is not to embrace but to crush us” (ibidem, 48). Because “Nature is no longer passive and fragile, suffering in silence” (ibidem, 48). As Hamilton argues, we no longer have to save nature but we should save ourselves from nature and from ourselves. The most existential threat is now in the fracture between the unprecedented human power to disrupt the earth system and “the uncontrollable powers of nature it unleashed in the Anthropocene” (ibidem, 49). The interesting conclusion is that we are not any longer free to treat the Earth as we please. Our enormous power comes with an unsettling moral responsibility: we no longer can choose between dominion and stewardship. We have to accept that the anthropocene is anthropocentric (ibidem, 50ff.) meaning that we have the power to change the course of the earth system. This leads to the ethical conclusion that “we must restrain ourselves and restrict what we do” (ibidem, 54). In the conflict between humanity’s unlimited desires and ambitions and the finitude of the earth system we must control the dark side of technological development. We must understand that the forces that were expected to bring us more freedom, more equality and more civilization also brought disruption of the earth system, lethal arms systems, unprecedented ubiquitous surveillance and a tweeting culture that effectively erodes whatever minimal deliberative social processes we had developed. In this moral conflict, we must explore whether our conventional ethical repertoire is adequate. Can we rely upon the will of God or our love for nature? Can we trust enlightened self-interest? Can the notion of collective public duty stand up against the solid individualism of a modern capitalist society. Will the drive towards self-preservation outlive the rampant media-induced indifference? Our future is a confrontation between humans and an unpredictable earth system. This has a certain outcome if we think we can afford indifference and an uncertain outcome—at best— if we treat an angry mother Gaia with the care she deserves. The question is whether today’s global community is capable of dealing with the existential risk of extinction. Can we constitute a global resilient community that can avoid this?

Conclusion

As Abraham Lincoln, later president of the USA, on 16 June 1858 after he had accepted the Illinois Republican Party’s nomination as that state’s US senator, famously stated “A house divided against itself, cannot stand”.3 In order to deal effectively with a formidable existential risk, we must develop communal resilience. This involves the difficulty of accepting genuine dissimilarities. It implies recognizing the other as responsible agent. It demands the critically probing of the arguments for different positions and accepting that togetherness is only possible when groups no longer monopolize the truth. And learning that fractures do not necessarily exclude “togetherness” as long they do not end in the dead alley of polarization.4

If peace is conceptualized as “celebrating moments of sheer human togetherness” and if we aspire to peaceful living together, we must overcome the great obstacle of polarized fragmentation. It may not be the fragmentation in so many different terrains on our planet that creates the essential obstacle to the cosmopolitan togetherness that is basic to collective joy. But the greater problem is that fragmentation is based upon a mindset that is characterized by the belief in singular identities, in the exclusion of alterity, in rampant individualism and in “thinking alone”. This perspective fits remarkably well in the hierarchical social orders that characterize also modern so-called democratic societies. For the conceptualization of peace as moments of collective joy, it is also important to note that such orders are antagonistic to collective festivities. “Ecstatic rituals still build group cohesion, but when they build it among subordinates – peasants, slaves, women, colonized people- the elite calls out its troops. In one way, the musically driven celebrations of subordinates may be more threatening to elites than overt political threats from below” (Ehrenreich 2007, 252).

#### Outweighs on magnitude. Polarization is a generator function for all existential risks. It’ll subvert any symptom-focused approach.

Tristan Harris & Daniel Schmachtenberger 21, Harris is the president and co-founder of the Center for Humane Technology; Schmachtenberger is a founding member of the Consilience Project, studies catastrophic and existential risk, “A Problem Well-Stated Is Half-Solved,” Center for Humane Technology, Your Undivided Attention, 6/25/21, <https://www.humanetech.com/podcast/36-unedited-a-problem-well-stated-is-half-solved>

HARRIS: So, if you think about the topics that we've covered, whether you've seen the social dilemma or you followed our interviews previously on topics like attention span shortening or addiction or information overwhelm and distraction, the fall of trust in society, more polarization, breakdown of truth, our inability to solve problems like climate change, well, this is really about an interconnected set of problems and the kind of core generator functions that are leading to all of these things to happen at once. So, I really encourage you to listen to this all the way through, and I think that we're going to get into some very deep and important knowledge that will hopefully be orienting for all of us.

One of my favorite quotes is by Charles Kettering who said that, "A problem not fully understood is unsolvable, and a problem that is fully understood is half solved." And what I hope we talk about with Daniel is, what about the framework that we are using to address or try to meet the various problems that we have has been inadequate, and what is the problem solving framework that we're going to need to deal with the existential crises that face us? So, Daniel, welcome to Your Undivided Attention.

SCHMACHTENBERGER: Thank you, Tristan. I've been looking forward to us dialoguing about these things publicly for a while.

HARRIS: Well, you and me both, and for those who don't know, Daniel and I have been friends for a very long time, and his work has been highly influential to me and many people in my circles. So, Daniel, maybe we should just start with, what is the meta crisis, and why are these problems seemingly not getting solved, whether it's the SDGs, climate change or anything that we really care about right now?

SCHMACHTENBERGER: I think a lot of people have the general sense that there is an increasing number of possibly catastrophic issues, and that as new categories of tech, tech that allows major cyber attacks on infrastructure, tech that allows weaponized drone attacks on infrastructure, biotechnologies, artificial intelligence, and moving towards AGI, that there are new catastrophic risks with all of those categories of tech and that those tech are creating larger jumps in power faster than any types of jumps of tech, including the development of the nuclear bomb in the past by many orders of magnitude.

So, there's a general sense that whether we're talking about future pandemic related issues or whether we're talking about climate change or climate change as a forcing function for human migration that then causes resource wars and political instability or the fragility of the highly interconnected globalized world where a problem in one part of the world can create supply chain issues that create problems all around the world, is that there's a sense that there's an increasing number of catastrophic risks, and that they are increasing faster than we are solving them, and that when you mention like with the UN, while progress has been made in certain defined areas of the Sustainable Development Goals and progress was made back when they were called the millennium development goals, we're very far from anything like a comprehensive solution to any of them. We're not even on track for something that is converging towards a comprehensive solution.

And, if we look at the core initial mandate of the United Nations in terms of thinking about how to, recognizing after World War II that nation state government alone wouldn't prevent world war now that world war was no longer viable because the amount of technology we had made it a war that no one could win, we still haven't succeeded at nuclear disarmament. We had some very limited nuclear disarmament success while doing nuclear arms races at the same time. We went from two countries with nukes to more countries with better nukes and that simultaneous to that, every new type of tech that has emerged has created an arms race. We haven't been able to prevent any of those. And the major tragedy of the commons issues like climate change and over-fishing and dead zones in the oceans and microplastics in the oceans and biodiversity loss, we haven't been able to solve those either.

So, rather than just think about this as like an overwhelming number of totally separate issues, the question of, why are the patterns of human behavior as we increase our total technological capacity, why are they increasing catastrophic risk, and why are we not solving them well? Are there underlying patterns that we could think of as, as you mentioned, generator functions of the catastrophic risk, generator functions of our inability to solve them, that if we were to identify those and work at that level, we could solve all of the expressions or symptoms, and if we don't work at that level, we might not be able to solve any of them?

Again, people who've been thinking about this for a long time notice these issues. They notice that you try to solve a ... The first one I noticed when I was a kid was trying to solve an elephant poaching issue in one particular region of Africa that didn't address the poverty of the people that had no mechanism other than black market poaching, didn't address people's mindset towards animals, didn't address a macro economy that created poverty at scale. So, when the laws were put in place and the fences were put in place to protect those elephants in that area better, the poachers moved to poaching other animals, particularly, in that situation, rhinos and gorillas that were both more endangered than the elephants had been. So, you moved a problem from one area to another and actually a more sensitive area.

We see this with, well, can we solve hunger by bringing commercial agriculture to parts of the world that don't have it so that the people don't either not have food or we have to ship them food? But if it's commercial agriculture based on the kind of unsustainable, environmentally unsustainable agricultural processes that lead to huge amounts of nitrogen runoff going into river deltas that are causing dead zones in the ocean, that can actually collapse the biosphere's capacity to support life faster, then we're solving for a short term issue that's important and driving even worse long-term issues. We see that many of the reasons people who oppose climate change solutions in the West, oppose them is because not because they have even really deeply engaged in the underlying science and say the climate change isn't real. That will oftentimes be what's said, but because of the solution itself seems like it'll cause problems to other areas that they're paying attention to that seem even more critical to them.

So, if the solution involves some kind of carbon tax or something that would decrease GDP for the countries that agree to it, and some other countries don't agree to it ... Let's say in this particular case, the model that many people have is Western countries agree to it. Their GDP growth decreases. China doesn't agree to it, and there's already a very, very close neck and neck fight for who controls power in the 21st century? Are we ceding the world to Chinese control that many people think it has less civil liberties and is more authoritarian in its nature? Or some people's answer to climate change is, well, we just have to use less energy, but when you understand the energy correlates directly to GDP and when GDP goes down, it affects poverty, people in extreme poverty first and worst, and wars increase because people who have desire to get more end up going zero-sum on each other, and only when it's very positive sum does that not happen. You see all these intricate theory of trade-offs, so we can't see that the problem is climate change.

Everybody knows the problem of climate change is like a big thing, but you've got to look at climate change plus the macroeconomic issues that would affect the poorest people and that would increase the chance of war and the geopolitical dynamics between the West and China, whatever, and the enforcement dynamics of international agreement. When you start to recognize that the problem is that suite of things together, in a way, it seems, well, that's too hard. We can't even begin to focus on it.

I would say that that's actually easier. Because trying to solve climate change on its own is actually impossible. Because if you're trying to solve something that is going to externalize harm to some other thing, maybe the other thing that you ... Maybe you solve that thing, but you find out that you're in a worse position. So, I would say that it's impossible to actually improve the world that way. Or half the world that is paying attention to that other thing disagrees with you so vehemently that all the energy goes into infighting, and whatever some part of the world is trying to organize to do, the other part of the world is doing everything they can to resist from happening. Then, all the creative energy just burns up as heat, and we don't actually accomplish anything.

So, I would say that the way we're trying to solve the problems is actually mostly impossible. It either solves it in a very narrow way while externalizing harm and causing worse problems, or makes it impossible to solve at all because it drives polarization. And so, going to the level at which the problems interconnect where that which everybody cares about is being factored and where you're not externalizing other problems, what seems more complex is actually possible, and possible is easier than impossible. So, it's not just that there's a lot of issues, right? There are a lot of issues and just that the issues are both more consequential at greater scope and moving faster than previous issues because of the nature of exponentiating technology. That's part of it. It's not just that the problems are all interconnected. It's also that they do have underlying drivers that have to be addressed. Otherwise, a symptomatic-only approach doesn't work.

The first underlying driver that, when people look at it, they generally see is they see things like structural perverse incentive built into macroeconomics. That the elephant dead is worth more than the elephant alive is and so as the rhino and so is the – and. So, how do you have a situation where that's the nature of incentive, where you're incentivizing an activity and then trying to bind it or keep it from happening? The same would be true with over-fishing. As long as live fish are worth nothing and dead fish are worth more, and you have ... There's something fundamentally perverse about the nature of the economic incentive. The same is true that when war goes ... When we have war and there's more military manufacturing, GDP goes up. When there's more addiction and people are buying the supply of their addiction, GDP goes up. When there are more sick people paying for healthcare cost, GDP goes up.

So, it's obviously a perverse kind of metric. So, anytime someone can fiscally advantage themselves or a corporation can, in a way that either directly causes harm or indirectly externalizes harm, we have to fundamentally solve that. If there's something like $70 trillion a day of activity happening that is a decentralized system of incentives that is incenting people to do things that are directly or indirectly causing harm, there's really nothing we can do with some billions of dollars of nonprofit or state or whatever money that is going to solve that thing. So, we have to say, well, what changes at the level of macroeconomics need to happen where the incentive of individuals and the incentive of corporations and the incentive of nations is more well aligned with the well-being and the incentive of others, and so we're less fundamentally rivalrous in the nature of our incentive?

So, we can see that underneath heaps of the problems, structures of macroeconomic incentive are there. That's the kind of maybe the first one that most people see. We can go deeper to seeing that even as an expression, because, whether it's a economic incentive for a corporation or whether it's a power incentive, a political power incentive for a political party or for a country, they're both instantiations of rivalrous-type dynamics that end up driving arms races because if you win at a rivalrous dynamic, the other side reverse engineers your tech, figures out how to make better versions, comes back, which creates an exponentiation and warfare. And eventually, exponential warfare becomes self-terminating on a finite planet. Exponential externalities also become self-terminating. So, if we want to say, what are the underlying generator functions of catastrophic risk, first, maybe just to make clear, the catastrophic risk landscape. Is this all right if we do a brief aside on that?

HARRIS: Yeah. Let's do it. Then, I think we ... Let's do that, and then let's recap just what these structures are, so people are tracking each of these components because you've already mentioned a few different things. I mean, the first thing is just, many listeners might hear what you're sharing as an overwhelming set of problems. And, I think just to recap, it's important people understand that it's overwhelming if you're not using a problem solving framework that allows you to see the interconnected nature of those problems because if you solve them with the limited tools we have now, of let's just solve the social media problem by pulling one lever and changing one business model of one company or banning TikTok, but then you get 20 other TikToks that come and sit in its place with the same perverse incentive of addiction, the same rivalrous dynamic competing for human attention, we're going to end up perpetuating those problems. So, just to sort of maybe recap some of that for listeners, and I think maybe let you continue with the other generator functions. Let's just make sure that people really get those frameworks. I think it's really important.

SCHMACHTENBERGER: Yeah. I mean, in the case that you and Center for Humane Technology have brought so much attention to with regard to the attention harvesting and directing economy, it's fair to say that it probably was not Facebook or Google's goal to create the type of effects that they had. Those were unintended externalities. They were second order effects. But they were trying to solve problems, right? Let's solve the problem, if we're Google, of organizing the world's information and making better search. That seems like a pretty good thing to do. Let's solve the problem with making it freely available to everybody. Well, that seems like a pretty good thing to do.

With the ad model, we can make it freely available to everyone, and let's recognize that only if we get a lot of data will our machine learning get better. So, we need to actually get everybody on this thing, so we definitely have to make it free. Then, we get this kind of recursive process.

Well then, the nature of the ad model doing time on site optimization and stuff I'm not going to get into because you've addressed it so well, ends up appealing to people's existing biases rather than correcting their bias, appealing to their tribal ingroup identities rather than correcting them and appealing to limbic hijacks rather than helping people transcend them. And as a result, you end up actually breaking the social solidarity and epistemic capacity necessary for democracy. So, it's like, "Oh, let's solve the search problem. That seems like a nice thing. The side effect is we're going to destroy democracy and open societies in the process, and all those other things." Those are examples of solving a problem in a way that is externalizing harm, causing other problems that are oftentimes worse. And so ... let's just focus on the opportunity and –

HARRIS: Typically, this will get accounted for as, oh, this is just an unintended consequence, but there's some other generator functions, I think, we should outline. I mean, if YouTube and Google didn't personalize search results and what video to show you next, then the other guy did, and TikTok starts personalizing, they're caught in a race to the bottom of whoever personalizes more for the best limbic hijack and so just to sort of connect some of those themes together for listeners.

# DA Answers

## Top Level

### Thumper---2AC

#### Article V’s cyber response limited now

FifthDomain Staff 17, “NATO might trigger Article 5 for certain cyberattacks,” 6/1/17, https://www.fifthdomain.com/home/2017/06/01/nato-might-trigger-article-5-for-certain-cyberattacks-cycon-tallinn/

TALLINN, Estonia — NATO will not rule out invoking Article 5 of its charter should one or more member nations find themselves under a serious cyberattack that threatens critical military and civilian infrastructure.

NATO officials told delegates at the International Conference on Cyber Conflict, or CyCon, in Estonia that the Western alliance would deliver a robust response in the event of a serious and prolonged attack on a member state in cyberspace. Article 5 provides for a united response by NATO states should a member nation come under attack.

Estonia came under a series of coordinated denial-of-service attacks in 2007 that caused serious disruption to state IT infrastructure, including military networks. The cyberattack also targeted online platforms run by the country’s leading banks, denying customers access to their accounts and basic services.

"Although many of the cyberattacks that we see fall below a level in their seriousness that could trigger NATO's Article 5, it is plausible that a cyberspace event of great magnitude could take place that might lead to the triggering of Article 5 in special circumstances," said Catherine Lotrionte, director of CyberProject at Georgetown University.

The special circumstances that could trigger Article 5 would need to be at a substantially higher threat and risk level than propaganda of social media intrusions, Lotrionte said.

"Most attacks in cyberspace use no force. We would need to have a legal threshold for such threat situations, but the triggering of Article 5 is a real possibility. There are other issues, like time factors. A grave threat would need to be current, and not an event that happened years ago," she added.

### Thumper---1AR

#### Article V gets circumvented now

Aurel Sari 19, Senior Lecturer in Law, University of Exeter; Director, Exeter Centre for International Law; Fellow, Supreme Headquarters Allied Powers Europe; Fellow, Allied Rapid Reaction Corps, “The Mutual Assistance Clauses of the North Atlantic and EU Treaties: The Challenge of Hybrid Threats,” Harvard National Security Journal, Volume 10, https://harvardnsj.org/wp-content/uploads/sites/13/2019/06/Mutual-Assistance-Clauses-of-the-North-Atlantic-and-EU-Treaties.pdf

It is important to appreciate that the bar for success in circumventing Article 5 NAT and Article 42(7) TEU is not necessarily high. The primary goal of a hybrid adversary is not to convince an expert audience that its activities do not amount to an armed attack or an act of armed aggression. Rather, its goal is to prevent the targeted state and its allies from making a compelling case that invoking Article 5 or Article 42(7) would be a lawful, legitimate, and prudent response to the threats they are facing. A plausible narrative that casts doubt on these points among domestic and international audiences might suffice to achieve that objective.278 States craft legal storylines to support their national security objectives on a regular basis.279 Although the idea that such verbal strategies are as important as military strategies may push the point too far,280 the significance of legal narratives and counter-narratives for opening up certain courses of action and for foreclosing others must not be underestimated. If anything, the progressive legalization of the conduct of foreign affairs and the vastly increased public interest in the legality of military action,281 amplified by social media,282 has boosted the impact of legal justifications. Assessing the potential vulnerabilities of the Transatlantic and European collective security arrangements from a narrow black letter perspective therefore risks misjudging their susceptibility to hostile strategic communication.

### Thumper---ILaw/Norms

#### Hybrid war forces inevitable changes to ilaw and norms---BUT ad-hoc modifications are worse than the AFF’s approach

Sascha-Dominik Bachmann and Håkan Gunneriusson 15, Bachmann is Associate Professor in International Law at Bournemouth University, UK, Gunneriusson is Associate Professor in War Studies at Swedish Defence University, “HYBRID WARS: THE 21st-CENTURY’S NEW THREATS TO GLOBAL PEACE AND SECURITY,” Scientia Militaria, South African Journal of Military Studies, Vol 43, No. 1, 2015, pp. 77 – 98, https://ung.edu/institute-leadership-strategic-studies/\_uploads/files/bachmann-gunneriusson-hybrid-wars-16-sep-2016-scientia-militaria.pdf?t=1569110400096

This article was written with the intention of making ‘hybrid threats’ as a 21st -century security threat known to the wider audience despite NATO’s decision not to adopt a comprehensive approach. This failure does not reduce the dangers of this category of global risks. Ongoing debate and academic engagement with the topic and rationale of ‘hybrid threats’, such as the Swedish experiment in 2012, will hopefully lead to further awareness and eventually preparedness. This submission concludes with a sobering prediction: it is the opinion of the authors that the present legal concepts on the use of military force, the jus ad bellum, have become relatively anachronistic and even partially outdated, something that will not suffice when dealing with the security threats and challenges of the 21st century. The authors predict that the emergence of hybrid threats and their recognition as potential threats to peace and security as such, the proliferation of low-threshold regional conflicts (such as the 2011 Libyan conflict, Syria and now Iraq), as well as continuing asymmetric warfare scenarios (such as Syria, Iraq, Afghanistan and Pakistan) will have a significant influence on the prevailing culture and prism of traditional military activity, which is still influenced by concepts from the previous century. With such a change of military doctrines, a change of legal paradigms will be inevitable: new adaptive means and methods of ‘flexible responsiveness’ through escalating levels of confrontation and deterrence will question the existing legal concept of the prohibition of the use of force with its limited exceptions, as envisaged under Articles 2(4) and 51 of the UN Charter and Article 5 of the NATO Treaty.53 Future direct intervention in failed state scenarios will require flexibility in terms of choice of military assets and objectives. Future responses to multi-modal threats will always include the kinetic force option, directed against – most likely – NSAs. They will also affect our present concepts of the illegality of the use of force in international relations, as enshrined in Article 2(4) of the UN Charter with limited exceptions available under Article 51 of the UN Charter, namely individual and collective self-defence (cf. Article 5 of the NATO Treaty) as well as UN authorisation. Already today, the continuing use of UAVs (unmanned aerial vehicles, or drones) for ‘targeted killing’ operations effectively emphasises the legal challenges ahead: the ongoing ‘kill’ operations in the so-called ‘tribal’ areas of Waziristan/Pakistan are kinetic military operations, which demonstrate how quickly the critical threshold of an armed conflict can be reached and even surpassed. These operations clearly fall within the scope of the definition of ‘armed conflict’ by the International Criminal Tribunal for the former Yugoslavia in the appeal decision in The Prosecutor v Dusko Tadic54 and therefore giving rise to the applicability of the norms of the so-called ‘Law of Armed Conflict’, the body of international humanitarian law governing conduct in war. The ‘lawfulness’ of such operations does, however, require the existence of either a mandate in terms of Article 51 of the UN Charter (in the form of a United Nations Security Council [UNSC] Resolution authorising the use of force in an enforcement and peace enforcement operation context) or the existence of an illegal armed attack in order to exercise a right to national or state self-defence in terms of Article 51 of the UN Charter. Whether such military operations are within the scope of these categories remains open to discussion.

## Deterrence DA Answers

### Deterrence DA---2AC

#### Zero link---the AFF only reduces NATO’s treaty-mandated cyber responses---voluntary coordination avoids NATO’s institutional deficits and solves

Dominick Namias & Jacob Chase 22, Helms School of Government, Liberty University, “U.S. Warfare Within the Fifth Domain: Deterring Russian Cyber Aggression,” <https://digitalcommons.liberty.edu/cgi/viewcontent.cgi?article=1267&context=hsgconference>

NATO has been primarily concerned with building up cybersecurity in member states. The next step, led by the United States, is to go on the offensive and accurately identify the sources of these cyber aggressions. On several occasions, Russia has been able to hide behind the idea that the cyber-attackers are not state-affiliated and fiend responsibility of aggressions from within the Federation:

Three successive U.S. administrations have failed to develop any form of doctrine to adequately address increasingly problematic cyberattacks from unattributable sources that plague U.S. businesses and can even endanger lives. Instead, the private sector has been left to deal with ever more destructive and dangerous ransomware attacks unassisted, and Russia continues to do nothing about cyberattacks originating from Russian territory.29

This is an epidemic that can be cured by shifting from a conservative policy regarding the cyberworld and towards a more proactive position. If the United States were able to identify actors with precision, further measures could be taken to prevent attacks on the U.S. infrastructure and on the private sector. In addition, being able to identify these actors would allow the United States and its allies to expose the perpetrators worldwide through media with solid evidence, damaging the perpetrator state’s reputation with the international community. Once the United States can present solid evidence against cyber criminals, the United States and NATO allies can voluntarily take conjoint actions against the perpetrator state/entity. This can be done through intelligence sharing, public statements of support for actions taken following an attack, and participation in the charges taken against the perpetrator state/entity. This strategy is reliant upon the ability of the United States and its allies to accurately identify perpetrators with a proactive joint campaign.

#### Zero-tolerance deterrence is not credible---cumulative deterrence is more effective for the grey zone

Whitney L. Cissell 20, MA thesis in Security Studies, Naval Postgraduate School, Army Major, Nuclear Nonproliferation Officer, March 2020, "DETERRENCE IN THE DANGER ZONE: HOW THE UNITED STATES CAN DETER RUSSIAN GRAY ZONE CONFLICT", https://calhoun.nps.edu/handle/10945/64844

2. Applying Deterrence in the Context of Russian Behavior

This section builds on the previous assessments and explores the application of deterrence theory at the sub-conventional level in the specific context of Russia as a state actor and its use of a gray zone strategy. It considers the value of tailoring a deterrent strategy against Russian gray zone conflict by supplementing conventional deterrence with “cumulative deterrence.” Recall that any deterrence strategy relies on sufficient capabilities, solid resolve, and strong communication of a threat, which in turn create credibility.225 Cumulative deterrence, elaborated in the following paragraphs, introduces the idea that credibility can be sustained across multiple encounters even if deterrence fails in certain instances, vis-à-vis classic zero-tolerance nuclear deterrence.

Regarding tailoring deterrence, Bunn writes, “If deterrence is about influencing the perceptions—and ultimately, the decisions and actions—of another party, it is logical that the requirements for deterrence will differ with each party that we might try to deter and may well differ in each circumstance or scenario.”226 Adapting deterrence to the subconventional level requires an understanding of the unique relationship between the states to identify the relative stability and instability that can inform deterrence strategy.

The stability–instability paradox applies to the nuclear and conventional level, and indeed, Russia’s effort to avoid conventional-level warfare with the United States strengthens stability between the states at the conventional level similar to the strategic nuclear level. While U.S.–Russian nuclear stability is based on parity, conventional stability in this relationship is more complex. As shown in Chapter II, Russia has a strong aversion to conflict with the United States and NATO at the conventional level. Russia would be outmatched in military superiority after two to three weeks of conflict and beyond its near abroad and, thus, prefers to operate at the sub-conventional level below the threshold of armed conflict.227 In effect, Russia’s strategy of avoiding any actions that might trigger conventional conflict aims to bolster a sort of “firewall” between conventional warfare and gray zone conflict. NATO, up to now, has effectively obliged this Russian strategy by not brandishing threats of conventional escalation in response to Russian gray zone aggression, let alone undertaking conventional responses. As much as Russia seeks to avoid escalation to conventional warfare it could not win, it is also learning how averse NATO is to threaten such escalation. This aversion is ironic insofar as Cold War–era extended deterrence relied on NATO’s threat of escalatory nuclear responses to conventional attacks.

These respective Russian and NATO postures enhance conventional stability, but at the cost of fueling instability at the gray zone level, reflecting a form of the stability– instability paradox familiar in nuclear strategies. This tailored application of the stability– instability paradox to the specific Russian context yields a tiered relationship of stability between the United States and Russia at each level of warfare, as depicted in Figure 1, and helps explain why the United States and Russia are the most unstable at the subconventional level, on which this research focuses.

Cumulative deterrence may be an option to address the issues created when adapting conventional deterrence to the sub-conventional level including the credibility and communication of the threat. Cumulative deterrence has not been a standard element of U.S. deterrence strategy in the past, and there is limited academic literature and strategic thought about its use in areas outside of cyber and terrorism. However, this new security environment characterized by great power competition at levels below open conflict requires a new way of looking at the deterrence landscape at the sub-conventional level. Subject matter experts for this research confirm that a zero-tolerance deterrence mindset will not work at the sub-conventional level and that the United States might have to choose what portions of the gray zone it wants to deter because it may be difficult to deter everything.229

There is a precedent for applying a cumulative model and mindset of deterrence to limit and shape the sub-conventional level of conflict, and this suggests it may also be applied to the current U.S. need to deter Russia’s gray zone conflict. According to Thomas Rid, cumulative deterrence “consists of a series of acts of force to create—and maintain— general norms of behavior for many political actors over an extended period. Using force, consequently, does not represent a principal failure of deterrence but its maintenance through swift, certain, but measured responses.”230 Cumulative deterrence has been a key part of Israel’s strategy for decades and was developed in the conventional and subconventional level focusing on limiting and shaping ongoing conflicts against both state and non-state actors at the conventional and sub-conventional level.231 In addition, cumulative deterrence has recently been considered for use in deterring terrorism and cyberattacks, as it is designed for long-term sustained conflict, such as competition in the gray zone.232

Doron Almong describes cumulative deterrence as functioning on two levels: the macro, which creates an image of overwhelming military superiority, and the micro, which relies on responses to adversarial actions.233 Almong also explains that cumulative deterrence has three key features.

First, its effectiveness is measured in terms of the number of victories accumulated over the duration of the conflict, which might be envisioned as “assets in a victory bank.” Second, over time, these victories produce increasingly moderate behavior on the part of the adversary and a shift in its strategic, operational, and tactical goals until there is a near-absence of direct conflict. Third, this moderation may eventually result in political negotiations and perhaps even a peace agreement.234 Almong is describing cumulative deterrence as applied to the conventional level of warfare; however, in the context of Russia, the construct can be transposed to the subconventional level. At the sub-conventional level, U.S. responses over time to Russian gray zone aggression could moderate Russian behavior, causing a shift in Russia’s decision calculus and strategic goals, thereby diminishing the conflict.

The advantage of layering a strong conventional deterrence strategy with cumulative deterrence is that it allows the restoration of deterrence over time if conventional threats fail to deter at the sub-conventional level. Over time, cumulative deterrence responses to gray zone actions bolster the credibility of the United States and alter Russia’s decision calculus at the sub-conventional level, therefore strengthening deterrence overall. Successful deterrence at the sub-conventional level requires a reorientation in how the U.S. views deterrence, moving from a zero-tolerance strategy to the long-term attrition of gray zone conflict. This renewed mindset allows for tailored punitive strategies that over time limit the bounds of the gray zone through the reiteration of unacceptable behavior through punishment. Regardless of the level at which a state wishes to conduct warfare, all deterrence strategies rely on three aspects that must work in concert: sufficient capabilities, solid credibility, and strong communication of a threat.235 As Rid explains, confrontations should be “seen as necessary evils that should be kept on as low a level as possible, but that could not be pushed down to zero.”236 This argument assumes escalation control, which is to say that the United States can control escalation at the sub-conventional level on its own terms.

Many authors challenge the notion of escalation control, claiming that it is risky and nearly impossible. Scholars claim that avoiding escalation requires deterring the action and that a policy to deter one action could in fact risk escalation to another. Additionally, scholars claim, “Escalation control or management is an inherently imperfect business. It can be done well or poorly, but it is extremely rare for any set of policies to eliminate the risk of significant escalation altogether.”237 These same scholars agree that the risk of inadvertent escalation can be reduced, but they are concerned that policy makers are incorrectly assuming it can be eliminated altogether.238 The concerns over escalation control are valid; however, it is possible to control escalation and use the threat of escalation to bolster deterrence. Mazarr explains that the gray zone puts the defender in the position to escalate, which is part of the challenge of deterrence.239 Both escalation control and deterrence fundamentally rely on communication and a thorough understanding of the adversary. Proper communication of the capability and the resolve to use the capability to deny or punish an action are just as crucial to escalation control as they are to deterrence. The same scholars who express concerns over escalation control also admit there is a way to control the risk: “Escalation depends heavily on an astute understanding of how the adversary will perceive and interpret events that have not yet occurred—not only in a general sense, but also under the specific and often difficult-to-predict conditions that will shape the opponent’s perceptions and responses when a particular event occurs.”240 The United States can both mitigate escalation and contribute to deterrence by adding an element of ambiguity to its deterrence threats that leave something to chance but also allow a response that limits or controls the escalatory response of the adversary.

When the United States responds with an instrument of state power in any DIME category, such as the expulsion of 60 Russian diplomats in response to the Russian nerve agent attack on a British citizen in 2018, it can strengthen cumulative deterrence credibility. Some of the literature on cumulative deterrence suggests that deterrence works by banking “wins” by responding to events with military power. However, when adapted to the gray zone, it seems critical that all elements of state power must be utilized, not just the military. The military is sometimes—not always—an appropriate response to an action in the gray zone, so threatening military retaliation for every tactic in the gray zone is not credible; however, a state must still have the ability to impose costs on an adversary for an action to make cumulative deterrence successful.

#### OCOs fail as a deterrence tool---it is too hard and slow to develop tools with kinetic capability.

Jeppe T. Jacobsen 21, Ph.D. candidate at the Danish Institute for International Studies and the Center for War Studies at the University of Southern Denmark, worked as cyber coordinator at the Ministry of Foreign Affairs of Denmark where he coordinated Denmark’s cyber diplomacy, “Cyber Offense in NATO: Challenges and Opportunities,” International Affairs, vol. 97, no. 3, 05/01/2021, pp. 703–720

The abovementioned incidents have led cyber-conflict scholars to point to several technical and practical difficulties in the operational integration of cyber effects.29 In the interviews and background conversations that contributed to this study, three of these difficulties were continuously reiterated when discussing successful integration of cyber effects into NATO operational planning: the temporal dimension of developing exploits; the assessment of battle damage; and the problem of confliction.

Developing exploits—a matter of time

One of the characteristics of cyber attacks that receives most attention is the fact that they hit suddenly and without warning.30 While this is often the case, the central question for operational integration is not the speed at which they hit their target, but the speed with which the tools and techniques that exploit IT vulnerabilities in order to deliver cyber effects can be developed. Like conventional weapons, the cyber tools—the exploits or cyber weapons—take time to develop. However, an exploit is often harder to reuse than a conventional weapon, as it is more dependent on a meticulous analysis and target preparation—in this case, specifically, the target’s IT infrastructure. Without knowing the adversary’s IT systems and its vulnerabilities better than the adversary itself, meaningful cyber weapons are impossible to develop.

The fact that knowledge about the target is linked not only to the deployment of a weapon but also to its development influences the extent to which it can be used and reused. Stuxnet, for example, required years of development, testing and perfecting before it could deliver the intended effect on the Iranian centrifuges. Despite the techniques used in the Stuxnet malware having been found in other malware,31 Stuxnet lost its ability to destroy the centrifuges when it was discovered and the IT vulnerabilities that enabled it were patched. Importantly, part of the complexity of Stuxnet relates to the US–Israeli intention to keep the effect secret. In a hot conflict, secrecy in terms of the effect is often less important, and thus the development and deployment of cyber effects do not necessarily have to be as complex and time-consuming.

This observation does not necessarily change the fact that the development of exploits often has to precede the military confrontation in which they are intended to be used. NATO states that want to deliver cyber effects in NATO operations must try to gain access to Russia’s or other potential adversaries’ critical military networks to identify and exploit IT vulnerabilities. As several informants emphasized, if states wait for a conflict to escalate before they begin the development of exploits, it is most likely to be already too late.32

The alternative to penetrating adversary networks in peacetime is for states to rely on the exploitation of vulnerabilities in as many commercial off-the-shelf products as possible. This can be done, for example, by purchasing exploits from private companies offering this service, in the hope that it will then be possible to quickly create an overview of the enemy’s IT infrastructure and adapt the exploits to this environment when a conflict escalates. The latter approach is more likely to succeed against adversaries with low network security, which does not apply in the case of Russia, or in contexts where less sophisticated and less closely targeted cyber effects are required.

Whether member states develop sophisticated exploits for future targeted effects or stockpile well-known exploits to cause more minor effects, they cannot—as several informants indicated—be certain that they will be able to deliver the cyber effect at the specific time it is requested by CYOC. This is because the IT vulnerabilities upon which exploits depend might not exist for ever. Cyberspace is a dynamic environment: vulnerabilities are patched, systems are updated or replaced and bad IT security practices are identified and improved. This means that exploits are temporary in nature and cannot be stored for later use.33 States must constantly ensure that the exploits still work, which requires minor adjustments when updates take place. As a consequence, the larger the military ‘cyber arsenal’, the more technically skilled human resources are needed for its maintenance. In the current labour market, where recruitment and retention of a cyber workforce is difficult, extensive investment is required for states to be able to stand ready with cyber effects available when requested.

In short, if a state is to offer a cyber effect in a NATO operation, then the state is likely to have to be able, first, to predict what Russian IT systems it is going to target months or years in advance, and second, to marshal the necessary resources to develop and maintain a large array of exploits that can be used against these systems. Even if this is successfully done, the state still faces difficulty in ensuring that an effect is delivered as promised.

#### Integrating cyber activities won’t contribute to conventional deterrence.

Jeppe T. Jacobsen 21, Ph.D. candidate at the Danish Institute for International Studies and the Center for War Studies at the University of Southern Denmark, worked as cyber coordinator at the Ministry of Foreign Affairs of Denmark where he coordinated Denmark’s cyber diplomacy, “Cyber Offense in NATO: Challenges and Opportunities,” International Affairs, vol. 97, no. 3, 05/01/2021, pp. 703–720

Deterring what?

Much of the scholarly debate on NATO is preoccupied with the current strategic adaptation of the alliance and the renewed focus on deterring Russia.48 Only a few contributors to this debate have addressed the addition of offensive cyber capabilities in NATO force structure and response doctrine as an element in work to strengthen the alliance’s deterrence posture.49 Neither in these contributions nor among the former and current NATO employees who have publicly articulated this ambition is it clear what kind of activity the integration of cyber effects in NATO seeks to deter.50 Is it supposed to add to the classical deterrence (through the threat of punishment) of conventional Russian threats to the territorial integrity of eastern Europe? Or to the deterrence of hybrid activities—specifically cyber activities—against allied countries below the threshold of armed conflict? This section addresses each of these possibilities in turn.

From Cold War deterrence and back

NATO’s founding purpose was to maintain a sufficient military strength to deter aggression and attempts at coercion, to prepare for the eventuality of deterrence failing, and to ensure stability among European powers.51 During the Cold War, the debates over NATO deterrence posture largely centred on the role of nuclear weapons, and specifically whether the United States would retaliate with these weapons in the event of a Soviet conventional attack against allied states.52 In short, NATO deterrence was about credibly extending the US nuclear (as well as conventional force) deterrence to allies to discourage a Soviet military offensive into eastern Europe.

While NATO and its member states adapted to the new security environment after the end of the Cold War by scaling down the military investments and presence in eastern Europe and by focusing more on crisis management,53 much of the Cold War deterrence language returned when the Russian–Ukrainian conflict broke out in 2014.54 What needs to be deterred today, much of the literature agrees, is not only a full-scale military invasion but to a larger extent the use and support of pro-Russian militant separatists who are willing to apply insurgency tactics in NATO’s post-Soviet member states.55 As a result, the allies’ military investments have been increasing again,56 a number of initiatives such as the Enhanced Forward Presence in the Baltic States and Poland have been introduced,57 and the discussions—and disagreements—on the nuclear deterrence (of non-nuclear threats) have re-emerged.58 Such responses are often presented as a renewed attempt by NATO to reassert its deterrence and assurance posture by signalling strength, preparedness and willingness to punish ‘bad’ behaviour.59

At first sight, the introduction of CYOC seems to add to these deterrence efforts. NATO added an offensive cyber option to reinforce its ability to impose costs sufficient to dissuade adversaries from acting aggressively. On closer examination, however, it is not self-evident that requesting member states’ delivery of offensive cyber effects in NATO operations constitutes a necessary or even a substantial addition to credibly signalling the ability and willingness to punish an adversary. NATO’s conventional capabilities are clearly already far superior to Russia’s—with or without fully integrated cyber effects. Thus, a deterrence failure, resulting for example in a scenario in one of the Baltic states similar to that which occurred in eastern Ukraine, will not be the result of NATO’s lack of available cyber tools in its military toolbox; rather, if the Russian leadership were to consider it in its interest to pursue such a scenario, it would mean that Russia’s decision-makers did not believe in the credibility of NATO’s article 5 or in NATO’s ability to mobilize its forces. The capacity to integrate cyber effects would do nothing to change that.

Furthermore, if the establishment of CYOC is an attempt to signal defensive strength and unity in cyberspace, it remains difficult to imagine that such signalling would dissuade adversaries from trying to penetrate NATO and allied systems. CYOC does not change the fact that NATO is not tasked to govern and secure national IT systems. In an operational setting, states might connect to each other through so-called federated mission networking; 60 but there is no tradition of ceding control of the deployed national networks to NATO during military operations. Hence, CYOC can only realistically seek to become a hub for cyber-threat information-sharing and to support states’ coordination and synchronization of various national responses to these threats. In other words, CYOC is unlikely to become an active defender in cyberspace that causes doubt in the adversary’s evaluation of its own cyber capabilities. This also means that even if CYOC’s coordination and information-sharing efforts manage to contribute to the denial of intrusions into allied systems, an adversary’s military is unlikely to be deterred from trying to hack these systems. In fact, actively articulating that CYOC is supposed to deter (through denial) a perceived adversary such as Russia from hacking NATO and allied operational systems creates an incentive to do just that and thereby show that the alliance is incapable of doing what it says it seeks to do.

#### Strategic ambiguity spurs escalation in cyberspace specifically because it’s an offense-dominant domain---norms solve

Mariarosaria Taddeo 19, Fellow in Cyber Security and Ethics in the Department of Politics and International Studies at the University of Warwick and Research Associate at the Uehiro Centre for Practical Ethics, University of Oxford, UK, “Norms and Strategies for Stability in Cyberspace,” Chapter 3 in “The 2019 Yearbook of the Digital Ethics Lab,” edited by Christopher Burr and Silvia Milano, https://link.springer.com/chapter/10.1007/978-3-030-29145-7\_3

Escalation follows from the nature of cyber attacks and the dynamics of cyberspace (Floridi and Taddeo 2014a, b; Taddeo 2014a, 2016, 2017). Non-kinetic cyber attacks—aggressive uses of information and communications technologies that do not cause destruction or casualties, e.g. Distributed Denial of Service (DDoS) attacks—cost little in terms of resources and risks to the attackers, while having high chances to be successful, e.g. impairing the services of targeted server or website. At the same time, cyber defence is porous by its own nature (Morgan 2012): every system has bugs in the program (vulnerabilities), identifying and exploiting them is just a matter of time, means, and determination. This makes even the most sophisticated cyber defence mechanisms ephemeral and, thus, limits their potential to deter new attacks.

Even when successful, cyber defence does not lead to strategic advantages, insofar as dismounting a cyber attack, may bring tactical success, but very rarely leads to the ultimate defeating of an adversary (Taddeo 2017). This creates an environment of persistent offence (Harknett and Goldman 2016), where attacking is tactically and strategically more advantageous than defending. As Haknett and Goldman argue, in an offence-persistent environment, defence can achieve tactical and operational success in the short term if it can adjust constantly to the means of attack, but it cannot win strategically. Offence will persist and the interactions with the enemy will remain constant. This is why inter-state cyber defence have shifted from reactive (defending) towards an active (countering) defence strategies.

In this scenario, state actors make policy decisions to protect their abilities to launch cyber attacks. Strategic ambiguity is one of these decisions. According to this policy, states decide neither to define nor to inform the international community about their red lines—thresholds that once crossed would trigger state response— for non-kinetic cyber attacks (Mariarosaria Taddeo 2011). This approach leaves de facto unregulated cyber attacks that remain below the threshold of an armed attack. Strategic ambiguity has often been presented as a way to confuse the opponents about the consequences of their cyber attacks. As the US National Intelligence Officer for Cyber Issues officer put it:

Currently most countries, including ours, don’t want to be incredibly specific about the red lines for two reasons: You don’t want to invite people to do anything they want below that red line thinking they’ll be able to do it with impunity, and secondly, you don’t want to back yourself into a strategic corner where you have to respond if they do something above that red line or else lose credibility in a geopolitical sense.6

By fostering ambiguity, state actors also leave open for themselves a wider room for manoeuvring. Strategic ambiguity allows state actors to deploy cyber attacks for military, espionage, sabotage, and surveillance purposes without being constrained by their own policies or international red lines. This makes ambiguity a dangerous choice, one that is strategically risky and politically misleading.

The risks come with the cascade effect following the absence of clear thresholds for cyber attacks. The lack of thresholds facilitates a proliferation of offensive strategies. This, in turn, favours an international cyber arms race and the weaponization of cyberspace, which ultimately spurs the escalation of cyber attacks. This is why strategic ambiguity is a policy hazard that fuels, rather than arrests, escalation of interstate cyber attacks. Cyber attacks would be deterred more effectively by a regime of international norms (defining proportionality criteria for responses, setting red lines, and procedure for accountability, and for capability building) that makes attacks politically costly to the point of being disadvantageous for the state actors who launch them.

As I mention in Sect. 3.1, stability of cyberspace hinges on both regulations and strategies. Having considered the limits of the existing approaches to the regulation of state behaviour in cyberspace, I shall now focus on existing view for the designing deterrence strategies for cyber attacks.

### Deterrence DA---AT: OCOs Good

#### Mistrust and uncertainty means deterrence fails now---AFF enables OCO effectiveness

Patrik Maldre 16, Adjunct Fellow at the Center for European Policy Analysis (CEPA), where he leads the CEPA Cyber Defense Initiative, “Moving Toward NATO Deterrence for the Cyber Domain,’ Center for European Policy Analysis, Cyber Intelligence Brief No. 1, May 2016, https://cepa.ecms.pl/files/?id\_plik=2446

Deterrence aims to discourage an adversary from taking offensive action. Traditionally, its two pillars have been deterrence-by-denial and deterrence-by-punishment. The first refers to measures that reduce or eliminate the benefits of a certain aggressive move, while the second seeks to impose additional costs for performing it. NATO’s traditional mandate of defending its own systems fits comfortably into the deterrence-by-denial part of this framework. Deterrence-by-punishment, however, is far more controversial because of the problem of attribution—which refers to the difficulty of identifying the perpetrators of operations. Finally, both concepts also rely on intent, capability and credibility. As it stands, a palpable lack of trust among member states hinders collective action on both fronts. Progress in the denial category will be easier and more visible, but countermeasures should be considered as well.

NATO has come a long way in terms of working together to shore up technical defenses in cyberspace. The main barrier to further cooperation, however, is the difference in technical and administrative capacities as well as human and financial resources among member states. This, along with differing national views, remains the main barrier to further integration. The alliance is only as strong as its weakest member. When it comes to deterrence-by-denial, therefore, all member states must have the basics in place: computer security laws, national cyber strategies, a police focus on cybercrime, national CERTs, public-private partnerships and capable intelligence agencies. From there, members should enact effective, actionable information-sharing programs. After that, the next step is to develop joint situational awareness. Typically, adversary espionage campaigns target multiple NATO and memberstate organizations simultaneously. Early warning and shared situational awareness can prevent multiple entities in different countries from being breached by the same operation. The end goal for the denial part of the deterrence strategy is, of course, resilience. If NATO and its members can effectively work together to prevent, detect, respond and recover from cyber attacks, this would significantly decrease the benefits and increase the costs for an adversary. NATO collective action should continue in this direction, and joint efforts can help to promote trust and confidence—a key ingredient in further cooperation in deterrence-by-denial, but even more crucial when it comes to deterrence-by-punishment.

Preventing adversaries from benefitting from offensive actions, or at least limiting their gains, can help discourage them from conducting such attacks in the first place. Punishing them after the fact is another. While the term has an aggressive connotation, this part of the strategy is defensive and retaliatory in nature. It can refer to a broad spectrum of actions—from naming-and-shaming to nuclear strikes. In the cyber domain, the problem of attribution hinders the goal of effective deterrence. For this reason, NATO and its member states should invest heavily in the technological and analytical capabilities necessary to discern signs of a particular adversary, including in cooperation with the private sector.

As numerous cases of attribution to Russian cyber threat actors demonstrate, this is already taking place. Furthermore, member states should complement technical attribution with political and diplomatic attribution. Currently, months and even years pass before politicians and leaders feel comfortable about ascribing blame. For deterrence to work, however, governments must carry out both high-level and private attribution in conjunction with media and private companies as soon as they have conclusive evidence. Calling out threat actors and their state sponsors in diplomatic forums, public discussions and private meetings can motivate them to conduct less aggressive operations.

NATO and its member states should also adopt joint approaches to developing and employing offensive capabilities for collective defense purposes. Laudably, many individual allies have already declared that they possess such capabilities and the doctrines for using them. However, considerable mistrust persists among the allies, creating an atmosphere of uncertainty and doubt—which weakens deterrence as a whole. To overcome this hurdle, allies can begin by making political statements about potentially using these capabilities in case of attack, and in accordance with international law as part of a collective defense response. Ultimately, NATO should move toward sharing these capabilities, perhaps by using existing models based on nuclear doctrine. Transparency and straightforwardness in this arena could contribute substantively to deterring adversaries and reinforce collective defense among NATO members.

Intent and credibility will play into adversaries’ calculations for any type of countermeasure. For this reason, policy innovations and capability development need to be complemented by effective strategic communication. You cannot achieve deterrence if your adversary doubts that you’ll do what you say— and even less so if it doesn’t think you can do what you say. From this perspective, demonstrations such as the Aurora test in 2007 can be quite useful.21 Other, more subtle means include presentations by top officials at security conferences. Operations against third-party adversaries other than the intended target of deterrence can also deter attacks; few doubt that Russia paid close attention to the Stuxnet case, or that NATO drew conclusions from the Ukraine grid attack. In sum, effective strategic communication— both public and private—can be a key component or complement of a deterrence-by-punishment strategy.

### Deterrence DA---AT: Revisionism

#### If Russia is revisionist deterrence inevitably fails and creates a self-fulfilling prophecy that risks war

CATO 20, “Security Threats in Contemporary World Politics: Potential Hegemons, Partnerships, and Primacy,” CATO Institute, 5/6/20, https://www.cato.org/publications/publications/security-threats-contemporary-world-politics-potential-hegemons

The Dangers of American Alliances

Primacy poses more dangers than simply failing to achieve its goals. Failed regional management may well induce American policymakers to fight, either to end the wars they could not prevent or for other reasons. Here, I highlight two considerations that might drive such a decision: (a) concerns about the credibility of American commitments and (b) expanding definitions of American core interests.

Primacy depends heavily on credibility: the belief among interested actors that, in the final reckoning, the United States will go to war to protect the status quo it has promised to defend. A related important belief is that the United States will go to war only to protect the status quo it has promised to defend. A primacy strategy engages in a combination of “extended” and “pivotal” deterrence: it aims to convince revisionists of all stripes of American willingness to punish those who seek to overturn the status quo.

As discussed earlier, the world with revisionist states motivated enough to make primacy useful will also be one where American credibility is open to question. Offensive realist states will be motivated by a view of uncertainty that sees alliances as often unreliable alternatives to self‐​help. States with non‐​security motives will have good reason to believe that they hold the balance of resolve on non‐​security issues far from American shores. In either case, there will be ample reason for risk‐​acceptant revisionist states to consider gambling against American intervention.

To be clear, revisionists would not be doubting U.S. capabilities, although clever diplomatic and military strategies might lead them to believe they could temporarily revise the status quo. Rather, revisionists would doubt that America’s interests were large enough to justify the costs of war. Daryl Press, who generally emphasizes the decisive influence of power considerations in deterrence decisions, argues that “adversaries will doubt whether the United States will take costly actions to defend interests of secondary or tertiary importance.” A good historical example is the German military’s view of the Anschluss. Even though senior Wehrmacht officers believed that Britain and France could intervene and defeat Germany during an invasion of Austria, they endorsed Hitler’s plans, largely because they doubted that the Western powers would risk war over the unification of German speaking peoples in one country.37

In the event that deterrence fails, what will Washington do when faced with a challenge to the status quo? There is good reason to believe that policymakers will follow through on their commitments, even though the costs of war may be quite disproportionate to American stakes in the issue under dispute. After all, wouldn’t a failure to defend the status quo reveal the entire primacy strategy to be a bluff? Revisionist states might be expected to draw that conclusion, no matter how the United States framed the situation. One does not need to believe that states carefully monitor each other’s past actions in order to draw inferences about likely future behavior to credit that notion. Backing down over a commitment might clarify for many interested parties American interests in defending other commitments—all far from U.S. shores and protecting interests far more important to others than to Washington— that look just like it.

Regardless of whether revisionist states make such inferences, it is crystal clear that American decisionmakers believe they do. Harry Truman’s decision to intervene in Korea was driven by the belief that the Soviet Union would draw inferences about American willingness to fight. “If we let Korea down,” Truman argued, “the Soviet will keep right on going and swallow up one piece of Asia after another. If we were to let Asia go, the Near East would collapse and no telling what would happen in Europe.” Conversely, “if we are tough enough now, if we stand up to them like we did in Greece three years ago, they won’t take any next steps.”38 The American commitment in Vietnam hinged on credibility concerns as well, especially with regard to what its allies in the North Atlantic Treaty Organization would think. Lyndon Johnson believed that escalation was required because “to leave Vietnam to its fate would shake the confidence of all these people [i.e., other U.S. allies] in the value of an American commitment.” Richard Nixon believed he had to stay in Vietnam because “the cause of peace might not survive the damage that would be done to other nations’ confidence in our reliability.” And John Kennedy was willing to risk nuclear war in the Cuban missile crisis because “for us to fail to respond would throw into question our willingness to respond over Berlin.”39

### Deterrence DA---AT: Hybrid Impact

#### OCOs are terrible at deterring hybrid activities

Jeppe T. Jacobsen 21, Ph.D. candidate at the Danish Institute for International Studies and the Center for War Studies at the University of Southern Denmark, worked as cyber coordinator at the Ministry of Foreign Affairs of Denmark where he coordinated Denmark’s cyber diplomacy, “Cyber Offense in NATO: Challenges and Opportunities,” International Affairs, vol. 97, no. 3, 05/01/2021, pp. 703–720

Deterring cyber activity below the threshold of collective defence

‘Hybrid’ has become a popular concept when describing the current threat environment. While discussions over the definition, novelty and usefulness of the concept continue, there seems to be agreement that, when used to qualify ‘threat’ or ‘warfare’, ‘hybrid’ refers to the blurring of the distinction between military and civilian, often in relation to the mixture of instruments used to obtain political objectives.62 NATO’s attempt to deter military and paramilitary instruments from being deployed has already been touched upon above. As a primarily military alliance, however, NATO is facing difficulty in addressing the instruments that are used deliberately to stay below the threshold of collective defence.

NATO has not been able to deter the perpetration of random ransomware incidents, election interference and targeted propaganda campaigns through hacks and leaks, or industrial cyber espionage and intrusion into critical infrastructures. The alliance’s conventional capabilities are not credible (proportional) responses to such malicious cyber activity. Thus, it has responded only by ‘naming and shaming’, and by expressing encouragement to member states to enhance the resilience of their networks.63 These responses, however, have yet to prove effective in halting the malicious cyber activity conducted below the threshold of collective defence.64 And the introduction of SCEPVA is not likely to change that; the integration of cyber effects is tied to NATO military operations only. While NATO member states are already compelled to maintain a level of cooperation in collective defence (article 3), and to consult together whenever any of them feels that its territorial integrity, political independence or security is threatened (article 4), NATO—with or without integrated cyber effects—is not an alliance designed to deal with non-military threats from a peer competitor.

### Deterrence DA---AT: Signaling

#### Civilian leaderships are terrible at using cyberweapons for political signaling because they don’t understand their military context or operational effects.

Erica Longergan & Keren Yarhi-Milo 22, Lonergan is an assistant professor in the Army Cyber Institute at West Point and a research scholar at the Arnold A. Saltzman Institute of War and Peace Studies at Columbia University; Yarhi-Milo is the Arnold A. Saltzman Professor of War and Peace Studies in the political science department and the School of International and Public Affairs, “Cyber Signaling and Nuclear Deterrence: Implications for the Ukraine Crisis,” War on the Rocks, 4/21/22, <https://warontherocks.com/2022/04/cyber-signaling-and-nuclear-deterrence-implications-for-the-ukraine-crisis/>

Civil-Military Relations and the Risks of Cyber Signaling in Nuclear Crises

But what if a state, such as the United States, wanted a cyber operation to be visible to an adversary, such as Russia, during a nuclear crisis — in other words, to send a cyber signal?

Signaling is essential for coercive diplomacy and international crises because it helps states convey their intent to one another. The civil-military relations literature has found that civilian (rather than military) leaders are more inclined to use military force as a form of signaling, rather than for operational effect.

Why does this matter? When civilian and military leaders have different views, civilians could make decisions around using military force for signaling purposes in a way that exacerbates ongoing crises. For instance, writing about Cold War nuclear crises, Scott Sagan has shown that civilian decision-makers have made crises more dangerous by taking actions without fully understanding the military implications and risks of inadvertent escalation. Jack Levy, writing about the causes of World War I, discusses how, during the July Crisis preceding the outbreak of war, civilians saw military mobilization as a political tool for coercive diplomacy, whereas military leaders, who were focused on the operational implications, perceived mobilization as a means of preparing for imminent war.

Differences in how civilian and military leaders see the use of military power are likely to be even more salient in cyberspace, for three reasons. First, cyberspace is a highly technical environment where civilians typically lack subject matter expertise. Practitioners are likely to have far more up-to-date operational experience and, therefore, fluency with the technical issues and constraints posed by cyber operations than civilian leaders (even those with prior and, potentially, outmoded experience). Cyberspace is also a highly classified environment — one in which information is highly segmented and only accessible to a select group of individuals. Therefore, some civilian officials may not be privy to all of the details surrounding cyber operations. Finally, unlike other technical and secretive environments, cyberspace has an additional element that makes it even more difficult for non-experts to grasp its nature. Specifically, cyberspace is also an esoteric environment; cyber operations and their effects are not easily visible in a way that other types of military capabilities are, making it difficult to conceptualize their utility in a tangible manner.

There is evidence supporting this idea. For instance, senior civilian leaders across multiple U.S. administrations, as well as in Congress, typically describe cyber operations as useful for signaling deterrence and resolve. Chris Inglis, the Biden administration’s inaugural National Cyber Director, described how he’d “like to change the decision calculus of those who transgress in this space,” and contemplated that “[p]erhaps our actions should be felt by an adversary. They should know that they have just felt the hand of whomever.” Similarly, Senator Angus King, discussing the threat of Russian-linked ransomware attacks in the summer of 2021, noted that he wants “somebody … in the Politburo to say, ‘Gee, boss, I’m not sure we ought to do this because we’re liable to get whacked in some way by those Americans.’”

John Bolton, former national security advisor under President Donald Trump, in multiple public statements, has depicted the purpose of U.S. cyber operations — especially offensive ones — as a means of influencing adversary perception. He described how the employment of offensive cyber power creates “structures of deterrence, so that it’s publicly known,” and that “it is important that our adversaries know [that] …we have authorized offensive cyber operations to … demonstrate to our adversaries that the costs of engaging in operations against us is higher than they want to bear.” Michael Daniel, the Obama administration’s cyber czar, depicted the purpose of imposing costs on Russia in response to its 2016 election interference as “to openly demonstrate that we could do it as a deterrent and also clandestinely disrupt their operations as well.”

In contrast, while some military leaders do talk about cyber deterrence, the language they employ is anchored in tactical and operational objectives, rather than aiming to influence adversary perception and decision-making. This is evident in how both civilian and military leaders use the language of “imposing costs.” Military leaders tend to describe cost-imposition as supporting the disruption, degradation, denial, or destruction of adversary offensive capabilities and operations. For instance, in December 2021, Gen. Paul Nakasone, commander of U.S. Cyber Command and director of the National Security Agency (NSA), described “imposing costs” against Russian-linked ransomware groups as the goal in itself. The month prior, at the November 2021 Aspen Security Forum, he argued for the United States to impose costs in cyberspace, but stated that a traditional deterrence strategy “does not comport to cyberspace.” In another example, in 2019, Lt. Gen. Stephen Fogarty, commander of Army Cyber Command, voiced skepticism about cyber deterrence in remarks about defending the 2020 elections against cyber interference, noting that “I don’t know of a single thing we could do that would prevent [adversaries] from competing, but I want to impose as much cost on them as possible.”

#### Cyber signaling fails and makes wars worse.

Erica Longergan & Keren Yarhi-Milo 22, Lonergan is an assistant professor in the Army Cyber Institute at West Point and a research scholar at the Arnold A. Saltzman Institute of War and Peace Studies at Columbia University; Yarhi-Milo is the Arnold A. Saltzman Professor of War and Peace Studies in the political science department and the School of International and Public Affairs, “Cyber Signaling and Nuclear Deterrence: Implications for the Ukraine Crisis,” War on the Rocks, 4/21/22, <https://warontherocks.com/2022/04/cyber-signaling-and-nuclear-deterrence-implications-for-the-ukraine-crisis/>

Implications for the Ukraine Crisis and Beyond

What are the implications of this for the current Ukraine crisis? Thus far, while cyber operations have been used on both sides of the conflict, they have not played a decisive role on the battlefield. So far, the United States has been focused on providing cyber defense support to Ukraine and NATO, reportedly to include dispatching Cyber Command’s cyber mission teams to Eastern Europe, as well as seeking to deter potential Russian cyber retaliation in response to U.S. and Western sanctions, especially attacks on U.S. critical infrastructure.

However, if the nuclear dimension of the crisis becomes more acute, policymakers may be tempted to turn to cyber operations to signal resolve to deter Russia in the nuclear domain. Such an approach could be seen as particularly appealing precisely because cyber operations are not kinetic and, therefore, less dangerous than other military moves. But this could have the inverse effect of making nuclear escalation, rather than deterrence, more likely, for the following reasons.

In 2020, Russia clarified its nuclear declaratory policy to state that Russia reserves the right to use nuclear weapons under a range of contingencies, including an adversary attack against “critical governmental or military sites of the Russian Federation, disruption of which would undermine nuclear forces’ response actions.” Cynthia Roberts has suggested that this particular scenario “likely include[s] cyber attacks against command and control infrastructure and/or attempted leadership decapitation.” Similarly, Dmitry Stefanovich wrote that “[t]here is a wide consensus within the Russian expert community that this also includes possible cyber threats as well as other non-nuclear dangers.” Interestingly, Russia’s declaratory policy contains parallels to the implicit link between cyber attacks and nuclear use contained in the 2018 U.S. Nuclear Posture Review. That document notes that the United States would consider using nuclear weapons under “extreme circumstances,” including “significant non-nuclear strategic attacks … [such as] attacks on U.S. or allied nuclear forces, their command and control, or warning and attack assessment capabilities.”

Therefore, a hypothetical attempt by the United States to conduct a cyber operation against Russian nuclear command, control, and communication systems for signaling purposes, such as to demonstrate resolve or convey a desire to deter the use of nuclear weapons could in practice make their use more likely. Unlike most cyber operations, which rely on secrecy, signals are meant to be seen. And to be sufficiently credible, this kind of cyber operation would have to demonstrate an ability to cause a meaningful effect against Russia’s nuclear systems, rather than a low-cost, unsophisticated cyber operation. Therefore, assuming such an attack were feasible, the chances are greater in this scenario that Russia could interpret U.S. cyber signals as an attack against its critical military systems.

### Deterrence DA---UQ

#### NATO is unable to respond to Russian grey zone threats – decision making time is too slow

Steve MacBeth 20, retired officer from the Canadian Forces and former Battle Group Commander of the NATO enhanced Forward Presence Battle Group in Latvia, 11/25/20, Targeting North Atlantic Treaty Organization Article 5: Assessing Enhanced Forward Presence as a Below War Threshold Response, https://www.realcleardefense.com/articles/2020/11/25/targeting\_north\_atlantic\_treaty\_orga[…]d\_presence\_as\_a\_below\_war\_threshold\_response\_651003.html

Author and / or Article Point of View:  The author believes that the North Atlantic Treaty Organization’s (NATO) Article 5 does not provide the agility for forward deployed forces to effectively respond to challenges below the threshold of war. These challenges are also known as Grey Zone activities. This paper is a summation of a chapter the author wrote for publication at the NATO Staff College in Rome, regarding NATO in the Grey Zone, which was edited Dr Howard Coombes, Royal Military College of Canada.

Summary:  Russia has been careful, for the most part, to avoid direct confrontation with NATO. The Russian focus on indirect mechanisms targets the weaknesses of NATO’s conventional response and highlights the requirement to revisit Article 5 within context of the deployed enhanced Forward Presence Activities. Conflict through competitive and Grey Zone activities is omnipresent and does not follow the template that Article 5 was designed for[1] .

Text:  U.S. Army Major General Eric J. Wesley, Commander, U.S. Army Futures Command, has noted that western militaries and governments may need to adjust between a “continuum of conflict” that denotes “war” and “peace” to an age of constant competition and covert pressure punctuated by short violent overt struggle[2]. The Chief of the Russian General Staff, General Valery Gerasimov reflected upon this approach for the Russian military journal VPK in 2013. “Methods of conflict,” wrote Gerasimov, have changed, and now involve “the broad use of political, economic, informational, humanitarian and other non-military measures.” All of this, he said, could be supplemented by utilizing the local populace as a fifth column and by “concealed” armed forces[3]. These actions demonstrate a Russian philosophy of achieving political objectives by employing a combination of attributable/non-attributable military and other actions. Operating under the threshold of traditional warfare, these adversarial behaviours, known as Grey Zone activities, deliberately target the weaknesses of the traditional NATO responses.

Reactions to aggression are governed by Article 5 of the North Atlantic Treaty. Article 5 provides the Alliance’s collective defence paradigm, stating an “attack on one is an attack on all,” signaling the shared intent to deal with armed aggression vigorously[4]. Article 5 does not address Grey Zone activities that demand rapid, unified decision making and action. NATO crisis response is predicated on a system that acts in a predictable and deliberate manner to deal with overt aggression. Though NATO has recognized the Grey Zone there has been little adaption to this threat and NATO has not demonstrated that it is prepared to act decisively in the case of a Russian Grey Zone incursion. The NATO forces positioned to deter potential Russian aggression on the Alliance’s eastern flank are the enhanced Forward Presence (eFP) battle groups. This military commitment is structured and authorized to counter overt Article 5 threats. Paradoxically, the most likely danger they may encounter are Grey Zone challenges. Combine this capability to likely threat mismatch with the speed at which political and military decisions are required during crisis, like a limited Russian incursion with pre-conditions set by Grey Zone actions, and NATO may not be able to react effectively. Consequently, it may be time for NATO to re-visit its current Article 5 deterrence activities, in the context of Grey Zone activities. This re-visit would acknowledge the Eastern NATO nations require every opportunity to answer any form of threat to their security and fully enable the NATO forces arrayed within their countries.

Presently, the enhanced Forward Presence is an ‘activity’ and not an NATO mission. The forces remain under national control for all, but specifically pre-agreed tasks and lack common funding resources. For all intents and purposes NATO missions, with the exceptions of “operational limitations,” indicating national caveats or activities in which a contributing nation will not participate, contribute to a single military force under a unified NATO command structure. In the eFP context, this unified command structure does not exist. Outside of an invocation of an Article 5 response, the various elements of the eFP battle groups remain under national command. The Russian determination of conflict leans towards a state of constant, below the threshold of war competition utilizing deception, information, proxies, and avoiding attributable action. Russian efforts are focussed on NATO’s greatest vulnerability and, at times, source of frustration, lengthy centralized deliberation. At the best of times this need for consensus creates slow decision making and resultantly a diminution of strategic, operational, and tactical agility[6]. If the Russian trend of Grey Zone actions continue, Article 5 responses by the Alliance may become irrelevant due to this slowness of decision making. For the eFP battlegroups, which can react to conventional threats, the Grey Zone poses difficult challenges, which were not fully recognized when the eFP concept was originally proposed and implemented[7].

The Baltic countries are strengthened by having eFP forces garrisoned within their nations, but there is a capability gap in providing Article 5 deterrence. The lack of authority for eFP battle groups to compete below the threshold of conflict leaves Baltic allies uncertain if and how NATO can support them. Enhanced Forward Presence battle groups are not currently able to deal with Grey Zone eventualities. Consequently, in several important aspects, the Alliance response remains handicapped. Bringing about achieving rapid consensus for a crisis response operations in the face of an ambiguous attack, or in response to ostensibly unrelated low-level provocations, like those imbued in the Grey Zone, will not be an easy task in the current framework[8].

#### Crimea and Ukraine prove

Peter Grier 17, Washington, D.C., editor for the Christian Science Monitor, is a longtime defense correspondent and a contributing editor to Air Force Magazine, “The Perils of Hybrid War,” Air Force Magazine, 1/30/17, https://www.airforcemag.com/article/the-perils-of-hybrid-war/

Is This War

NATO worries that hybrid war can inch toward a geopolitical objective while remaining under the threshold for Article 5, which triggers collective armed defense of a threatened member.

Russia’s incursion in Crimea and Ukraine is a case in point. It was rooted in the Russian determination that blocking Ukraine’s further economic and political integration into Europe was a vital interest.

It began with misdirection. As protests roiled Ukraine in early 2014, Russia mounted a large military exercise within striking distance of the Ukraine border. This distracted the newly installed pro-Western government in Kiev, as the Russian force was big enough that the exercise was a plausible preinvasion movement.

Meanwhile, the little green men appeared, and Moscow began to close its grip on Ukraine’s Crimean Peninsula. After it became apparent what was happening, the nearby Russian force helped dissuade Kiev from mounting its own military move to try and forestall Crimea’s fall.

On March 1 President Vladimir Putin orchestrated a Russian referendum authorizing him to use force in Ukraine. Regular infantry units moved into Crimea, covered by airpower from the Russian Black Sea fleet.

Meanwhile, Russia successfully exploited the information dimension of the conflict, according to a 2015 NATO study of hybrid war incidents. It flooded local media with propaganda depicting Moscow as the protector of Russian-language residents of the region, who were depicted as threatened by potential atrocities.

This sort of propaganda has made Putin hugely popular in Russia and may have helped deter the West from a more muscular support of Ukraine.

#### Article V gets circumvented now

Aurel Sari 19, Senior Lecturer in Law, University of Exeter; Director, Exeter Centre for International Law; Fellow, Supreme Headquarters Allied Powers Europe; Fellow, Allied Rapid Reaction Corps, “The Mutual Assistance Clauses of the North Atlantic and EU Treaties: The Challenge of Hybrid Threats,” Harvard National Security Journal, Volume 10, https://harvardnsj.org/wp-content/uploads/sites/13/2019/06/Mutual-Assistance-Clauses-of-the-North-Atlantic-and-EU-Treaties.pdf

It is important to appreciate that the bar for success in circumventing Article 5 NAT and Article 42(7) TEU is not necessarily high. The primary goal of a hybrid adversary is not to convince an expert audience that its activities do not amount to an armed attack or an act of armed aggression. Rather, its goal is to prevent the targeted state and its allies from making a compelling case that invoking Article 5 or Article 42(7) would be a lawful, legitimate, and prudent response to the threats they are facing. A plausible narrative that casts doubt on these points among domestic and international audiences might suffice to achieve that objective.278 States craft legal storylines to support their national security objectives on a regular basis.279 Although the idea that such verbal strategies are as important as military strategies may push the point too far,280 the significance of legal narratives and counter-narratives for opening up certain courses of action and for foreclosing others must not be underestimated. If anything, the progressive legalization of the conduct of foreign affairs and the vastly increased public interest in the legality of military action,281 amplified by social media,282 has boosted the impact of legal justifications. Assessing the potential vulnerabilities of the Transatlantic and European collective security arrangements from a narrow black letter perspective therefore risks misjudging their susceptibility to hostile strategic communication.

### Deterrence DA---Cyberdeterrence Fails

#### Cyberdeterrence fails---‘meatspace’ concepts don’t translate into the digital environment.

Soesanto Stefan 22, senior cyber defense researcher at the Center for Security Studies (CSS), ETH Zürich, Switzerland, currently working on the Cyberdefense Project with the Risk and Resilience Team, “Cyber Deterrence Revisited,” ETH Zurich, 04/07/2022, p. 49 p.

Cross-Domain Deterrence

Cross-domain deterrence describes the spectrum of strategic measures a nation-state is willing to leverage outside the cyber domain in reaction to an event inside cyberspace. Actions can range from criminal indictments of cyber operatives and trolling campaigns in the information warfare space to imposing economic sanctions and launching retaliatory nuclear strikes.83

The primary problem with cross-domain deterrence is ascertaining whether such measures will deter future aggression in cyberspace or result in spillover effects that remove long-standing deterrence mechanisms elsewhere. Spearheaded by the US Department Justice (DOJ), the indictment of nationstate cyber operatives for crimes committed against US-based entities has become the focal point to hold individuals personally liable for their actions and orders followed. Some analysts claim this is evidence of a concerted naming and shaming strategy by the US government (i.e., deterrence by delegitimization). However, the DOJ’s overarching legal aim is, and has always been, to attribute attacks and hold individuals accountable in a US court—whether adversarial cyber operators that hit non-military targets or foreign civilians that hit US entities. Tonya Ugoretz, deputy assistant director of the FBI’s Cyber Division, aptly states, “nothing says attribution like an indictment.”84

While nation-state cyber operatives indicted by the DOJ have remained outside the reach of US law enforcement, two cases stand out for counterintelligence purpose. Although not per se a “cyber” operative, the case of Yanjun Xu, deputy division director at the Chinese Ministry of State Security’s Sixth Bureau in Jiangsu Province, highlights that the DOJ’s indictments of foreign government operatives can net results abroad. Arrested in Brussels, Belgium, on April 1, 2018, Xu was extradited to the United States on October 9th.85 According to US officials, Xu’s extradition marked the first time a Chinese spy has been brought to the US to face prosecution.86 On November 5, 2021, a federal jury convicted Xu of “conspiring and attempting to commit economic espionage and steal trade secrets from multiple U.S. aviation and aerospace companies.”87 He is currently awaiting sentencing. The second case concerns Vladislav Klyushin, a Russian businessman and first deputy director of cybersecurity company M-13. Klyushin was arrested in Switzerland on March 21, 2021, on the request of US authorities who charged him with “alleged involvement in a global scheme to trade on non-public information stolen from U.S. computer networks that netted tens of millions of dollars in illegal profits.”88 While waiting for his extradition hearing, Swiss news outlet 24heures reported that former GRU (Russian intelligence agency) operative Ivan Sergeyevich Yermakov—wanted by the FBI for hacking into the DNC and interfering in the 2016 US presidential election—was actually employed by M-13.89 Following Klyushin’s extradition to the United States in December 2021, CNN reported in January 2020 that according to former US officials, Klyushin “could be a valuable asset in US efforts to gather more information on Russian interference in the 2016 election as well as other intelligence operations.”90 Similarly, Assistant US Attorney Seth B. Kosto argued at Klyushin’s pretrial hearing in Boston that “we do submit that he’s not simply any Russian citizen. . . . He is a Russian citizen who is employing a former military intelligence officer, who has a photograph in his internet service provider records of a medal of honor from the president of the Russian Federation.”91

The US Treasury Department by contrast has been leveraging targeted economic sanctions since April 2015, when President Obama signed Executive Order 13694 and declared a national emergency to deal with the “increasing prevalence and severity of malicious cyber-enabled activities originating from . . . outside the United States [that] constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States.”92 In December 2016, EO13757 amended EO13694 “to include an Annex of sanctioned persons and to expand the scope of cyber-enabled activities subject to sanctions.”93 Other cyber-related sanction programs followed in subsequent years, including EO13722, Blocking Property of the Government of North Korea and the Workers’ Party of Korea, and Prohibiting Certain Transactions With Respect to North Korea (March 2016) and the Countering America’s Adversaries Through Sanctions Act (August 2017). Since then, the Office of Foreign Assets Control (OFAC) has imposed cyber-related sanctions on close to 200 individuals and companies hailing from China, Iran, North Korea, and Russia.94 Thus far, none of the countries in question have discernably decreased their cyber-related activities vis-à-vis the United States.

The European Union has partially emulated the US approach with EU Council Decision 2019/797 and Regulation 2019/796 of May 2019 on “restrictive measures against cyber-attacks threatening the Union or its Member States.”95 As of this writing, the council has imposed two cyber sanction packages that imposed asset freezes and travel restrictions on those listed. The first package on June 30, 2020, listed six individuals and two entities for the OPCW hack, WannaCry, NotPetya, and APT10’s CloudHopper campaign.96 The second package was imposed on October 22, 2020, against two GRU officers and the GRU’s Unit 26165 for the 2015 Bundestag hack.97 Similar to the sanctions imposed by the US Treasury Department, it is currently entirely unclear what kind, if any, effects EU cyber sanctions produce on the adversarial end. In contrast to US sanctions, EU restrictive measures do not serve as a vehicle for public attribution, as the decision to attribute or not remains a sovereign political decision of the individual EU member states. As of this writing, the EU nonetheless continues to argue in document after document that sanctions are “intended to prevent, discourage, deter and respond to continuing and increasing malicious behaviour in cyberspace.”98 Probably most insightful when it comes to deterrence in this context is the UK’s National Cyber Strategy 2022. It acknowledged for the first time that “the development of the autonomous UK cyber sanctions regime has added another disruptive tool that we have used to respond to incidents such as the WannaCry and NotPetya attacks. However, despite all this, our approach to cyber deterrence does not yet seem to have fundamentally altered the risk calculus for attackers.”99

While it is indeed tempting to cross-connect preexisting deterrence frameworks elsewhere to the cyber domain, it is highly questionable whether the outcome is a more robust deterrence posture in cyberspace or a weakening of the deterrence posture in real space. For example, connecting nuclear deterrence to the cyber domain is probably an area where it could in fact be destabilizing or counterproductive. In January 2018, the New York Times reported that the language used in a draft of the 2018 US Nuclear Posture Review would “permit the use of nuclear weapons to respond to a wide range of devastating but non-nuclear attacks on American infrastructure, including what current and former government officials described as the most crippling kind of cyberattacks.”100 Amy Zegart, senior fellow at the Hoover Institution, questioned at the time, “Do we really think the United States government would launch a nuclear retaliatory strike after a cyberattack of how ever consequential damage might be on the United States? . . . Lots of debate about that. Is that really a robust deterrence strategy? Probably not.”101

Similarly, Harknett and Fischerkeller argued in 2017 that expanding deterrence to “include threats of law enforcement penalties, sanctions, and ‘name and shame’ approaches—denoted as whole-of-government deterrence— should be recognized for what it is—the addition of weaker forms of punishment because robust costs cannot be credibly imposed. Adding to a menu of weak options does not make deterrence stronger; it only reveals its inherent incompatibility with the challenge of the [cyber] domain.”102

Having critically dismantled six deterrence mechanisms that have emerged over the past years, let us now turn to the questions of when cyber deterrence is deemed theoretically successful and when it is not.

When Is Cyber Deterrence Successful?

Testifying before the House Committee on Armed Services in 2017, RAND’s Martin Libicki carefully explained that a successful deterrence posture in cyberspace necessitates four prerequisites: (1) the ability to correctly attribute cyberattacks, (2) the ability to effectively communicate US redlines, (3) the credibility of response if those red lines are crossed, and (4) the capabilities to successfully retaliate.103

To put Libicki’s theory into practice, let us consider a few simple deterrence scenarios between a fictional country A (the aggressor) and a fictional country B (the defender). B’s aim is to deter A’s hostile behavior in cyberspace.

First, deterrence in cyberspace succeeds if country A abstains from initiating hostilities against country B. A’s behavior could be due to a strategic rationale to avoid conflict, the negative outcome of a comprehensive cost-benefit analysis, B’s ability to effectively communicate redlines, or none of the above. Lacking any evidence that might explain A’s inaction, it is impossible to ascertain whether B’s deterrence posture worked as desired. As such, none or all of Libicki’s prerequisites would need to be fulfilled for this outcome to occur. This scenario has unfolded over the years with several researchers asserting that the absence of cyberattacks that cross the threshold to an armed attack is evidence of constraint and the functioning of deterrence in cyberspace.104 While, logically, the absence of evidence can be considered evidence in itself, the absence of any theoretical underpinnings that can explain the supposed causal deterrence mechanisms at work creates a circular logic that delivers no answers at all.

Second, deterrence in cyberspace succeeds if country B responds (proportionally or disproportionally) to an attack from country A (within a proximate temporal range), and hostilities subsequently terminate. Three of Libicki’s prerequisites would need to be fulfilled for this deterrence scenario to commence. The ability of effectively communicating redlines is redundant after the fact. However, we have not witnessed any exchange that would fit into this tit-for-tat category. This absence might indicate that escalation dynamics work entirely different in cyberspace—if at all—or might feed into a different political threat perception and strategic calculus that currently does not yet naturally translate down to the operational end and kicking off an immediate offensive response in cyberspace. Time likely moves magnitudes slower when it comes to decision-making processes for actions and reactions in cyberspace. Thus, decisions in real space and dynamics in cyberspace move independently from each other—in turn breaking down any escalation ladder before it can manifest itself. This time lag or causal disconnect would also explain why persistent engagement might not elicit an escalatory response or probably will not become entangled in an escalation ladder.105

Third, deterrence succeeds if country B responds out of domain to a cyberattack from country A by leveraging existing deterrence frameworks elsewhere (i.e., cross-domain deterrence), and subsequent adversarial actions in cyberspace terminate. All four of Libicki’s prerequisites would need to be fulfilled for this scenario to occur. However, if, for instance, country B responds with economic sanctions or criminal indictments—which are not connected to traditional deterrence dynamics—then country A might not be deterred by B’s retaliatory actions. The European Union and US Justice and Treasury Departments are currently locked into the latter scenario. It is uncertain whether their actions deter anyone or impose relevant costs on adversarial operations.

Fourth, cyber deterrence partially succeeds if country A attacks country B, and B responds by attacking country C due to misattribution. If country A deliberately left behind forensic evidence that would point toward country C (i.e., a false flag operation), then B’s cyber deterrence posture inherently failed. However, if country B experienced a massive intelligence failure on its end and struck country C purely by mistake, then B’s willingness to forcefully respond against country C might deter A from future attacks. In this scenario, only three of Libicki’s prerequisites would need to be fulfilled. Given the complexity of this scenario, we have not yet witnessed anything like it in cyberspace.

Fifth, if hostilities between country A and B (1) can be curtailed to episodic engagements, (2) are limited in their intensity, (3) remain constrained to the cyber domain, and (4) do not pull in civilian targets or allied forces, cyber deterrence could theoretically succeed in what Herman Kahn describes as a state of limited conflict or “agreed battle.”106 However, if any of those tacitly agreed on limitations are broken, deterrence fails, and escalation might reign supreme. For this interaction to play out, the only prerequisite necessary is for A and B to be able to correctly attribute each other’s cyberattacks.

Scenario two combined with scenario five is where persistent engagement currently falls within the deterrence conundrum. Persistent engagement necessitates effectively communicating redlines (scenario two), but in contrast to traditional deterrence thinking, it also actively seeks out adversarial contact (scenario five).

When Is Cyber Deterrence Unsuccessful?

First, deterrence fails if country A conducts a “first strike” against country B without country B responding in self-defense. This reaction may be due to simple self-restraint, entanglement, or paralysis by analysis. A war-gaming example for such behavior was observed by Jacquelin Schneider, assistant professor in the Strategic and Operational Research Department at the US Naval College, during the DoD’s annual war-game series Deterrence and Escalation Game in Review (DEGRE) in 2011. According to Schneider, the red team conducted offensive cyber operations against blue prior to any conventional military exchange. Instead of responding in kind, the blue defense lead explained, “I do not feel any of the cyber-attacks raised to the level where retaliation was needed and/or warranted! It was not risking nuclear war!”107 Most of the other blue players echoed the sentiment, with one commenting that “cyber-attacks[,] although annoying[,] do not appear crippling.”108 Yet when blue discussed employing offensive cyber operations themselves, they immediately self-restrained by creating “an equivalency between cyber operations and nuclear attack,” arguing that “any cyber attack would necessarily lead to a nuclear response.”109 The example illustrates the meatspace logics and assumptions being made on the strategic level when it comes to deterrence by punishment and cross-domain deterrence. They also fundamentally contradict the logics of war entailing the maximization versus the moderation of force. As Clausewitz wrote in On War, “to introduce the principle of moderation into the theory of war itself would always lead to logical absurdity.”110

Second, cyber deterrence fails if country B preemptively attacks country A. Such was the case in DEGRE’s 2012 exercise. As Schneider noted, the blue team went all in on preemptive cyber network operations to “degrade the enemy’s ability to conventionally respond to US operations.”111 Schneider stated that “the perception by the blue team was that blue was just as vulnerable . . . as the red team [if not more so] . . . and therefore had to preemptively strike red’s ability to conduct both cyber and kinetic attacks against blue command and control.”112 While this example is close to the logics of persistent engagement, it is also much more aggressive in nature. The caveat here is that while persistent engagement aims to create friction within an adversary’s cyber capabilities and infrastructure, the blue team in DEGRE conducted offensive cyber operations to degrade and affect the red team’s conventional war-fighting capabilities. That being said, country B might succeed in establishing a cyber deterrence posture after hostilities have ceased in this scenario.

Third, cyber deterrence fails when strategic signaling between both countries collapses at the most basic level. This was the case in DEGRE’s 2013 wargame exercise. As Schneider explains, the blue team started by implementing strict rules of engagement on computer network exploitation to create a deterrence policy that would disincentivize red from conducting preemptive cyberattacks. This approach led to the rather absurd situation where blue worried about the detection of their cyber espionage efforts (not attack) amid a naval blockade that saw the exchange of gunfire and 20 of red’s aircraft being shot down. Blue even tried to refine its deterrence policy by using cyber operations as a means of “signal[ing] potential capability while trying to avoid inadvertently signaling aggression or the willingness to escalate.”113 Schneider observes that “the red team failed to understand this elegant distinction.”114 In terms of responses, the blue team viewed red’s cyberattacks “as less escalatory than other kinetic options and therefore believed it was not worth a response.”115

And fourth, cyber deterrence fails if country A initiates hostilities, country B responds proportionally, and country A repeatedly escalates, potentially locking both into an escalation ladder. An example of such a crisis escalation scenario was on display during the four-day Schriever Wargame in 2010, hosted by Air Force Space Command and featuring some 600 military, civilian, and allied players.116 According to Maj Gen Susan J. Helms, director of Plans and Policy at US Strategic Command, hostilities commenced when “in a response to a perceived provocation, a regional adversary disabled the cyber and space assets of a key US ally.”117 While debating how to deter attacks on US and allied space and cyber capabilities, the blue team realized that the enemy continued to attack time and time again and “was not deterred from further escalation.” General Helms added, “As we came to learn, the leaders of this provocative regional state had defined their objectives (although those objectives were not obvious to us) and had already thought through the overall costs and benefits of their plan. In other words, they had assessed our likely behavior in the context of the scenario at hand, determined that, for them, the benefits of action outweighed the risks and they made their decision to ‘move out.’ At that point, options for deterrence by the US and her allies were ‘late to need.’ ”118

Granted, these war-gaming examples are not ideal cases to adequately reflect the decision-making dynamics playing out regarding cyberspace. But they provide valuable insights into the flawed logics and strategic concerns that hinder developing sensible deterrence strategies and enabling operational tactics in the cyber domain.

#### Conventional deterrence fails for cyber attacks

Mariarosaria Taddeo 19, Fellow in Cyber Security and Ethics in the Department of Politics and International Studies at the University of Warwick and Research Associate at the Uehiro Centre for Practical Ethics, University of Oxford, UK, “Norms and Strategies for Stability in Cyberspace,” Chapter 3 in “The 2019 Yearbook of the Digital Ethics Lab,” edited by Christopher Burr and Silvia Milano, https://link.springer.com/chapter/10.1007/978-3-030-29145-7\_3

3.4 Conventional Deterrence Theory

Concerned by the risks of escalation, international organisations such as NATO, the UN Institute for Disarmament Research (UNIDIR), and national governments, like the UK and US have started to consider whether, and how to, deploy deterrence to foster stability of cyberspace.

However, deploying cyber deterrence strategies is challenging. For conventional deterrence theory (hereafter: deterrence theory) does not work in cyberspace, as it does not address the global reach, anonymity, or the distributed and interconnected nature of this domain. Deterrence theory has three core elements: attribution of attacks, defence, and retaliation as types of deterring strategies; and the capability of the defender to signal credible threats (see Fig. 3.1). None of these elements is attainable in cyberspace.

Consider attribution first. Prompt, positive attribution is crucial to deterrence: the less immediate is attribution, the less severe will be the defender’s response. The less positive the attribution, the more time will be necessary to respond. In cyberspace, attribution is at best problematic, if not impossible. Cyber attacks are often launched in different stages and involve globally distributed networks of machines, as well as pieces of code that combine different elements provided (or stolen) by a number of actors. In this scenario, identifying the malware, the network of infected machines, or even the country of origin of the attack is not sufficient for attribution, as attackers can design and route their operations through third-party machines and countries with the goal of obscuring or misdirecting attribution. The limits of attribution in cyberspace pose serious obstacles to the deployment of effective deterrence. Recalling Fig. 3.1, without attribution defence and retaliation, as well as signalling, are left without a target and are undermined by the inability of the defender to identify the attacker.

Signalling credible threats is also problematic in cyberspace. This element hinges on state’s reputation. In kinetic scenarios, reputation is gained by showcasing military capabilities and by showing ability to resolve (to deter or defeat the opponent) over time. To some extent, the same also holds true in cyberspace, where a state’s reputation also refers to a state’s past interactions in this domain, its known cyber capabilities to defend and offend, as well as its overall reputation in resolving conflicts. However, state’s reputation in cyberspace may not necessarily correspond to actual capabilities in this domain, as states are reluctant to circulate information about the attacks that they receive, especially those that they could not avert. This makes signalling less credible and, thus, more problematic than in other domains of warfare.

Also conventional deterrence strategies, defence and retaliation, are problematic in cyberspace. Every system has its security vulnerabilities and identifying and exploiting them is simply a matter of time, means, and determination. This makes vulnerable even the most sophisticated defence mechanisms, thus limiting their potential to deter new attacks by defence. Unlike deterrence by defence, deterrence by retaliation may be effective in cyberspace. However, this strategy is coupled with serious risk of escalation. This is because the means to retaliate, i.e. cyber weapons, are malleable and difficult to control. Cyber weapons can be accessed, stored, combined, repurposed, and redeployed much more easily than it was ever possible with other kinds of military capability. This was the case, for example, of Stuxnet. Despite being designed to target specific configuration requirements of Siemens software installed on Iranian nuclear centrifuges, the worm was eventually released on the Internet and infected systems in Azerbaijan, Indonesia, India, Pakistan, and the US (Farwell and Rohozinski 2011).

#### Deterrence fails for Cyber

Jim Chen 18, National Defense University, Fort McNair. 03/09/2018. “Effectively Exercising Deterrence in the Cyber Domain.” Proceedings of the 13th International Conference on Cyber Warfare and Security: National Defense University Washington DC, USA.

Let us check the reality first. The cyber deterrence strategies currently used rely on defense and punishment. They are not very effective as they fail to scare adversaries away in cyber attacks. For example, Morgan (2017) estimates that global ransomware damage costs is up from $324 million in 2015 to $5 billion in 2017, "a 15X increase in two years, and expected to worsen". Larson (2017) lists the major cyber hacks of 2017 such as Equifax data breach with the loss of the personal data of 145 million people, leaked government tools, WannaCry that got spanned in more than 150 countries and took down many businesses, NotPetya virus that targeted Ukrainian businesses with compromised tax software, Bad Rabbit ransomware campaign that compromised news and media websites, almost 200 million voter records exposed, and hacks that targeted school districts. In addition to some of the hacks mentioned above, Mittal (2017) includes the following into the list: Cloudbleed security bug that leaked sensitive data of affected users such as passwords and authentication tokens, and HBO hack with 1.5 terabytes of information stolen including scripts and episodes of popular TV show Game o f Thrones. There are other reasons for the unsuccessful implementation of deterrence in the cyber domain. They cover various aspects such as legal, psychological, strategic, financial, and operational aspects. First, legally, attribution is slow as it needs time in acquiring, examining, and analyzing evidence in an investigative process. To make things even more complicated, attackers have developed various ways of hiding their identity by using botnets or hijacked hosts while launching attacks. The camouflage further slows down attribution. Second, psychologically, people's responses towards attacks in the virtual world are different from people's responses towards attacks in the physical world. As damages cannot be seen with eyes in most cases, attacks in the virtual world seem to be less severe than those in the physical world in many cases. In other words, not seeing is less believing. Besides, Wells (2017) discusses disinformation campaigns that "aim to undermine citizen confidence and core beliefs". Such a campaign may not be recognized at the time when it is launched. It may take days, weeks, months, or even years to recognize such a campaign. Should it be recognized, it is still difficult to quantitatively measure the true damage that it has caused. This renders quick and well-cooperated countermeasures impossible. Third, strategically, most cyber attacks are deliberately designed to be below the threshold of physical armed attacks. This makes it difficult for defenders to carry out retaliation traditionally used in the physical world. In many cases, intruders walk away without being punished. This sets bad examples for other intruders. Fourth, financially, the cost of retaliation is not cheap. Depending upon the measures used in varied domains, the cost may go higher. In addition, an economic sanction may affect multiple parties in a global economic environment even the intruder side gets the hard hit. Fifth, operationally, collaboration requires a great amount of time and efforts from all parties involved due to diverse interests and capabilities. Should an economic measure or a military operation be deemed necessary after a severe cyber attack from an adversary, a response must be well orchestrated from all the relevant domains to guarantee its effectiveness. All these factors make deterrence hard to be implemented in the cyber domain.

#### Deterrence fails

Joshua Rovner 19, associate professor in the School of International Service at American University. He served as scholar-in-residence at the National Security Agency and U.S. Cyber Command in 2018 and 2019, “CAN THE UNITED STATES DETER ELECTION MEDDLING?,” War on the Rocks, 11/8/19, https://warontherocks.com/2019/11/can-the-united-states-deter-election-meddling/

A Skeptics’ Guide to Deterrence in Cyberspace

The United States has recently become outspoken about using cyberspace operations to impose costs on its adversaries. U.S. Cyber Command argues that persistent engagement can have a cumulative effect on great power rivals, which up to now have been able to operate freely without many consequences. More assertive efforts may disabuse adversaries of the notion that they can act with impunity. A forward defense may raise the long-term cost of cyberspace operations against the United States, reducing adversaries’ belief that they can erode U.S. power by working through the digital domain. Stability may emerge over time as rival powers settle on tacit norms about what kinds of cyberspace operations are tolerable.

None of this is relevant for stopping Russian mischief in the next election, however. The goal is not long-term stability, but immediate deterrence. The United States is facing a specific threat with a clear deadline. If U.S. officials are right that Russia is ramping up its effort in advance of the election, then they will likely conclude that economic sanctions and military posturing are not enough. Observers may turn to more aggressive cyberspace operations in the hopes that reciprocal attacks on Russian networks may force it to reconsider its approach. Imagine a barrage of debilitating cyber operations, employing sophisticated tools to inject friction into Russian government agencies. Imagine Russian officials worrying about the kind of ransomware attacks that hit Baltimore and Atlanta. Now imagine U.S. officials making specific warnings along these lines. Would they work?

Probably not. For a host of reasons, such threats are unlikely to deter Moscow. Economic threats and military posturing have had little effect so far, and the addition of cyberspace operations to the mix adds little in terms of coercive leverage. While there has been enduring interest in the notion of cyber deterrence, a growing body of research finds that the concept has limited value. It may be possible to deter particularly destructive attacks requiring extensive organizational resources – think here of something like an attack designed to cripple a civilian power grid. And recent work on cross-domain deterrence explores the possibility of using non-cyber tools to inspire caution among states considering offensive cyberspace operations. But in most other cases, deterrence is dubious. This is especially true when the actions we seek to deter are not destructive.

The basic problem is that cyberspace is a lousy domain for coercion. Individuals, firms, and states are relatively tolerant of cyber operations, and willing to engage online even in the wake of high-profile cybersecurity breakdowns. Retaliatory threats lack teeth because key actors in cyberspace are not remarkably fearful or vengeful. Experimental studies find that the public is also cautious about escalation in the wake of hypothetical cyberattacks. This tendency not only creates an escalation firebreak but also undermines the credibility of deterrent signals, which require a willingness to accept risk.

Other domestic factors work against deterrence. Sending clear signals in cyberspace is tricky, for example, because states do not control the infrastructure of the domain. Public-private coordination is necessary both to make threats and execute them, but such coordination is difficult and sometimes contentious.

International and technological factors also make deterrence difficult. As Erik Gartzke and Jon Lindsay point out, coercion in cyberspace is difficult because the domain is built on voluntary connections. This reduces the credibility of threats to conduct truly damaging attacks, because such threats give the target a reason to disconnect. Other research has reinforced the conclusion that cyberspace operations have limited coercive value, both in peacetime and war. The theoretical requirements of effective coercion do not map easily onto cyber operations, and empirical studies suggest that they are only useful when they support other policy instruments.

All this suggests that cyberspace coercion is difficult even against vulnerable states that are particularly sensitive to foreign pressure. Putin’s Russia is not one of those states. It has been willing to absorb substantial costs rather than back down from its strategic choices, however dubious. And the cost-benefit equation continues to favor Russian activism: the ability to affect the United States through election meddling is probably irresistible for a country that faces overwhelming military, economic, and diplomatic disadvantages. Meddling is cheap. As Sen. Mark Warner puts it, “if you add up all Russia spent in the Brexit vote, the French presidential elections, and the 2016 American elections, it’s less than the cost of one new F-35 airplane.”

### Deterrence DA---OCOs Fail

#### NATO OCOs fail---commanders can’t accurately gauge effects or collateral damage. This chills cyber activity due to fear of violating laws of war.

Jeppe T. Jacobsen 21, Ph.D. candidate at the Danish Institute for International Studies and the Center for War Studies at the University of Southern Denmark, worked as cyber coordinator at the Ministry of Foreign Affairs of Denmark where he coordinated Denmark’s cyber diplomacy, “Cyber Offense in NATO: Challenges and Opportunities,” International Affairs, vol. 97, no. 3, 05/01/2021, pp. 703–720

Challenges to a smooth integration of cyber effects

Assessing effects—ensuring proportionality and discrimination

How likely is it that the requested cyber effect will be delivered? The answer to this question is not clear, in respect of either its preparation or its execution. This is not only because IT vulnerabilities are constantly discovered and patched; it is also because of the difficulty of assessing the effects and possible side-effects of an exploit when navigating and analysing complex IT infrastructures. In other words, reconnaissance is difficult in cyberspace, and so is the containment of effects. The Russian attempt to use ransomware aimed at disrupting critical Ukrainian infrastructure in 2017, for example, succeeded—but simultaneously encrypted computers globally, causing substantial economic damage to multinational businesses such as Maersk and FedEx.34

Collateral damage and unintended consequences are serious issues for NATO. The alliance takes pride in its adherence to the principles laid out in international law, such as proportionality and discrimination, as former NATO Deputy Assistant Secretary-General Jamie Shea has emphasized.35 Thus, disruptions of servers with huge negative implications for civilians, or the use of generic cyber tools that risk spreading their effects far and wide, are most likely not going to be considered for use in NATO operations. Indeed, one of the main challenges to US efforts to disrupt servers in working against ISIS was finding ways to ensure that civilians were not hit by their cyber effects.36

Another aspect of the difficulty of assessing the cyber effect relates to adversaries’ cyber defence efforts. For the more sophisticated players in cyberspace, cyber defence has developed into more than simply patching, clearing and updating systems. Cyber defence is also increasingly about following an intruder’s activity in one’s own network and creating ‘honeypots’ or ‘honeynets’; or about following data traffic back to the intruder’s network. In short, cyber defence is also about deception and active defence.37 This approach to cyber defence offers valuable insights into the intruder’s techniques and strategies; but the mere knowledge that deception is becoming a predominant defensive strategy also introduces doubts into the intruder’s assessment of possible effects.

Consequently, as Russia is considered a peer competitor with considerable cyber-defensive capacities, one informant expressed scepticism about the extent to which smaller member states are confident in their ability to deliver a cyber effect when it is requested by NATO.38 This is especially the case if operational success depends on a specific effect. Even if a state has developed the appropriate exploit, it must also be able to verify that the effect is achieved and ensure that the effect is contained to minimize collateral damage. And even if a state is confident about its current ability to contain and verify an effect, it must also be confident that it can deliver, verify and contain the effect at the specific time in the future when CYOC requests it.

The process of integration is further complicated by the fact that NATO must be willing to hand over to contributing states the responsibility for making battle damage assessments and collateral damage estimations. As the following subsection shows, states are generally unwilling to share classified information about exploits. Hence, the delegated NATO commander is unlikely to receive much useful information about how cyber effects are delivered before a decision about their deployment must be taken. As commanders would prefer to have control over the capabilities used, member-state cyber effects are likely choices of method only if alternative, conventional effects are unavailable.

The challenges associated with assessing cyber effects are naturally most significant in relation to those effects that enable other kinetic effects that are necessary to achieve operational success. For cyber effects that seek to maintain a persistent annoyance of Russian networks, these challenges are less of an issue. If the aim is to create confusion and drain resources by targeting networks and operations that are otherwise difficult and expensive to disrupt using conventional means, then cyber effects can support strategic goals without causing irreversible damage to civilians. As I will conclude at the end of this section, such a change demands an adaptation of the way in which CYOC operates.

#### Members will say no to deconfliction efforts---secrecy is a red line.

Jeppe T. Jacobsen 21, Ph.D. candidate at the Danish Institute for International Studies and the Center for War Studies at the University of Southern Denmark, worked as cyber coordinator at the Ministry of Foreign Affairs of Denmark where he coordinated Denmark’s cyber diplomacy, “Cyber Offense in NATO: Challenges and Opportunities,” International Affairs, vol. 97, no. 3, 05/01/2021, pp. 703–720

The third challenge to the integration of cyber effects in NATO operations relates to a well-known military concept, deconfliction. The coordination by allies and military units of their efforts to avoid confliction, between for example an air operation and a special forces operation in the same area, is a central element in every military campaign. Deconfliction is all about openness and communication between allied partners. But in cyberspace, deconfliction comes with several difficulties. At the core of these difficulties is the fact that the tools and techniques that produce cyber effects—which are often also used and heavily depended on for intelligence collection—are developed in secret and must stay secret until the effect is achieved. If the IT vulnerabilities and exploits are known, vendors or adversaries can fix or replace the software and thereby render the effect impossible to achieve.39 In an alliance not known for sufficient mutual trust among members to share intelligence,40 there is little indication that allies will become more open about the cyber tools and techniques they currently have at their disposal. The request-based model is the result of that lack of trust. And the unwillingness to share cyber intelligence seriously challenges NATO’s ambition to use CYOC to facilitate information-sharing to increase situational awareness and thereby achieve the ‘cyber readiness’ and ‘cyber resiliency’ that NATO Deputy Secretary-General Mircea Geoană hopes to attain.41

Furthermore, lack of coordination and discussion about the use of military cyber capabilities, both internally in each state and among allies, can have negative implications for intelligence activities and general network security. A conventional military decision to deliver cyber effects is rarely concerned with maintaining access and staying secret after an effect is achieved. Even though it is customary to try to obscure the vulnerabilities that are being exploited, it is difficult to ensure that those operating the targeted system or third-party network analysts do not identify and fix the vulnerabilities in, for example, commercial products used all over the world. Thus, military plans to engage other state entities need to weigh the benefit of delivering cyber effects against the risk of losing intelligence capacity, as well as the risk that other actors (allies, corporations, adversaries, criminals, etc.) will use the same exploits against oneself. In other words, there is a conflict of interest between attack, intelligence collection and internal defence in each NATO member state.42 The desire of the US Cyber Command to become more independent from the National Security Agency (NSA) is precisely an attempt to gain a stronger voice when the US government assesses whether a vulnerability should be disclosed to vendors, retained for intelligence purposes or used to deliver ‘loud’ cyber effects.43

The risk of confliction among allies arises from the fact that a similar assessment procedure does not exist across NATO. As conversations with several national representatives at the CDC reveal, such a procedure is unlikely to be agreed upon owing to the different perspectives on offence, defence and espionage in cyberspace currently prevailing among member states.44 If the Netherlands, for example, offers to deliver a ‘loud’ cyber effect in a NATO operation, British or American intelligence operations could end up being disturbed because they rely on the same vulnerabilities which—when used in military operations—risk being exposed and subsequently fixed.45 When deploying ‘loud’ cyber effects, malicious actors such as criminals are also given the opportunity to identify and exploit the same vulnerabilities in unpatched systems in allied countries. The ransomware incidents known as WannaCry and NotPetya are examples of the damage that can emerge from government exploits becoming publicly available—even though the specific vulnerabilities were already patched by Microsoft and updates released to supported systems.46

In short, there is a dilemma both internally, between intelligence agencies and the military, and externally, between allies. While it is difficult to do much about the latter, the internal power dynamics in most states, with the intelligence agencies as the primary cyber actors, are likely to limit the willingness of most states to deliver military cyber effects—whether offensive or defensive—when CYOC makes requests. They also limit the willingness to share cyber threat information across the alliance through CYOC.

This section has pointed to three characteristics about cyberspace that limit the integration of cyber effects in NATO operations. In a complex and constantly changing cyberspace, it continues to be difficult to develop and maintain sophisticated exploits for targeted cyber effects. This is especially the case if the cyber effects are requested for a specific time and place in order to guarantee operational success, and if they simultaneously have to be verifiable and conform to international legal principles. Neither the member states, which face an internal dilemma between attack, intelligence collection and defence in cyberspace, nor the NATO commander, who will prefer to control the capabilities used, are likely to feel sufficiently confident about the targeted or highly integrated cyber effects to choose that option if other capabilities are available.

While these challenges are likely to persist, the cyber effects that constantly cause temporary annoyances hold a largely unappreciated potential in military operations. Even though each of these effects is unlikely to have a measurable strategic effect on its own, they stay true to the dynamic cyber environment while being able to drain resources and cause confusion and doubt. To embrace this potential fully, CYOC needs to adopt a more flexible and open-ended approach when requesting cyber effects. A focus on highly targeted effects requested at a specific time needs to be supplemented by more attention to requests that give member states the freedom to contribute with a variety of (offensive and actively defensive) effects when they become available. This means, for example, a willingness from NATO to accept member states’ reluctance to share cyber intelligence and to give up exclusive control over deciding on potential targets. To make SCEPVA work, there must be a constant line of communication between the national cyber units, CYOC and the NATO commanders to ensure rapid decision-making on whether to use cyber effects when they become available.

If NATO displays this willingness and maintains this line of communication, the integration of cyber effects will become as effective as possible for an organization without close intelligence cooperation. CYOC, however,—even in its more flexible versions—is not likely to fulfil NATO’s stated ambition to strengthen its broader deterrence by integrating offensive cyber effects in its operations.47 The next section explains why.

## Innovation DA Answers

### Innovation DA---2AC

#### Transparency over collective defense key to enable operational planning

Marios Efthymiopoulos 19, PhD from the University of Crete in Security and Strategic Affairs on NATO issues and NATO-Russia relations, Chairman of the Board of Advisors of Strategy International, 6/24/19, "A cyber-security framework for development, defense and innovation at NATO", Journal of Innovation and Entrepreneurship, Volume 8, Article 12, https://innovation-entrepreneurship.springeropen.com/articles/10.1186/s13731-019-0105-z

NATOs cyber-resilience experienced in crisis management and communication

Societal security, an emerging phenomenon in the field of strategy and security, requires good crisis management skills but also communication effectiveness in both the real and virtual worlds. Business continuity at NATO requires as foresaid the Alliance, to be resilient and surely for the purposes of this research paper, the Alliance and allies to be or become cyber-resilient.

By methodological approach, societal vulnerability continues and will always continue to exist, so far and as long as threats are there. Considering the current civil need to be always preparing for a new “cold era,” among others, considering the unlawful annexation by Russia of Crimea in 2014 (BBC, 2014) and following the disintegrating relations of NATO due to the unlawful act of Russia to Ukraine, the establishment of the USA and then taken over by NATO, of the Missile installation in Romania (Reuters, 2016) and the immediate reaction and accusation of Russia in regard to these developments (New York Times, 2016), the refugee challenges as an outcome on the constant fight against ISIS (US Homeland Security Committee, 2015), but also the phenomenal changes in the financial world (i.e., The Panama Papers (The International Consortium of Investigative Journalists (ICJ), 2016)), NATO is required to become truly resilient NATO, as should also nations and leaders.

All aforementioned elements are crisis management factors. NATO provides the tools and methodologies, in which the Alliance is requested to reply strategically and operationally. To mitigating plans for pre-crisis, during crisis and after crises situations. For and during operations, logistics of deployment or information gathering and or training purposes, among others.

In such similar cases, the legal and political perspectives also on cyber operations should be clear. The success of an operation lays to effective logistical and operational support. Therefore, the legal aspects that come with sharing of information, on how to deploy forces, identify key threats and elements in cyber-space, are important. The Internet has no borders. And threats can easily infiltrate the national e-space and boundaries. Leaders are welcomed upon to take strong strategic-led decisions.

NATO is to ensure protection of all infrastructure. The Allies should be able to anticipate, identify, mitigate, and recover from “hybrid attacks (NATO Review, 2016)”—the dimension(s) of simultaneous attacks, while reducing the threat of destabilization and or spreading fear.

In a civic society, it is our responsibility to ensure adequate awareness on cyber-defense and security. To learn about the necessity to protect all infrastructures, NATO’s collective defense should be characterized by burden sharing, openness, flexibility, and transparency in cooperation and information flow among member states. Through preparedness, strategic and operational awareness, strategic resilience can be achieved. Response time and framework will then allow NATO to counter threats as they emerge.

#### BUT, tech investment without clarifying article 5 first causes offensive ops---those escalate and turn the DA

Sophie Arts 18, program coordinator supporting The German Marshall Fund of the United States’ (GMF) security and defense policy work in Washington DC., “Offense as the New Defense: New Life for NATO’s Cyber Policy,” GMF Policy Brief No. 039, 2018, https://www.gmfus.org/publications/offense-new-defense-new-life-natos-cyber-policy

Against the backdrop of a fast-developing cyber threat landscape, NATO has struggled to enact a comprehensive strategy that sufficiently prepares allies to deter or defend themselves against cyberattacks. While important steps have been taken, the alliance is still nowhere near ready to face cyber threats at the ‘speed of relevance’. Individual members’ guarantees to use their cyber capabilities on behalf of the alliance – as the United States announced this year – can help fill that gap in strategy.

Yet, without a well-defined policy agreement between the member states and a clear command structure in overseeing NATO operations, this approach risks unintended consequences – particularly as offensive cyber operations have the potential of cascading into conventional conflict. To prevent such a scenario, allies should further formalize their cyber strategy through top-down guidance and increase their cooperation with partners to broaden their spectrum of potential responses. Most importantly, NATO needs to streamline its decision-making process in the cyber domain and to define potential response scenarios – including and short of evoking the collective-defense clause under Article 5.

#### Grand is about ambiguity in respect to adversaries actions---ie allies need to accept that hybrid warfare involves ambiguity and plan for contingencies, which IS the AFF

#### The AFF maintains strategic ambiguity with respect to responses but sets clear red lines for thresholds which solves the DA AND avoids miscalc

Charlie Dunlap 16, former deputy judge advocate general of the United States Air Force, joined the Duke Law faculty in July 2010 where he is a professor of the practice of law and Executive Director of the Center on Law, Ethics and National Security, ““Cybervandalism” or “Digital act of war”? America’s muddled approach to cyber incidents won’t deter more crises,” Lawfire, 10/30/16, https://sites.duke.edu/lawfire/2016/10/30/cybervandalism-or-digital-act-of-war-americas-muddled-approach-to-cyber-incidents-wont-deter-more-crises/

What to do? Develop norms as to the “red lines”

It is vitally important, however, to appreciate that simply because a particular cyber act may legally constitute an “armed attack” that might qualify for the political characterization of an “act of war,” that doesn’t mean that a country is obliged to respond to it with force. Indeed, there are many political reasons that would counsel against doing so. This is where Mr. Painter goes wrong with his discussion about “strategic ambiguity.”

In deterrence, ambiguity may be useful with respect to a response, but it is markedly less so when you are talking about the threshold. Misunderstandings as to where the proverbial “red lines” are set can lead to dangerous miscalculation, unintended escalation, and unwanted conflict. Given the enormous potential of cyber acts to do harm, potential actors ought not to get mixed messages as to how the U.S. considers harmful cyber activities.

Frustrations with the opaqueness as what cyber activity would constitute a casus belli appears to have motivated Congressman Mike Rounds to propose a bill earlier this year that would require the President to develop a policy for determining “when an action carried out in cyberspace constitutes an act of war against the U.S.”

Rounds points to testimony of Marine Lt. Gen. Vincent Stewart, director of the Defense Intelligence Agency, as part of his rational for the legislation. Stewart admitted that a “much fuller definition of the range of things that occur in cyber space [is needed], and then [we should] start thinking about the threshold where an attack is catastrophic enough or destructive enough that we define it as an act of war, I think that would be extremely helpful.”

Stewart isn’t alone in not “fully” understanding where the threshold lies. Other Pentagon leaders apparently are equally uncertain, something that raises the obvious question: if our leaders don’t know, how can we expect potential adversaries to understand which acts might spark a full-blown war? At the same time, except in the most aggravated cases, enumerating in advance precisely which cyber acts exceed the use of force threshold might be nearly impossible.

This is where norm development in international law comes into play. In doing so, the U.S. needs to use the language of international law. Political terms like “digital acts of war” are unhelpful not only because they do not track with the language of the law, they also can imply to the general public a level of response that is unnecessarily provocative and even inconsistent with the proportionality and necessity factors intrinsic to a lawful exercise of self-defense, especially in the complex cyber arena.

#### Innovation is stalling.

Christopher Cole 21, partner at Crowell Moring, “Lawmakers Worry Rampant Mergers Crushing US Innovation,” Law360, lexis.

Innovation across the U.S. economy has suffered as antitrust laws fall short in stopping predatory merger deals and enforcers allow massive industry consolidation to continue unabated, experts said Wednesday on Capitol Hill.

In the latest congressional hearing focused on possible overhauls of American competition laws to deal with industry concentration in sectors ranging from technology to pharmaceuticals, real estate and agriculture, a Senate panel zeroed in on the impact of monopolies on the development of cutting-edge products and services.

Antitrust advocates and business figures testified that the U.S. economy faces a growing threat from large companies' merger and acquisition strategies that aim to knock out startups and growing rivals, then take advantage of market power to continue profiting off old technologies. The trend stifles U.S. innovation and harms consumers, they said.

Senators looked to the experts to inform the lawmakers' biggest push in years to revamp antitrust laws, including a major bipartisan bill introduced in October, the American Innovation and Choice Online Act. The bill would make it harder for online sales platforms to self-preference their own products. Sens. Amy Klobuchar, D-Minn., and Chuck Grassley, R-Iowa, are lead sponsors of the bill, one of numerous antitrust proposals circulating on Capitol Hill.

"It's always been innovation that has fueled the American economy," said Klobuchar, who chairs the Senate Judiciary antitrust panel, but that "cannot thrive without open and competitive markets."

Monopoly power is on the increase in industries "from cat food to caskets," Klobuchar said, and that stifles the ability of new companies that may develop better products or services to gain funding and enter the market competitively. "We also have to remember that innovation is all about competition," she said.

Utah Sen. Mike Lee, the ranking Republican on the subcommittee, also voiced concern about consolidation suffocating the economy. Lee said that "I'm a huge advocate of the consumer welfare standard" that federal courts use to assess whether market behavior is unlawfully anticompetitive but "when competition suffers, so does innovation."

"One might say that competition is itself the mother of innovation," said Lee, who has been working closely with Klobuchar and Grassley, the full committee's ranking Republican, on antitrust legislation this year.

Still, Lee said lawmakers and enforcers must take care not to carry out "regulatory overreach" that ends up protecting no one except market incumbents when they make it harder for startups to succeed. Lee touted Utah's "pro-free market" approach that he said has been a magnet for new businesses and driven the quality of life higher in the Beehive State. "I do worry, however, that D.C. bureaucrats may spoil the party for everyone," he said.

Conservatives also voiced concern that consolidation of power in Big Tech has allowed the top companies to rein in free speech, and Lee pointed to the controversy over the startup social media platform Parler, which almost sunk amid the turmoil over the 2020 election.

The vast technology sector was only one aspect of Wednesday's hearing, however, as several witnesses talked about growing monopolies in pharma, real estate and other parts of the economy where they said behemoths' market power was holding back innovation.

Diana Moss, president of American Antitrust Institute, told senators there are many reasons that innovation is currently struggling in the U.S. economy. She said the financial markets' "laser focus on shareholder returns" based on the bottom line and short-term profits was making it more difficult for companies to invest in much-needed research and development.

"Another reason is weaker antitrust enforcement over the last 40 years," Moss said.

Alex Harman, competition policy advocate at Public Citizen, the liberal-leaning advocacy group, called unfettered merger and acquisition activity and the massive buildup of a small number of companies "one of the most critical issues of our time." Harman said there had been an "alarming increase in consolidation throughout the economy."

Another witness, Roger Alford, a professor at Notre Dame Law School, identified multiple competitive problems rippling through the economy. One of the sectors hard-hit by a resulting lack of innovation is real estate sales, said Alford, a former deputy assistant attorney general with the U.S. Department of Justice Antitrust Division.

### Innovation DA---AT: China Impact

#### AFF solves Chinese hybrid threat by contingency planning---that’s key to security

Lauren Speranza 20, director for trans-Atlantic defense and security at the Center for European Policy Analysis, 7/8/20, “China Is NATO’s New Problem,” https://foreignpolicy.com/2020/07/08/china-nato-hybrid-threats-europe-cyber/

Over the past decade, Chinese companies have invested billions of dollars throughout Europe—buying up critical infrastructure and increasing Beijing’s political clout across the continent. As Chinese firms, often with strong ties to the state and Chinese Communist Party (CCP), acquire parts of sensitive ports, pipelines, and telecommunication networks, China’s incursions into Europe’s security umbrella are drawing serious concern.

But NATO, long worried about Russia, has largely been silent on China. Now, that is changing. NATO Secretary-General Jens Stoltenberg recently called on the alliance to stand up to Beijing’s “bullying and coercion,” underscoring how China’s rise is fundamentally shifting the global balance of power. It’s apparent that NATO can no longer ignore the threat. If the alliance hopes to remain competitive, it will need to develop a new strategy for dealing with Beijing.

First, NATO needs a common assessment of China’s hybrid threats—a mix of diplomatic, economic, security, information, and technological actions designed to quietly undermine democratic states and institutions to Beijing’s benefit while avoiding a traditional conflict. While China’s conventional military threat in the Indo-Pacific is far from NATO’s borders, its hybrid activities are happening in the alliance’s own backyard.

Cyber-espionage, intellectual property theft, infiltration of critical infrastructure, debt manipulation, and disinformation are prime examples. While these threats may seem to fall outside of NATO’s purview, they pose serious security risks for the alliance. For instance, China’s desire to invest in Lithuania’s Klaipeda Port may not look like a problem for NATO on its surface. But its investments have worrying strings attached that give China operating control over the infrastructure. That control could decrease allies’ willingness to move military forces—including sensitive technologies—through the port and its surrounding networks. This could lead to disrupted planning and fewer military exercises, decreasing NATO’s ability to defend the Baltic States during a crisis with Russia. This could also open the door for pragmatic collaboration between China and Russia to undermine trans-Atlantic security.

Allies need to forge a shared understanding of these risks through information-sharing and dialogue—no small feat for countries that do not see eye to eye on China. Some are even willing to ignore such vulnerabilities, due to economic benefits or disenchantment with trans-Atlantic institutions. The United States has a critical role to play in getting allies on the same page and setting common goals for countering China’s hybrid activities.

Second, NATO needs to focus on public diplomacy. NATO has an important role to play in the battle against the CCP’s global narratives, which Beijing promulgates through hybrid activities. To defend the trans-Atlantic values on which the alliance is built—freedom, democracy, rule of law, and human rights—NATO should clearly communicate China’s violations of these principles and its propaganda efforts to cover them up. (These include, among others, human rights abuses against ethnic Uighurs in Xinjiang and violations of the U.N. Convention on the Law of the Sea in the South China Sea.) NATO should also enhance its outreach to key partners in the Indo-Pacific, such as Australia, Japan, New Zealand, and South Korea, which can serve as important counterweights to Chinese influence in the region. Effective public messaging also means getting serious about attributing the blame for attacks, as the European Commission recently did over Chinese disinformation around COVID-19, to raise the pressure on Chinese officials. Trans-Atlantic countries have struggled to shape China’s behavior because they cannot prove malign intent or agree to call out Beijing for its subversive efforts. Allies should develop clearer guidelines—what needs to be proved, by whom, and to what degree—to enable collective attribution. NATO is strongest when it speaks with one voice. It should use that voice to demand transparency and change from China.

Third, the alliance should step up its counteroffensive. China’s hybrid actions intentionally blur the lines between what is legally permissible, politically inappropriate, and downright escalatory.

This makes it difficult for leaders to determine appropriate responses, producing a reactionary approach thus far. But an intensifying geostrategic competition has already begun. To compete in this environment, the trans-Atlantic community needs a more proactive approach. Rather than waiting for China to invest in the next major European port, allies should coordinate legislation to prevent the riskiest Chinese acquisitions. And rather than waiting for more Chinese cyberintrusions, allies should collaborate on responsible, targeted offensive cyberactions. Over time, this would help dissuade China from manipulating investments in critical infrastructure, conducting cyber-espionage, and other hybrid activities. While adopting a more offensive posture remains controversial among certain allies, it is gaining traction across Europe and is strongly supported in Washington. Although NATO, as a defensive alliance, should not implement such a counteroffensive, policymakers should leverage it as the primary forum to coordinate actions among willing nations.

Fourth, NATO needs to deepen its cooperation with other key players, such as the European Union and the private sector. Where NATO lacks the mandate and means, the EU and multinational businesses play critical roles in developing, implementing, and enforcing the legislation and financial incentives necessary to counter Chinese hybrid threats. Complementary to that, NATO and its allies can focus on providing intelligence, defending cyberspace, developing capability targets for new technologies, conducting exercises and contingency planning, informing resilience requirements for secure infrastructure, and bolstering deterrence. Despite the political obstacles that impede more formal NATO-EU cooperation, allies should look to the European Centre of Excellence for Countering Hybrid Threats in Helsinki to bring together NATO and EU staff, national officials, and industry voices in one place to align their counter-hybrid policies for China.

The Chinese government’s manipulative efforts around the coronavirus have thrust China’s hybrid activities to the center of trans-Atlantic debates. Policymakers need to seize the moment and respond by “using NATO more politically,” in Stoltenberg’s words. NATO is first and foremost about its nations. In the fight against China’s hybrid threats, these nations bring much more to the table than military power alone. They have access to a broad range of tools—military, political, economic, technological, and information—which the alliance can use to its collective geopolitical advantage in the competition with China. What NATO needs now is a strategy to leverage those tools in a coordinated manner. That will go a long way in solving NATO’s China problem.

#### Russian success spurs Chinese aggression---we solve best

Sascha Dominik (Dov) Bachmann et al 19, Professor, Canberra Law School, “Competition short of war – how Russia’s hybrid and grey-zone warfare are a blueprint for China’s global power ambitions ,” Australian Journal of Defence and Strategic Studies Vol. 1 No. 1, November 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract\_id=3483981

China’s territorial ambitions as a ‘hybrid threat’?

China has participated in more territorial disputes than any other state since the end of the Second World War.40 Many of these disputes could be considered expansionism, with the exception of Taiwan, which has remained a reunification objective of the People’s Republic of China (PRC) since 1949. The disputes include land border claims and counter-claims, such as with India, and arguments with Hong Kong over its separate legal system are also increasingly a source of tension. However, the primary focus of Chinese expansionism tends to be in the maritime environment with disputes over the Paracel and Spratly Islands in the South China Sea and the Senkaku Islands in the East China Sea.

The Chinese maritime disputes especially in the South China Sea are complex, involving multiple overlapping claims with other regional states but also with other stakeholders who seek peaceful resolution of claims and assurance of freedom of navigation. The establishment of military facilities on the islands, in breach of a ruling of its claim by The Hague, exacerbated the situation, leading US and other navies to conduct regular freedom of navigation exercises through the South China Sea.

In addition to China’s ambitions associated with territory in its direct proximity, China has developed a strategy for its future economy with the Belt and Road Initiative. Critics of this strategy assert that the associated infrastructure elements of the initiative are essentially an alternative means of securing key overseas territory, or a new form of colonialism.41 An obvious example of this strategy is China’s effective acquisition of the port of Hambantota in Sri Lanka.42

China’s approach to its territorial claims is one in which changes are implemented incrementally and thereafter become the new normal. Occupation of South China Sea islands is an example, in which China’s 2019 Defence White Paper characterises international freedom of navigation as ‘countries from outside the region… illegally entering China’s territorial waters… undermining China’s national security’.43

In a 2010 article, Fravel asserted that China was unlikely to resort to armed conflict or even aggressive expansionism in pursuing their territorial claims. 44 However, since that publication, we have seen examples in the East and South China Seas in which aggression has been clear, with challenges between military platforms and with conflict often narrowly averted.

Despite these tensions and occasional incidents, China’s conduct of expansionism in the South China Sea primarily has been in the grey-zone, in that each step has been calculated to achieve objectives without crossing a threshold of warfare. However, can we consider it to be hybrid warfare? That is, has the posturing of forces been complemented by other activities to achieve their goals? Hoffman regards China as being ‘well organized to conduct operations short of military conflict’45 utilising three forms of nonwarfare, namely noncontact (fei jierong), nonlinear (fei xianshi) and nonsymmetric (fei duicheng)’.46

Such influence activities are widely suspected to be behind the Philippines government’s softening of their stance against China in relation to the South China Seas dispute.47 Such influence may be overtly undertaken through incentives such as Belt and Road Initiative agreements, although there is evidence that such initiatives can have a covert element and take advantage of corrupt regimes.48 Influence can extend to attempted corruption of Western politicians to advocate for Chinese policies over the dispute.49 China more broadly exerts influence through a combination of political warfare activities, including mobilisation of diasporas, tasking of students, financial assistance to individuals and institutions, economic manipulation and large-scale cyber and other information operations.50

Hybrid Lawfare – exploiting the legal grey-zone of modern conflict

Hybrid warfare is an open concept with different elements. Lawfare, for example, is a new aspect of non-kinetic conflict aiming at ‘using law as a weapon to manipulate legal paradigms’.51

Lawfare is being used by Russia and China (in the context of the South China Sea as discussed in this article) both within and outside the scope of traditional armed conflict. For Russia the use of lawfare is ‘a continuation of its policy of using every tool at its disposal to achieve its political and geo-strategic goals’52 and a ‘force multiplier’ to meet its political, military and legal objectives, as highlighted in its Military Doctrine of 2014 and its National Security Strategy of 2015.

Both China and Russia have been active in the use and abuse of the rule of law in order to either prepare military action or to justify it after completion of the mission. Russian justification of the occupation and then subsequent annexation of Crimea is an example of the latter; while the Chinese justification for its claims over the South China Sea is an example of the preparation of a legal basis for the potential use of force in self-defence when protecting own sovereign rights and (island-) territory.

Lawfare in conjunction with hybrid warfare ‘provides a layer of “fake” legitimacy, or at least reduces the erosion of apparent legitimacy, due to the nonattributable aspects inherent in hybrid warfare while using “easy” hybrid warfare methods’.53 Lawfare can be used as a method of hybrid warfare or influence operations.54 US writer, Kittrie came up with the following test: (1) the actor uses law to create the same or similar effects as those traditionally sought from conventional kinetic military actions—including impacting the key armed forces decision-making and capabilities of the target; and (2) one of the actor’s motivations is to weaken or destroy an adversary against which the lawfare is being deployed.55

Russia’s use of lawfare in Ukraine thus exploits both (1) the undefined definition of the conflict as aggression and (2) the unwillingness of the international community to label it as such. And, it maintains uncertainty through a strategic (dis)information campaign which keeps the nature of the conflict open, so it is unclear whether it is international armed conflict, non-international armed conflict or civil unrest.56 Here clear parallels regarding China’s actions in the South China Sea can be drawn.

China and Russia’s use of the ‘weaponisation’ of the maritime environment as grey-zone tactics or consolidation of a hybrid warfare based approach

We are now turning to the example for such a lawfare approach: the so-called weaponising of the maritime environment through terraforming as part of a multifaceted security strategy. China’s Defence Minister, Wei Fenghe, argued in 2018 that, ‘The islands in the South China Sea have long been China’s territory. They’re the legacy of our ancestors and we can’t afford to lose a single inch of them’.57

Officially, China claims that its overall intention was to use the extension of its territorial waters peacefully and to serve solely its commercial needs. This is doubtful, given that China has actively weaponised the claimed territories. Sumihiko Kawamura, a former rear admiral and commander of Japan’s Maritime Self-Defence Force’s antisubmarine air wing, suspects that China wants to use the South China Sea as leverage against the US Pacific security projection. Kawamura believes Beijing is trying to turn the South China Sea into ‘a safe haven’ for its nuclear-powered submarines, which are armed with ballistic missiles that can reach the United States. 58

In this context, it is worthwhile to note that China did lose its case for claiming the SCS waters in a 2015 case brought before the UN Permanent Court of Arbitration by one of the affected states, the Philippines. China therefore failed spectacularly with its attempt to successfully use lawfare by manipulating the provisions of the United Nations Convention on the Law of the Sea to argue own sovereign rights (like exclusive economic and fishing rights) over the majority of the SCS waterways.59 China later decided to ignore the ruling and to consolidate its illegal position further by illegally maintaining, and even expanding, so-called Exclusive Economic Zones in the disputed SCS waters.60 This consolidation manifests itself in Chinese below the threshold grey-zone tactics like policing its falsely claimed territorial waters around artificially built islands, interference in air-traffic and challenging US and allied navies in their rightful freedom of seas navigation patrols, to name just a few examples.61 China has created, like Russia in respect to the illegally annexed Crimea, a fait accompli.

In Russia’s case, immediately following the annexation of Crimea in 2014, Russia began the planning and construction of the Crimean Bridge over the Kerch Strait in Ukraine to support its territorial claims. The project was successfully completed in May 2018 as the so-called Unification Bridge and was followed subsequently by Russian military action to ensure regional observance of the new status quo.62 Russian naval units attacked and boarded three Ukrainian vessels in autumn 2018 for having allegedly violated Russian territorial waters when passing through the Kerch Strait.63 What became known as the ‘Kerch Strait’ incident was followed by the effective closure of a part of the Sea of Azov waterway whenever Russia decided to conduct live fire naval exercise,64 thus violating Ukrainian territorial waters, as the annexation of Crimea was and continues to be regarded as illegal.65

Russia’s actions can be seen as consolidation action of its gains from its successful hybrid warfare campaign against the Ukrainian state when seizing Crimea. With the annexation complete and little to fear in terms of military action or meaningful sanctions, Russia can now resort to the use of traditional hard power in consolidating and protecting its position.

Both China and Russia have provided examples of how territorial gains made through hybrid warfare and grey-zone tactics can be weaponised further to serve wider national security aims and ambitions by warranting the question of how to respond in an effective manner.

Russian warfighting stratagems as dangerous precedent

The question arises of what is new in Russian warfare since 2008. Among a host of features of the new war some are indeed noteworthy: the non-declaration of war, the use of armed civilians, non-contact clashes like the blockade of military installations by ‘protestors’, the use of asymmetric and indirect methods, simultaneous battle on land, air, sea, and in the informational space, and the management of troops in a unified informational sphere.66

The authors have written extensively about hybrid warfare and its Russian equivalent as reflexive control67 and nonlinear warfare. Russian Hybrid Warfare has become known as the so-called ‘Gerasimov’ doctrine68— though while Western military authors (including us) continue to use this reference, it is at least questionable if General Gerasimov actually intended to have his thoughts and reflections on evolving Russian military operational approaches be regarded as a military ‘doctrine’ in a strict sense.69 So, while the existence of such a doctrine is debatable, the overall success of contemporary Russian warfighting is not, and the term hybrid warfare is a good characterisation of Russia’s contemporary aggressive foreign policy.

The actual consequences of Russia’s hybrid warfare are far-reaching. Russia’s foreign policy (and also China’s) of assertive nationalist posturing, meddling in internal affairs, political warfare, and hybrid warfare disrupt the Western narrative of globalisation, rule of law, democracy and interconnectivity. This creates an untenable situation where the West is responding to ad hoc threats in an increasingly less assertive way instead of defining and implementing a joint foreign policy that would deter such an adversary.

Russia’s version of hybrid warfare, whether we refer to it as Gerasimov’s doctrine, Russian Hybrid Warfare or reflective control, has been successful. Firstly, Russia proved successfully ‘that this warfare not only includes nonstate actors but also states’.70 Secondly, it proved the effectiveness of this form of warfare because Russia’s departure from its reliance on kinetic resources also reduced the need for using conventional military power in a conventional sense, which benefits the ‘weaker’ opponent. And thirdly, hybrid warfare as part of a wider information-operation and lawfare approach provided false legitimacy due to attribution questions and the potential for denial by the target state for political reasons. This Russian success with hybrid warfare is what China seems to be emulating in respect to its current territorial expansion: the use of ‘little blue men’, information operations, economic and diplomatic pressure and lawfare (which albeit failed).

### Innovation DA---UQ

#### US total factor productivity has been abysmal since the 70s.

Alexander Kersten 21, Deputy Director and Fellow, Renewing American Innovation Project, “Why Renewing American Innovation? The “Endless Frontier Act” and Biden’s Bid for Maintaining U.S. Global Competitiveness,” CSIS, https://www.csis.org/analysis/why-renewing-american-innovation-endless-frontier-act-and-bidens-bid-maintaining-us-global

Despite Silicon Valley and the millennial generation’s supposed penchant for innovative disruption, U.S. total factor productivity has been slowing since the 1970s. Productivity today is the lowest in more than a century. Innovation, historically a clear driver of U.S. productivity, means the creation of ideas and inventions that are translated into practical value and improve the quality of people’s lives directly or via their ability to grow the economy. Whether measured in terms of triadic patents (patents filed in the United States, Europe, and Japan), most available measures of productivity, or even startup company creation, the United States’ trademark innovative spirit has been gradually dampening for decades. And if not for China’s meteoric rise this century, the United States might still be sleepwalking—optimistically but without a serious plan—instead of waking up to the need for a coherent national strategy.

U.S. Complacency, and How We Got There

Noted George Mason University economist Tyler Cowen and other experts have recognized a growing “complacency” in American life as the indicator of a societal shift from the United States’ early dynamism. From the turn of the twentieth century until roughly the moon landing of 1969, the breakneck pace of groundbreaking technologies that directly affected the quality of life and the structure of U.S. society was simply astounding. Yet, since the first moon landing in 1969, only the internet and its application to more and more parts of our lives can claim to have made any meaningful impact—meaning that physically the world of 1969 is much more like that of 2021 than 1969 was of the early twentieth century. This, of course, is not meant to discredit the great advances in medicine and human genomics made in the last few decades, for example, but to show how the rate of society-changing innovations has not maintained the pace that existed from the mid-nineteenth century until roughly 1969.

In the developed world, this slowdown has unfortunately contributed to wage stagnation, the shrinking of the middle class, and greater political polarization domestically. Coinciding with the waning days of the Soviet Union’s power in the 1980s, the U.S. innovation decline was masked at home. Further, the Soviets of that period no longer posed a technological threat to the United States. Japan on the other hand, posed a great technological threat in the 1980s but was and is a staunch U.S. ally, and not a security threat. Unchallenged abroad and riding the dual-edged optimism of the internet boom of the 1990s and the victory over communism, the United States missed the ways in which it was giving up the advantages that made it such a powerhouse in the mid-twentieth century.

#### US manufacturing and high-tech innovation are both in deep decline.

Robert D. Atkinson 20, PhD, founder and president of ITIF, “How Nine Flawed Policy Concepts Hinder the United States From Adopting the Advanced-Industry Strategy It Needs,” ITIF, 8/10/20, https://itif.org/publications/2020/08/10/how-nine-flawed-policy-concepts-hinder-united-states-adopting-advanced

THE CASE FOR ACTION

Before describing the chain of logic that points directly to the need for an advanced-industry strategy, it’s important to lay out the case for some sort of action. In short: Over the last two decades, the U.S. economy has lost its competitiveness edge

Perhaps the most obvious sign of U.S. economic decline has been the erosion of the country’s manufacturing base. From 2001 to 2010, the United States lost 42,400 factories (three-quarters of which employed at least 500 workers while in operation), 32 percent of its manufacturing jobs, and much of its technical edge.1

Since then there has been further erosion. From 2007 to 2019, while GDP grew by 22 percent, real manufacturing value-added grew by just 5.6 percent. As a result, manufacturing’s share of gross domestic product (GDP) fell from 13.2 percent to 11.4 percent. This also obscures significant differences within industry sectors. All of the eight nondurable goods sectors (such as paper, chemicals, and plastics) produced less in absolute terms in 2019 than they did in 2007. Moreover, as a number of analysts—including the Information Technology and Innovation Foundation (ITIF)—have shown, the Bureau of Economic Analysis (BEA) significantly overstated the output growth of the computer sector (NIACS 334) because it assumes that when a computer doubles in speed due to Moore’s Law, actual output also doubles. Leaving out the production of computers—most of which has moved overseas—U.S. manufacturing output actually declined by 3 percent.

Just as troubling is that U.S. manufacturing is in a productivity slump. In 15 out of 18 years from 1990 to 2007, manufacturing productivity grew faster than overall non-farm business productivity, often by more than twice as much. But between 2008 and 2019, manufacturing productivity grew faster in just 3 of the 12 years. In 2019, while business productivity grew 1.9 percent, manufacturing productivity grew just 0.1 percent. One reason for this might be U.S. manufacturers increased capital expenditures by just 17 percent between 2008 and 2017 (the latest year for which data is available), or one-third the rate of the information sector (e.g., Internet, communications, etc.). Without robust productivity growth, manufacturing gets less competitive globally, which is why it grows more slowly than GDP.

One would think, with manufacturing productivity growing more slowly than the rest of the economy, job growth would be robust (and as other sectors become relatively more efficient). But at the end of 2019, manufacturing employment was still 6.5 percent below its pre-recession levels.

But even if America is losing manufacturing, surely it is still leading in innovation, right? So goes the thinking (as if manufacturing is not innovative). But on many measures, when controlling for the size of the economy—such as government and business research and development (R&D) expenditures and patenting—the United States is no longer the leader. It ranks 12th in patent cooperation treaty patents filed as share of GDP, 23rd in researchers per capita, 27th in high-tech exports as share of trade, and 44th in scientific and technical articles as a share of GDP.2 Moreover, in 2019, the United States ran an all-time-high trade deficit of $132 billion in advanced technology products, down from a $4.5 billion trade surplus in 2001.3 With China, the trade deficit in electronic products was $184 billion in 2017, as U.S. exports totaled just $21 billion.4

Also, many once-iconic U.S. advanced-industry firms have lost significant global market share or even gone out of business. Forbes issues a list of the top 2,000 firms each year. To be sure, from 2006 to 2019, a number of U.S. technology firms increased their global ranks significantly, particularly in software (e.g., Microsoft); semiconductors (e.g., Intel, Micron, and Nvidia); and Internet services (e.g., Facebook). But many hardware and related firms either lost ground or went out of business. Once-global leaders such as Lucent, Motorola, and Nortel (a Canadian firm that at one time employed thousands of U.S. workers) are now defunct. And leaders such as IBM, Hewlett Packard, Agilent (formerly part of HP), and General Electric all fell significantly. (See table 1.)

#### China is out innovating the US in the SQUO

Christopher Darby & Sarah Sewall 21, Christopher Darby, CEO of In-Q-Tel, National Security Venture Capital Arm, Sarah Sewall, Executive Vice President for Policy at In-Q-Tel. Formerly U.S. Undersecretary of State for Civilian Security, Democracy, and Human Rights, The Innovation Wars: America’s Eroding Technological Advantage, Foreign Affairs, https://www.foreignaffairs.com/articles/united-states/2021-02-10/technology-innovation-wars

THE CHINESE JUGGERNAUT

The changes in American innovation would matter less if the world had remained unipolar. Instead, they occurred alongside the rise of a geopolitical rival. Over the past two decades, China has evolved from a country that largely steals and imitates technology to one that now also improves and even pioneers it. This is no accident; it is the result of the state’s deliberate, long-term focus. China has invested massively in R & D, with its share of global technology spending growing from under five percent in 2000 to over 23 percent in 2020. If current trends continue, China is expected to overtake the United States in such spending by 2025.

Central to China’s drive has been a strategy of “military-civil fusion,” a coordinated effort to ensure cooperation between the private sector and the defense industry. At the national, provincial, and local levels, the state backs the efforts of military organizations, state-owned enterprises, and private companies and entrepreneurs. Support might come in the form of research grants, shared data, government-backed loans, or training programs. It might even be as simple as the provision of land or office space; the government is creating whole new cities dedicated solely to innovation.

China’s investment in 5G technology shows how the process works in practice. Equipment for 5G makes up the backbone of a country’s cellular network infrastructure, and the Chinese company Huawei has emerged as a world leader in engineering and selling it—offering high-quality products at a lower price than its Finnish and South Korean competitors. The company has been buoyed by massive state support—by The Wall Street Journal’s count, some $75 billion in tax breaks, grants, loans, and discounts on land. Huawei has also benefited from China’s Belt and Road Initiative, which provides generous loans to countries and Chinese companies to finance infrastructure construction.

Massive state investments in artificial intelligence have also paid off. Chinese researchers now publish more scientific papers in that field than American ones do. Part of this success is the result of funding, but something else plays a big role: access to enormous amounts of data. Beijing has fueled the rise of powerhouse companies that sweep up endless information about their users. These include Alibaba, an e-commerce giant; Tencent, which developed the all-purpose WeChat app; Baidu, which began as a search engine but now offers a range of online products; DJI, which dominates the consumer drone market; and SenseTime, which provides facial recognition technology for China’s video surveillance network and is said to be the world’s most valuable artificial intelligence company. As a matter of law, these companies are required to cooperate with the state for intelligence purposes, a broad mandate that is almost certainly used to force companies to share data for many other reasons.

That information increasingly involves people living outside China. Chinese companies have woven a global web of data-gathering apps that collect foreigners’ private information about their finances, their search history, their location, and more. Those who make a mobile payment through a Chinese app, for example, could have their personal data routed through Shanghai and added to China’s growing trove of knowledge about foreign nationals. Such information no doubt makes it easier for the Chinese government to track, say, an indebted Western bureaucrat who could be convinced to spy for Beijing or a Tibetan activist who has taken refuge abroad.

China’s hunger for data extends to some of the most personal information imaginable: our own DNA. Since the COVID-19 pandemic began, BGI—a Chinese genome-sequencing company that began as a government-funded research group—has broken ground on some 50 new laboratories abroad designed to help governments test for the virus. China has legitimate reasons to build these labs, but it also has an ugly record of forcibly collecting DNA data from Tibetans and Uighurs as part of its efforts to monitor these minorities. Given that BGI runs China’s national library of genomics data, it is conceivable that through BGI testing, foreigners’ biological data might end up in that repository.

Indeed, China has shown great interest in biotechnology, even if it has yet to catch up to the United States. Combined with massive computing power and artificial intelligence, innovations in biotechnology could help solve some of humanity’s most vexing challenges, from disease and famine to energy production and climate change. Researchers have mastered the gene-editing tool CRISPR, allowing them to grow wheat that resists disease, and have managed to encode video in the DNA of bacteria, raising the possibility of a new, cost-effective method of data storage. Specialists in synthetic biology have invented a new way of producing nylon—with genetically engineered microorganisms instead of petrochemicals. The economic implications of the coming biotechnology revolution are staggering: the McKinsey Global Institute has estimated the value of biotechnology’s many potential applications at up to $4 trillion over the next ten to 20 years.

Like all powerful technologies, however, biotechnology has a dark side. It is not inconceivable, for example, that some malicious actor could create a biological weapon that targeted a specific ethnic group. On controversial questions—such as how much manipulation of the human genome is acceptable—countries will accept different degrees of risk in the name of progress and take different ethical positions. The country that leads biotechnology’s development will be the one that most profoundly shapes the norms and standards around its use. And there is reason to worry if that country is China. In 2018, the Chinese scientist He Jiankui genetically engineered the DNA of twin babies, prompting an international uproar. Beijing portrayed him as a rogue researcher and punished him. Yet the Chinese government’s disdain for human rights, coupled with its quest for technological supremacy, suggests that it could embrace a lax, even dangerous approach to bioethics.

THINKING BIGGER

Washington has monitored China’s technological progress through a military lens, worrying about how it contributes to Chinese defense capabilities. But the challenge is much broader. China’s push for technological supremacy is not simply aimed at gaining a battlefield advantage; Beijing is changing the battlefield itself. Although commercial technologies such as 5G, artificial intelligence, quantum computing, and biotechnology will undoubtedly have military applications, China envisions a world of great-power competition in which no shots need to be fired. Technological supremacy promises the ability to dominate the civilian infrastructure on which others depend, providing enormous influence. That is a major motivation behind Beijing’s support for high-tech civilian infrastructure exports. The countries buying Chinese systems may think they are merely receiving electric grids, health-care technology, or online payment systems, but in reality, they may also be placing critical national infrastructure and citizens’ data in Beijing’s hands. Such exports are China’s Trojan horse.

### Innovation DA---Link Turn

#### Article 5 clarification key to enable operational planning

Piret Pernik 14, Researcher of Strategy Branch of the NATO CCDCOE, “Improving Cyber Security: NATO and the EU,” International Centre for Defence Studies, September 2014, https://icds.ee/wp-content/uploads/2010/02/Piret\_Pernik\_-\_Improving\_Cyber\_Security.pdf

Operational planning and capabilities development

A report by the defence committee of the UK parliament finds that NATO is poorly prepared to respond to the Russia’s use of asymmetric warfare, including cyber attacks, information and psychological operations. The committee urges the Alliance to develop its own asymmetrical warfare capabilities, discuss how to deal with these attacks and operations, and mount its own offensive operations.58 . It also calls NATO to re-examine the legal and military doctrines, criteria, and responses for the declaration and use of both Article 4 and Article 5.59 Likewise, James Stavridis, retired NATO's Supreme Allied Commander (SACEUR) believes NATO should stand up a cyber defence operations force under the SACEUR, as well as explore the utility of offensive cyber weapons.60 The need to integrate cyber into NATO’s military operations and operational planning has been acknowledged also by Jamie Shea.61 Operational planning both for Article 5 and non-Article 5 events along with capability development must be adjusted to the reality of asymmetrical or hybrid warfare that employs a range of tools, including information operations and cyber attacks.

In addition to the need to integrate cyber into both military and civil emergency operational planning, NATO must improve the interoperability of cyber capabilities of the Allies and this process can be facilitated by the means that will be provided by the newly established NATO’s cyber range.

Furthermore, realistic cyber threat scenarios, as well as clear and tested response procedures and mechanisms should be in place. Operational contingency plans must clarify which capabilities NATO nations are prepared to make available to the Alliance, and the mechanisms for collective assistance by the individual Allies. A full range of response options (including kinetic means) accompanied by appropriate plans and capabilities need to be worked out. Since a simultaneous strike against NATO’s own and the member state’s infrastructure is likely, it would be prudent to ensure enough common capabilities to respond to both tasks. The existing two small RRTS consisting of a permanent core of six experts may be inadequate for simultaneous tasks.

In order to enable military operational planning NATO should consider the development of cyber warfare doctrine. It should establish a joint cyber command or headquarters (not unlike the Special Operations Headquarters), aligning joint strategy with political ends, at Supreme Headquarters Allied Powers Europe (SHAPE). Concerns about the legality of an offensive action in cyberspace aside, while NATO does not have an offensive cyber capability, member states’ capabilities could be used under Article 5 circumstances. NATO needs to ponder also what could be done to help an Ally experiencing a cyber attack causing serious damage to its private critical infrastructure.

#### Setting a framework for cyber defense is also key to tech innovation

Marios Panagiotis Efthymiopoulos 19, designated Dean and Associate Professor of International Security and Strategy of the College of Security and Global Studies, at the American University in the Emirates AUE, “A cyber-security framework for development, defense and innovation at NATO,” Journal of Innovation and Entrepreneurship (2019) 8:12, https://link.springer.com/content/pdf/10.1186/s13731-019-0105-z.pdf

Setting the stage

Cyber-security is yet to be globally, legally, operationally, and strategically defined. The scale of a security perspective is more attractive at this time considering the geostrategic challenges and threats. The possibility of innovation and entrepreneurship in the field is also a tangible reality, due to the necessary research and development methods. More so, the possibility of an open market economy sharing of knowledge and technological skills makes security and cyber-security or defense for that matter more attractive. What lacks in the world wide legal and political framework of operations, exchange of information and protectiveness from new sources or methods that can be deemed as elements of infiltration.

The article’s aim is to examine and recommend a global strategic framework for operational capacity and management resilience between allied and cooperative partners in the field of cyber-security. The current article is a follow up of prior scientific publications made in 2014 first and later in 2018, on NATO’s cyber-security strategy, presented through a framework of Cyber-Development, Cyber-Democracy, and Cyber-Defense (Carayannis, Campbell & Efthymiopoulos, 2014; Carayannis, Campbell & Efthymiopoulos, 2018). The aim is to converge diversified information on cyber-security, in a single strategic framework; reflect to the actual practical needs in understanding operations and tactical ability to deliver in multi-complex and dimensional world through management and operational efficiency capabilities. The article requests interoperability of aims and objectives under a global framework of cyber-security; through a strategic framework on cyber-security, global law can be proposed, defined, and adopted by the international community. The strategic framework will define structures that are needed to be put in place on a global scale, when reflecting issues of cyber-security and inclusive for NATO. It will define threats and challenges, as cyber-attacks are real. Cyber-security is not an asymmetrical or hybrid threat, but an existential one. Its destructive capacity can be multi-leveled and can also lead to human casualties. The future of e-safety lays at both a global estimation framework of what constitutes cyber-security and how we react to it; it lays in between cooperation of allies and members of wider alliances, against specified or approximate threats. Yet, its framework of aims and objectives, management, command and control, and operations will be defined and decided by allied parties only such as is the case of NATO.

Operationally, national and cooperative forces need to be continuously agile and technologically advanced. In an asymmetrical world, which is complete with unforeseen challenges and threats, we need forces with flexibility, adaptability, operational and strategic command structure, based on high technologically sophisticated information “coming in,” but also being used while in training or through active operations.

On a theoretical scale, the current article requests a cyber-security strategic framework adoption of resilient adaptability and interoperability policy in the framework of safety and defense. The article considers that understanding the realities of threats is by definition a natural innovation and as we move ahead, we structure and operate a single strategy on cyber-security against a virtual threat from wherever it comes from. Its long-term resilience may be more complex as operational capacity needs to constantly develop and adapt into the convergence of societal structures, and methods; where socio-economic, technological, defense even health, and education issues are affected.

When theory on cyber-security, resilience, and operational capacity will be applied at NATOs level, it will enable allies and members, jointly, to create a true policy and strategy for cyber-security resilience against hybrid virtual threats. The methodology on how to is presented through this current article.

The article’s design is based on cross-disciplinary and interdisciplinary approaches. It combines elements of global security and strategy, national and international law, economic development, and technological research and advancement and most importantly is innovative and entrepreneurial; its understanding will enable us to comprehend global and regional market establishment and convergence, as also economic changes. The setting of the study required lapse of time to showcase the need and the necessity of the subject. Current output reflects a set of written analyses, rules, and primary experiences. It methodologically acquired sources of information of related necessity and relevance, shaped the understanding, and need to point out for a framework of rules, regulations, management, and operations on cyber-security.

The article and its author frames a specific policy recommendation with regards to the creation of not only a regional alliance (NATO-based scale), Cyber-Security Strategy for the twenty-first century but a global one. The article defines the “dynamism” of cyber-security both as a topic and subject. Cyber-security is a twenty-first century element of policy orientation; a necessity for both collective and individual defense and security resilience.

In specific, a cyber-security strategy for NATO will enhance its innovation and creativity core of operations and methodologies against any kind of virtual threats. It will set standards, policy procedures, and recommendations. NATO’s strategy of cyber-security through its new Cyberspace Operations Centre, in Mons (Belgium) as decided in the Brussels Summit of July 2018 (Cyber-Space Operations Center Mons Belgium, 2018) unfolds options and opportunities, innovation, and entrepreneurship in operations efficiency and capabilities application. Current technological advancements and dynamisms through innovation and sustainable futuristic advancement will soon be evident

### Innovation DA---AT: Resilience Solves AFF

#### AFF key to resilience

Marios Efthymiopoulos 19, PhD from the University of Crete in Security and Strategic Affairs on NATO issues and NATO-Russia relations, Chairman of the Board of Advisors of Strategy International, 6/24/19, "A cyber-security framework for development, defense and innovation at NATO", Journal of Innovation and Entrepreneurship, Volume 8, Article 12, https://innovation-entrepreneurship.springeropen.com/articles/10.1186/s13731-019-0105-z

Smart defense and more so in the field of cyber-security is NATOs main priority policy. It does however reflect as well on to the tools and mechanisms used to innovated in and for management operations, processes, and tactics. It allows for defense entrepreneurial thinking and application. Constant changes in strategy and policy do request efficient leadership and management skills to operate. And so, should NATO’s cyber-resilience strategic policy.

Through a methodological period, such as in the NATO Summit in Brussels of July 2018, NATO will now have to show an enhanced progress report within the second quarter of 2019, assuring current and future abilities also in cyber-security, to counter current and emerging challenges in cyber-space. Defense planning, operations, and lessons learned are therefore a continued process that allows the evolution of NATOs capabilities which always need to be taken into account and more so in the field of cyber-security where the Cyberspace Operations Center will play a key role into it.

Resilience through smart and cooperative innovative defense requires NATOs policy on Cyber-defense to be also effective. As said, it requires decision-making and leadership in this policy context. In the framework of cyber-defense, NATO needs to align supranationalized national capability priorities and standardize processes, through NATO processes. In the framework of cyber-resilience at NATO, policies on standing management of operations need to be agreed upon. Therefore, cooperative and consensus leveled agreements need to come forth; NATO should produce a cost-effective projection planning and application for all operational exercise theaters reflecting the real yet also virtual worlds.

Cyber-resilience and methodological specialization through leaders’ policy decisions at the level of Heads of States and Governments in operational planning and practically applied are key components of and for success for the Alliance, considering threat assessments. Resilience with coordinated efforts may lower costs, fiscal, administrative, and human, but will require developed technology infrastructure. It will guarantee national engagement of states to NATO policies, when correctly pointed out. Let us not forget that specialization as a key national policy is and will always remain a form of national interests, which examined changing variables based on geographical interests, strategic sharing of costs, technological information, and intelligence sharing or operating in regional or global environments.

## Politics DA Answers

### Politics DA---2AC

#### Secret agreement avoids the DA

Ashley S. Deeks 17, Associate Professor, University of Virginia Law School, “A (QUALIFIED) DEFENSE OF SECRET AGREEMENTS,” Arizona State Law Journal, https://arizonastatelawjournal.org/wp-content/uploads/2017/09/Deeks\_Pub.pdf

1. Secret Political Arrangements in U.S. Law

Section A identified a group of agreements that meet the definition of “treaty” found in the VCLT. But there are almost certainly many more secret arrangements that states do not intend to be governed by international law.35 In common parlance, these are political arrangements that happen to be secret. Some of these arrangements, which set out rules or modes of operation to be followed in one or more interactions between or among states, are surprisingly detailed. A paradigmatic example would be a secret memorandum of understanding (MOU) between the U.S. Defense Department and a foreign military agency to guide specific types of intelligence interactions.36 Other examples include arrangements between the CIA and its foreign counterparts and oral or tacit arrangements between the United States and foreign states, the legal status of which may be ambiguous. Pakistan’s reported consent to the U.S. use of armed drones to target individual members of al Qaeda in the Federally Administered Tribal Areas may reflect such a secret tacit arrangement.37 Some of these secret arrangements explicitly state that the parties do not intend them to create legally binding obligations.38

Compared to secret agreements (at least those to which the United States is a party), secret arrangements often are seen and approved by fewer people because the Executive has no statutory obligation to transmit them to Congress.39 The Case Act establishes a mechanism by which the Department of State (DOS) should be informed of these arrangements, so that the DOS can determine whether the arrangement is or is not an international agreement.40 However, it is not clear that each agency actually shares every one of its arrangements with the DOS. Some arrangements may be highly classified, which might make the initiating agency reluctant to share the arrangement’s contents. Alternatively, agencies may have worked out a modus vivendi with the DOS, whereby the DOS determines that certain categories of arrangements do not represent international agreements and thus effectively blesses another agency’s conclusion of such arrangements without DOS involvement.

#### AFF popular OR no one cares

Ted Galen Carpenter 19, senior fellow is security studies at the Cato Institute and a contributing editor to the National Interest, “NATO’s Dirty Little Secret Is Out,” CATO, 12/4/19, https://www.cato.org/publications/commentary/natos-dirty-little-secret-out

Few (if any) surveys of U.S. public opinion about NATO even hint about the extent of the risks Americans incur because of Washington’s obligations under Article 5 of the North Atlantic Treaty, which commits the signatories to consider an attack on any member as an attack on all. A typical poll question will ask respondents whether the United States should defend country X, if Russia attacks that country. A more honest question would be whether the United States should defend country X from a Russian attack, even if doing so might result in a nuclear war with Russia that could kill millions of Americans.

Granted, such an outcome is a worst‐​case scenario, but Washington’s Article 5 obligations bring it into play. The escalation risk is especially relevant with respect to defending Estonia and the other Baltic republics. A 2016 RAND Corporation study concluded that it would be nearly impossible for NATO to defend its Baltic members against a full‐​scale Russian invasion for more than a few days without an extensive upgrade of the Alliance’s existing force deployment. Even after such an upgrade, the outcome of a struggle waged solely with conventional weapons would be uncertain. Escalation to the nuclear level would remain an ever‐​present danger.

Even without a robust “truth in advertising” requirement, U.S. public support for NATO is slipping. Mark Hannah, a senior fellow at the Eurasia Group Foundation, concedes that point following a survey his organization recently conducted. He notes: “For a second year in a row, when faced with a hypothetical scenario in which Russia invaded Estonia, a NATO ally, Americans were roughly split on whether they wanted the United States to respond militarily. And that was after respondents were reminded of Article 5, the part of the NATO treaty that obligates the United States to respond to such aggression, and after they were told that U.S. action could be the only way to expel Russia.”

In other words, even with wording designed to elicit positive responses—and no disclosure of a potentially dire nuclear risk arising from America’s military obligation to a NATO ally—the survey showed no clear public mandate for defending that ally. Hannah concludes: “It’s not just President Donald Trump who is skeptical of the North Atlantic alliance, in other words. It’s the American people. To the extent that U.S. citizens think about NATO at all, they disagree about whether honoring its commitments would be worth the sacrifice.” He’s correct, and if they were explicitly told about the nuclear risk, it is highly probable that anti‐​NATO sentiment would surge.

### No Link---Not Perceived

#### Foreign policy doesn’t matter on the political stage

Dr. James M. Lindsay 20, Senior Vice President, Director of Studies, and Maurice R. Greenberg Chair at the Council on Foreign Relations, MA, MPhil, and PhD from Yale University, AB in Economics and Political Science from the University of Michigan, “Campaign Foreign Policy Roundup: Foreign Policy Is AWOL”, Council on Foreign Relations, 9/11/2020, https://www.cfr.org/blog/campaign-foreign-policy-roundup-foreign-policy-awol

Today on the nineteenth anniversary of September 11 it is notable how little of the 2020 presidential campaign has been about foreign policy. It’s not just terrorism that has receded from the headlines. The same could be said about China, Russia, Iran, and a whole host of other issues.

To an extent, the fact that foreign policy has been AWOL on the campaign trail isn’t surprising. Domestic issues typically dominate presidential campaigns, and COVID-19 is perhaps the mother of all domestic issues. It has upended the economy, disrupted daily life, and exacerbated existing racial and social inequalities. Even so, it was only a few months ago that some experts were speculating that COVID-19 would catapult U.S. policy toward China to the forefront of the campaign and give Donald Trump a cudgel with which to beat Joe Biden. So far that hasn’t happened.

This state of affairs seems to fit the public mood. A Pew survey of registered voters conducted this summer found that 57 percent of registered voters said that foreign policy was “very important” to them when voting. That sounds like an impressive figure, but 79 percent of respondents flagged the economy as “very important” and 68 percent flagged health care. Voters accord even less importance to specific foreign policy issues. Pew reported that just 42 percent of respondents said climate change was important to their vote, and it didn’t even bother to ask about terrorism.

#### Small shifts don’t trigger political waves.

Alex Seitz-Wald 19, Political reporter for NBC News, "Trump's Facing Crises Around The World. So Why Aren't Democratic Candidates Talking About Foreign Policy?," NBC News, 5/19/2019, https://www.nbcnews.com/politics/2020-election/democratic-candidates-aren-t-talking-about-foreign-policy-why-cone-n1007131

But among Democratic primary voters, there's little interest. A recent NBC News/Wall Street Journal poll found just 11 percent of respondents said national security and terrorism should be the top priority of the federal government, down from 21 percent at a similar point in the last presidential election cycle. And those questions rarely get put to candidates by voters as they visit the early voting states around the country. "It's hard to get people to care about foreign policy, generally," said Tommy Vietor, a former Obama national security spokesperson who now hosts Pod Save the World, a foreign policy spinoff of the popular Pod Save America podcast. But he predicted candidates won't be able to avoid the issues forever and noted that foreign policy is the one place where presidents can implement their vision without worrying too much about Congress or the courts. "It's surprising to me how much time candidates spend debating policy that they may never end up getting through Congress when, on foreign policy, as president, you have full latitude to act on your own," he said. One reason is that few of the Democratic presidential candidates have much experience in international relations and may feel more comfortable sticking to familiar domestic turf, especially when voters aren't demanding it. It used to be accepted as fact that no one could win the White House without passing the "commander-in-chief test," which meant projecting strength, a steady hand and expertise on national security, but recent elections have scrambled the rules of American politics. Clinton twice tried and failed to exploit the test. First, in 2008 against Obama, her campaign produced an ad asking voters if they wanted Obama, an inexperienced freshman senator from Illinois, answering a 3 a.m. phone call about a global crisis. Then, Clinton and her allies tried in 2016 when they borrowed the mushroom cloud page from Lyndon Johnson's playbook to question Trump's temperament. In both cases, her successful opponents countered that they had better judgment on world affairs, even if she had more experience. Stephen Miles, the director of Win Without War, a progressive national security coalition, said Trump was effective in 2016 by painting Democrats as defenders of a creaky foreign policy establishment that had led to endless wars, controversial trade deals and pointless foreign aggression. In 2020, he said, candidates should offer an alternative not only to Trump, but also to the old way of doing things. "Trying to defend the failed status quo is not going to fly, so what is your take?” he said. But he pointed to some candidates who have started to take steps to do that, even if it's far from being the centerpieces of their campaigns. Sanders has given some speeches on foreign policy, hired a well-known adviser and pushed congressional resolutions against the Trump administration’s policy toward the Yemeni civil war. Sen. Elizabeth Warren, D-Mass., who joined the Senate Armed Services Committee a few years ago in part to bolster her limited foreign policy experience, recently has become more active on that panel and laid out her vision in a speech and article in Foreign Affairs. And while many Democrats may not agree with her worldview, longshot contender Rep. Tulsi Gabbard, D-Hawaii, a military veteran, has made foreign policy central to her presidential bid. But the candidate with by far the most experience in that realm is former Vice President Joe Biden. When speaking, he weaves in stories about world leaders and mockery of Trump's warmth to North Korean leader Kim Jong Un. "I know all the world leaders," Biden said in an interview with a South Carolina NBC affiliate. "I'm the guy that told the Chinese that when they set up these air defense zones, we're going to fly right through them." Jesse Lehrich, a foreign policy spokesperson on Clinton's 2016 campaign, summed it up: "I get it — Democratic primary voters aren't clamoring for detailed plans on countering terrorism in the Sahel. But there's a real opportunity to put forward an affirmative vision of American leadership."

### No Link---AT: Polling

#### Their polling is flawed

Ted Galen Carpenter 19, senior fellow is security studies at the Cato Institute and a contributing editor to the National Interest, “NATO’s Dirty Little Secret Is Out,” CATO, 12/4/19, https://www.cato.org/publications/commentary/natos-dirty-little-secret-out

Few (if any) surveys of U.S. public opinion about NATO even hint about the extent of the risks Americans incur because of Washington’s obligations under Article 5 of the North Atlantic Treaty, which commits the signatories to consider an attack on any member as an attack on all. A typical poll question will ask respondents whether the United States should defend country X, if Russia attacks that country. A more honest question would be whether the United States should defend country X from a Russian attack, even if doing so might result in a nuclear war with Russia that could kill millions of Americans.

# CP Answers

## Top Level

### Now Key

#### Now is key

Erica D. Lonergan & Sara B. Moller 22, Lonergan is an assistant professor in the Army Cyber Institute and a research scholar at the Saltzman Institute of War and Peace Studies at Columbia University; Moller is a former Eisenhower Fellow at the NATO Defense College and will be joining the Center for Security Studies at Georgetown University later this year, “NATO’s Credibility Is on the Line with its Cyber Defense Pledge. That’s a Bad Idea.,” Politico, 4/27/22, https://www.politico.com/news/magazine/2022/04/27/nato-credibility-cyber-defense-pledge-russia-ukraine-00027829

With little chance of improved NATO-Russian relations any time soon, time is of the essence to get this right. The allies should begin the hard political legwork now to ensure members get on the same page before NATO’s June summit, if not sooner. Achieving consensus on significant cyber issues has previously taken time. NATO’s attribution of the Microsoft Exchange hack last summer to China was an important step for the alliance and sent a strong signal to our adversaries. But it took months to reach agreement on the statement; the hack was uncovered in March 2021 and the NATO statement was not made public until July. In the current crisis, the alliance will not have the luxury of waiting four (or more) months to agree on a response. To avoid incurring damaging costs to NATO’s credibility and its deterrent powers, the allies should refine their cyber policy, now.

### Legal Ambiguity Bad

#### Legal ambiguity causes escalating attacks---clarity deters hybrid attacks and reduces risk of miscalc

Michael Schmitt 17, Professor of International Law at the University of Reading in the United Kingdom, “Tallinn Manual 2.0 on the International Law of Cyber Operations: What It Is and Isn’t,” Just Security, 2/9/17, https://www.justsecurity.org/37559/tallinn-manual-2-0-international-law-cyber-operations/

Moreover, understanding the points about which application and interpretation are subject to disparate views allows States to focus their efforts where clarification of the law is needed and in their national interest. Such clarification will help deter other States from exploiting these grey zones in the law of cyberspace. For instance, Russia has very adroitly operated within this grey zone, as in the case of its operations in the Ukraine and, more recently, in respect of interference in the U.S. elections by means of the DNC hacks and the subsequent release of emails via Wikileaks and other outlets. In the latter case, an active debate surrounds whether the Russian operations satisfy the “coercion” element that is necessary to establish an act of prohibited intervention under international law. Such grey zones allow for maneuver space in the sense that the cyber operations in question cannot be definitively styled as unlawful, thereby weakening any international blowback that might result.

Some argue that clarity in the law is counterproductive, as ambiguity allows for tactical, operational, and strategic-level leeway. The flaw in this argument is that it ignores the principle of sovereign equality. When States operate in the grey zone, they open the door for other States to do likewise, including when conducting operations against the former States.

My view is that normative clarity lends stability to international relations by laying out “the rules of the game” by which every State must play. It contributes to deterrence because internationally wrongful acts may be responded to by means of countermeasures (acts that would be unlawful but for the fact that they respond to another State’s internationally wrongful act). This being the case, States will know that their actions risk costs rising above the level of retorsion (e.g., sanctions and the expulsion of diplomats). Additionally, clear rules may prevent escalation because the “game” becomes more understandable to the participants. They lower the chance that the States involved in a cyber exchange will misinterpret the actions of their opponents.

### US Lead Key

#### US lead-initiatives in NATO key to norm building for cyber

Angelo Sanakli 20, writer at IAR, 4/30/20, "America Should Engage Like-Minded Partners for a Safer Cyberspace", International Affairs Review, https://iar-gwu.org/2020/04/30/america-should-engage-like-minded-partners-for-a-safer-cyberspace/

The United States and twenty-six other nations came together during last year’s United Nations General Assembly to issue a call-to-action on making cyberspace safer. This came after the United Nations rolled out two independent norm-building processes on advancing responsible behavior in cyberspace. Yet conflicting interests suggest that nations will not be able to reach consensus on new rules in either process anytime soon. The United States should instead engage like-minded partners to work towards making cyberspace safer for all nations.

Resolutions passed in 2018 established the Open-Ended Working Group (OEWG) and the Group of Governmental Experts (GGE). The OEWG, supported by nations including China, Russia, and Iran, is a new norm-building process with membership open to all nations. The GGE, backed by the United States and like-minded partners including Australia, France, Germany, Japan, South Korea, and the United Kingdom is part of a long-standing existing process with membership limited to twenty-five nations. Neither group has yet to reach consensus on new norms.

The last set of norms came in 2015 during a previous GGE. It set out that nations should not carry out cyber acts that seek to intentionally damage other nations’ critical infrastructure, such as power grids, water supplies, and financial services. The GGE process came to an abrupt end in 2017 owing to considerable push back from China, Russia, and Cuba. They opposed majority positions on the right to self-defense and the application of international humanitarian law, which regulates the humanitarian aspects of armed conflict. Conflicting interests on rules on, or related to, “free internet” and “cyber sovereignty” will continue to play out in both GGE and OEWG talks. Future push-back will only continue to stifle progress on norm-building. So what does this mean for the United States?

The United States needs to engage like-minded partners. They not only share like interests but play a vital role in projecting American interest abroad. Take for example how the North Atlantic Treaty Organization (NATO) broadened its collective defense commitment to include provisions for “cyber attacks” in 2014, or how the United States and Japan similarly broadened their mutual defense commitment in 2019. Here’s what the United States and like-minded partners should do next:

Reinforce existing norms: Like-minded partners should introduce enforcement procedures for nations that don’t abide by existing norms. They should affirm that there are consequences for bad behavior in cyberspace. Some possible examples of enforcement include facilitating robust information-sharing to thwart other nations’ wrongful cyber acts and developing defensive and offensive joint cyber operations. Nations that don’t follow the rules must know that they will be held accountable.

Develop new norms: Like-minded partners should also develop new norms, especially where OEWG or GGE consensus is unlikely. Some possible examples of norm-building include the right to respond to wrongful cyber acts in self-defense and the application of international humanitarian law in armed conflicts involving cyberspace. The progress on norms must be wrapped into both OEWG and GGE talks to push consensus in the right direction.

Norm-building on cyberspace remains controversial. Some will say that working with like-minded partners undermines United Nations processes. Yet existing norms are a clear indication that these processes protect the United States’ interests and make cyberspace safer for all nations. The OEWG or GGE talks will not reach consensus anytime soon, therefore the United States should press ahead with like-minded partners all the sooner.

The United States needs to step up and lead. It needs to engage like-minded partners. It needs to reinforce existing norms and develop new ones to affirm that there are consequences for bad behavior in cyberspace. The United States can’t risk the possibility of adversaries at the forefront of norm-building. This is an opportunity for American leadership to make cyberspace safer for all nations.

## Advantage CP Answers

### Interoperability Deficit

#### CP can’t solve interoperability

Dominika Kunertova 20, postdoctoral research fellow at the Center for War Studies in Denmark. With a Ph.D. in Political Science from Université de Montréal, she researches trans-Atlantic security and defense cooperation, NATO-EU relations, and military technology, “CAN THE NEW ‘MAGI’ SAVE NATO?,” War on the Rocks, 4/24/20, https://warontherocks.com/2020/04/can-the-new-magi-save-nato/

You Can’t Buy Interoperability

In contrast to statistical engineering that aims to adjust numbers to fit the desired “fair share,” true burden-sharing would put emphasis on defense capabilities and operational readiness. Shifting the emphasis away from abstract macroeconomic numbers to practical cooperation based on strategic needs should inform the content (which capabilities to buy), not only the form (defense spending levels), of burden-sharing debates. This highlights the problem that allies cannot just buy interoperability, as it requires enhanced cooperation and coordination. Although interoperability is considered the alliance’s core business, it has not been systematically treated in the burden-sharing debate. In addition, burden-sharing that includes the mutual-aid dimension would further refine the cash, capabilities, contributions — or “three C’s” — framework regularly mentioned by the current NATO secretary-general.

The current defense spending narrative is thus a symptom of empty formalism in NATO that reflects a lack of clarity about the alliance’s purpose, and favors statistical deceptions over effectively implementing the mutual commitment to defend each other. A February 2020 poll by the Pew Research Center revealed a worrying trend: While NATO is generally seen in a positive light across publics within the alliance (a median of 53 percent view NATO positively, though with double-digit percentage point declines in Germany and France over the past 10 years), many in 16 surveyed NATO countries seem reluctant to fulfill Article V collective defense obligations. A median of 50 percent across 16 NATO member countries is against their country defending an ally, while only 38 percent express willingness to come to help a fellow ally.

Future Defense Spending in Peril right, especially in the context of the short- and long-term consequences of the ongoing COVID-19 pandemic. While the scope of the economic impact is still unclear, it is likely to reshuffle financial priorities in NATO countries. Defense ministries will find it more difficult to reach the 2 percent spending level by 2024 or even to maintain the current defense expenditures programs. Moreover, with economies put to halt and eventual drops in national GDP, even if countries fulfill the 2 percent pledge, they could end up spending less in real terms. If NATO members continue to frame fairness in terms of the 2 percent defense spending target, it will further aggravate the burden-sharing problem, seriously test NATO solidarity, and ultimately endanger the alliance’s ability to adapt to the increasingly unpredictable security environment and the changing nature of security threats.

Improving NATO’s cohesion and its political role will not happen overnight or through high-level political declarations. If there are any lessons to be learned from the Three Wise Men’s effort back in 1956, it is that perseverance, personal relationships and reputation, pragmatism, and humility matter a great deal.

### AT: New START Plank---2AC

#### Extending New START fails and turns the DA

Michaela Dodge 19, Research Scholar at the National Institute for Public Policy, “New START Sunk by Old Problem – Russian Cheating,” Heritage, 5/29/19, https://www.heritage.org/europe/commentary/new-start-sunk-old-problem-russian-cheating

Analysts at the Brookings Institution have called extending the New Strategic Arms Reduction Treaty (New START) a “no brainer.” In reality, the United States is better off letting New START expire.

The arms control treaty with Russia was negotiated in 2010 — five years before Moscow dismembered Ukraine — by an administration that assumed Russia was no longer an adversary.

That assumption led to a treaty hopelessly lopsided in Russia’s favor. Consider this: It did not require Russia to eliminate a single warhead. Instead, it allowed Russia to increase its countable nuclear warheads, even as it made the United States continue to draw down.

Proponents of New START argue that the treaty’s verification provisions provide an important element of transparency between two countries. There is a grain of truth to that — the provisions increase transparency, but they have little to do with verification. In fact, they make it hard to detect Russia’s potential noncompliance.

For example, New START does not provide a basis to learn how many warheads Russia deploys on each of its intercontinental ballistic missiles (ICBMs). The Obama administration negotiated away telemetry provisions that would allow us to get an insight into this important characteristic.

Moreover, warheads in maintenance facilities and systems away from a base are off-limits to inspectors, further diminishing our understanding of the composition of Russia’s nuclear forces. Inexplicably, the treaty also allows concealment activities on ICBM bases.

These lackluster verification provisions mean that even if Russia cheated on New START, it would be almost impossible for the United States to find out about it and then charge Russia with violating the treaty. And Moscow has a long record of disregarding treaty obligations.

Indeed, Russia has cheated on almost every arms control agreement it has ever signed. Its blatant deployments of intermediate-range ballistic missiles led to the demise of the Intermediate-Range Nuclear Forces Treaty. Russia killed a British citizen and poisoned three others by using a chemical weapon, despite having ratified the Chemical Weapons Convention.

The notion that Moscow was no longer a national security headache was naive in 2010. After all, Russiahad invaded Georgia in 2008 and had never ceased making nuclear threats against U.S. allies.

Today, that notion is even more far-fetched, what with Russia’s occupation of Crimea, its ongoing military aggression in Ukraine and its destabilizing adventurism in Syria.

Forget about a Russian “reset.” The era of a great power competition is back, and Russia is serious about winning. Its nuclear forces are about 80 % modernized now and will be pretty close to 100 % modernized by next year, according to Gen. John Hyten, commander of U.S. Strategic Command.

Moreover, Russia is building new nuclear weapons outside of the New START: a new ICBM capable of carrying multiple nuclear warheads, a nuclear cruise missile, and an autonomous nuclear-armed underwater torpedo. The relevance of New START decreases every day.

Perhaps New START’s greatest flaw, however, is that it left Russia’s tactical nuclear weapons unscathed. It’s a huge problem, because Russia has at least a 10:1 advantage in this class of weapons. To make matters worse, Russia seems keen on adopting and exercising strategies that envision using tactical nuclear weapons first in conventional conflict — as a way to communicate resolve and make the United States back down.

### AT: Hotlines---2AC

#### Hotlines don’t solve conflict---Russia will suspend their use in conflict

Hananh Levintova 17, reporter at Mother Jones, 4/7/17, "Russia Threatened to Shut Down the “Deconfliction” Hotline. Here’s Why That’s Terrifying.", Mother Jones, https://www.motherjones.com/politics/2017/04/deconfliction-hotline-syria-trump-russia/

Following the US attack on a Syrian airbase overnight, Russian officials expressed outrage. Russia, which is allied with Syrian dictator Bashar al-Assad, denounced the missile strikes as a “violation of the norms of international law.” Russia also took an even more ominous step, announcing that it would be shutting down the “deconfliction” hotline it shares with the United States.

The deconfliction hotline may sound obscure, but it’s actually a key channel through which the two countries communicate about their military activities in Syria. The US and Russia are backing different sides in Syria’s civil war; the US and its allies are attacking ISIS (and now Assad), while Russia is attacking Syrian rebels. This creates the potential for an unintended incident between US and Russian forces to escalate into a larger conflict between the two powers. The hotline helps prevent that from happening by allowing both sides to coordinate their planes in Syria’s crowded airspace, avoiding collisions.

#### The CP is unnecessary because hotlines exist now---only question is whether they’ll be used

Matthew Robinson 18, 4/13/18, "US-Russia hotline ‘ACTIVE’ to avoid escalating conflict over Syrian air strikes", Express, https://www.express.co.uk/news/world/945422/world-war-3-Russia-US-hotline-active-avoid-escalation-conflict-Syrian-air-strikes

RUSSIA has claimed a secure hotline between the US and the Kremlin is “active” and being used by both nations to communicate their planned operations and military responses in Syria following the chemical attack in Douma.

## T---Security Cooperation

### T---SC---2AC

#### We meet:

#### 1. FUNCTION---the DOD does the plan even if other actors are involved.

#### 2. TEXT---plan text in a vacuum is most objective, alternatives incentivize vagueness.

#### COUNTER-INTERPRETATION: “Security cooperation” is not only DOD action and includes Security Assistance. Their interpretation is in the context of the DOD and doesn’t assume how other agencies function.

Albert Zaccor 5, Colonel in the US Army and Atlantic Council Senior Fellow, August 2005, “Security Cooperation and Non-State Threats: A Call for an Integrated Strategy,” https://www.files.ethz.ch/isn/46290/2005\_08\_Security\_Cooperation\_and\_Non-State\_Threats.pdf

Defining Security Cooperation28

Security Cooperation is a Department of Defense (DOD) term that refers to "...all DOD interactions with foreign defense establishments to:

• Build defense relationships that promote specific U.S. security interests;

• Develop allied and friendly military capabilities for self-defense and coalition operations, including allied transformation;

• Improve information exchange and intelligence sharing to harmonize views on security challenges; and

• Provide U.S. forces with peacetime and contingency access and en route infrastructure."29

Security Cooperation is not the same as Security Assistance. The latter term refers only to programs such as Foreign Military Financing (FMF), Foreign Military Sales (FMS), the International Military Education and Training Program (IMET), and other programs governed by the Foreign Assistance Act and managed by the Defense Security Cooperation Agency. The Department of State plays a key role in providing policy direction for Security Assistance programs. Security Cooperation is a much broader term that, in addition to Security Assistance, includes such categories of activities as combined exercises, combined training, combined education, military-to-military contacts, humanitarian assistance, and information operations.30 It also refers to the planning process DOD organizations use to implement these activities.

In essence, the Security Cooperation planning process is a systematic method for translating strategic guidance into programmatic objectives. The Office of the Secretary of Defense issues annual Security Cooperation Guidance (OSD SCG) to guide the planning and activities of Unified and Specified Commands, the military services, and other DOD agencies and actors.31 The SCG promulgates strategic objectives based on security themes derived from the National Security and Defense strategies. It also provides regional and country priorities, objectives, and measures of effectiveness for assessment.32 The Unified and Specified Commands, the services, and other DOD players develop subordinate plans to execute Security Cooperation activities in support of OSD's objectives. The Unified Commands, for example, develop regional strategies and country plans to guide the implementation of security cooperation activities in their Areas of Operation.33

It is an oft-repeated mantra that in order to defeat transnational terrorism, and by extension other related non-state threats, the United States must apply all the elements of national power, including diplomatic, informational, military, and economic.34 The OSD SCG directs that DOD Security Cooperation "will be integrated with other elements of national power.. .in order to achieve national security, defense, and foreign policy objectives."35 This formulation, while helpful, obscures two key facts. First, Security Cooperation includes activities that by their very nature involve the simultaneous application of more than one element of national power. Security Cooperation at a minimum requires the combination of diplomatic relations, military assistance, military-to-military contacts, and public diplomacy. In other words, Security Cooperation is itself an application of at least three of the classic elements of national power.36 Second, DOD is not the only entity in the USG that interacts with foreign governments to achieve the stated objectives: relationships, capabilities, information and intelligence, and access. The Department of State, the Intelligence Community, and to a lesser extent, other departments and agencies, conduct activities aimed at the accomplishment of these objectives, broadly understood. There is, however, no common USG, or interagency, definition or concept of Security Cooperation.37 We will return to this issue in the final section of this paper. For the purposes of the present discussion, this paper offers the following working definition of Security Cooperation:

Security Cooperation refers to all USG assistance provided to foreign law enforcement, security, and defense establishments in support of national defense, security, and foreign policy objectives.38

#### PREDICTABILITY---DOD definition is arbitrary.

Albert Zaccor 5, Colonel in the US Army and Atlantic Council Senior Fellow, August 2005, “Security Cooperation and Non-State Threats: A Call for an Integrated Strategy,” https://www.files.ethz.ch/isn/46290/2005\_08\_Security\_Cooperation\_and\_Non-State\_Threats.pdf

Part III of this paper offered a definition of Security Cooperation that could be common to the entire USG, not just the Department of Defense. The USG interagency has no such common definition because it lacks a common conceptual understanding of how to translate higher level strategic guidance into specific programs designed to accomplish strategic objectives.

The Department of Defense, despite its size, its diversity, and the scope of its Security Cooperation activities, has such a common understanding. DOD's process is not without its flaws.113 During the late 1990s and the early 21st century, however, the department has successfully established a rational set of procedures for translating the strategic guidance in the National Security, Military, and, now, Defense Strategies, into specific programs executed by the military commands, services, and defense agencies.114 This process promotes discipline by forcing subordinate organizations to demonstrate that their Security Cooperation activities directly support specific objectives in the higher-level strategies. Efforts are under way to discipline the process further by establishing an assessment mechanism to provide feedback on the effectiveness of programs and activities.115 One reason for the success of the DoD program is oSD's publication of periodic Security Cooperation Guidance. This document, in addition to providing authority for subordinate organizations' Security Cooperation activities (see more below), serves the purpose of an informal doctrine, stipulating not only the "what," but the "how" and the "why" of Security Cooperation.116

In order for the USG interagency to plan and execute Security Cooperation programs and activities in an integrated and synergistic manner, a doctrine, or common conceptual framework, for Security Cooperation is necessary. Such a doctrine would have to define what Security Cooperation is, and, what it is not.117 It would have to define precisely which departmental and agency programs qualify as Security Cooperation and outline a procedure for combined interagency planning, programming, and execution. Armed with such a common conceptual framework, executive branch officials and program managers will be better equipped to engage in integrated planning and program execution. True success in this effort, however, will depend on the resolution of the other problems of authority, funding, and process and organization.

[Footnote 117]

As has been suggested here, activities to improve foreign partners' security capabilities conducted by any department or agency would qualify as Security Cooperation. In contrast, general foreign development assistance, although related to security and part of broader U.S. foreign policy, would probably not. Even within DOD, this is not totally clear. Officials in OSD's Counter-proliferation Policy office refused to admit that activities intended to improve the maritime security capabilities of Azerbaijan and Kazakhstan in support of counter-proliferation would be included under the definition of Security Cooperation and declined to integrate their program formally with other DOD Security Cooperation efforts.

#### AFF GROUND---limiting the AFF to the DOD eliminates core affs like arms sales, training, and information sharing which require the guidance and resources of other agencies.

#### NEG GROUND---affs still include the DOD, granting the neg the DOD PIC and trade-off DA, and including other actors gives the neg more PIC and DA ground.

#### GRAMMAR---the resolution says, “The USFG should…” the USFG isn’t only the DOD.

#### REASONABILITY---good is good enough.

# NEG

## Deterrence Turns

### OCOs Turn---1NC

#### Limiting commitment hurts OCOs---turns the case

Ion A. Iftimie 20, Eisenhower PhD Candidate Fellow, NATO Defense College, and Senior Advisor, European Union Research Center, George Washington University School of Business, “NATO’s needed offensive cyber capabilities”, NDC Policy Brief, No. 10, May 2020, http://www.ndc.nato.int/news/news.php?icode=1441

Over the past decade, Allies have identified a steep increase in cyber activities targeting the critical infrastructure sectors that NATO military operations rely upon. Directly or indirectly, these malicious cyber activities can also disrupt the Alliance’s logistics and forward operations. NATO’s commitment to “operate and defend itself ”5 in the cyber domain as effectively as in the geographic domains came, thus, as a direct recognition of cyber as a hybrid threat to both the Allies and the Alliance.

Compared to the air, land and sea domains, the cyber domain is not constrained by national borders (although certain physical aspects of it might be located within them). This distinction between the cyber and the geographic domains is important to note, because NATO was founded in response to external military threats without the right to intervene in internal security matters, where member states maintain the monopoly over the use of force. In the cyber domain, the distinction between internal and external security threats is harder to ascertain. When integrating offensive cyber capabilities into its defence and deterrence mandate, NATO would inevitably tackle certain aspects inherent to internal security; and yet, not legally infringe on the sovereignty of the Allies as long as effects amounting to force or intervention are not employed against the physical systems residing in these nations.6 Operating in the cyber domain requires, thus, that member states better integrate their offensive cyber capabilities into NATO operations not just to win future wars, but also to avoid elements of friction between Allies, which may arise from unilateral cyber effects to defend critical infrastructure.

NATO’s adversaries in the cyber domain

Warfare in the cyber domain is already conducted against NATO member states by both state and nonstate actors. It is also conducted by NATO member states against these external threats. Within the Alliance, however, offensive cyber effects are not yet part of the mission planning process and integration of national offensive cyber capabilities into joint NATO operations is voluntary. Integrating these national offensive cyber capabilities into NATO operations, thus requires, not only a clear understanding of these capabilities, but also agreement on the cyber threat environment, characterized by the intent and capabilities of NATO’s current and/or potential future adversaries.

#### Effective OCOs contain all conflict---anything else escalates.

Ion A. Iftimie 20, Eisenhower PhD Candidate Fellow, NATO Defense College, and Senior Advisor, European Union Research Center, George Washington University School of Business, “NATO’s needed offensive cyber capabilities”, NDC Policy Brief, No. 10, May 2020, http://www.ndc.nato.int/news/news.php?icode=1441

All future military confrontations are expected to be fought with cyber weapons. These offensive cyber capabilities in the hands of adversaries pose a significant threat to the military forces and critical infrastructure of NATO member states; and the Alliance recognizes that cyber-attacks (as hybrid threats) can be as damaging as conventional ones. This is because malicious cyber activities against computers that control physical processes can be as dangerous as threats that are purely physical in nature and could lead to explosions, nuclear meltdowns, blackouts, or financial crises. As put by NATO Secretary General, “in just minutes, a single cyberattack can inflict billions of dollars’ worth of damage to our economies, bring global companies to a standstill, ~~paralyze~~ our critical infrastructure, undermine our democracies and ~~cripple~~ our military capabilities”.4

Over the past decade, Allies have identified a steep increase in cyber activities targeting the critical infrastructure sectors that NATO military operations rely upon. Directly or indirectly, these malicious cyber activities can also disrupt the Alliance’s logistics and forward operations. NATO’s commitment to “operate and defend itself ”5 in the cyber domain as effectively as in the geographic domains came, thus, as a direct recognition of cyber as a hybrid threat to both the Allies and the Alliance.

Compared to the air, land and sea domains, the cyber domain is not constrained by national borders (although certain physical aspects of it might be located within them). This distinction between the cyber and the geographic domains is important to note, because NATO was founded in response to external military threats without the right to intervene in internal security matters, where member states maintain the monopoly over the use of force. In the cyber domain, the distinction between internal and external security threats is harder to ascertain. When integrating offensive cyber capabilities into its defence and deterrence mandate, NATO would inevitably tackle certain aspects inherent to internal security; and yet, not legally infringe on the sovereignty of the Allies as long as effects amounting to force or intervention are not employed against the physical systems residing in these nations.6 Operating in the cyber domain requires, thus, that member states better integrate their offensive cyber capabilities into NATO operations not just to win future wars, but also to avoid elements of friction between Allies, which may arise from unilateral cyber effects to defend critical infrastructure.

NATO’s adversaries in the cyber domain

Warfare in the cyber domain is already conducted against NATO member states by both state and nonstate actors. It is also conducted by NATO member states against these external threats. Within the Alliance, however, offensive cyber effects are not yet part of the mission planning process and integration of national offensive cyber capabilities into joint NATO operations is voluntary. Integrating these national offensive cyber capabilities into NATO operations, thus requires, not only a clear understanding of these capabilities, but also agreement on the cyber threat environment, characterized by the intent and capabilities of NATO’s current and/or potential future adversaries.

State adversaries in the cyber domain include Russia, China and/or Iran. These are countries known to be building offensive cyber capabilities specifically for the purpose of using them against NATO member states.7 In Russia’s case, cyber attacks were conducted against the critical infrastructure of NATO member states and partner nations, as for example against US energy infrastructure in 2017 (including against a nuclear powerplant near Burlington, Kansas)8 or against the Ukraine power grid in December 2015. China has also been conducting persistent cyber espionage using offensive cyber capabilities against core military and critical infrastructure of NATO member states for years. For this reason, the US Secretary of Defense, Mark T. Esper, remarked at the 2020 Munich Security Conference that the 5G Huawei infrastructure is a serious threat to NATO.9 Lastly, Iran’s offensive cyber capabilities have also been observed during multiple attacks against the critical infrastructure of NATO partner nations in the Middle East.

### Overview---2NC

#### Allied OCOs are inevitable

Ion A. Iftimie 20, Eisenhower PhD Candidate Fellow, NATO Defense College, and Senior Advisor, European Union Research Center, George Washington University School of Business, “NATO’s needed offensive cyber capabilities”, NDC Policy Brief, No. 10, May 2020, http://www.ndc.nato.int/news/news.php?icode=1441

At the 2016 NATO Summit in Warsaw, cyberspace was recognized as an operational domain in which NATO military forces must be able to maneuver as effectively as they do on land, at sea and in the air. Since then, Allies have conducted several successful offensive cyber operations1 against non-state adversaries, such as Daesh. Due to technological transformations in recent years, cyber is no longer viewed by NATO and its member states only as a hybrid threat, but also as a weapon in its own right and as a force multiplier2 in current military operations. Over the next two decades, NATO will look for new ways to integrate cyber weapons (or offensive cyber capabilities) into its operations and missions.3

#### The only question is if they’re unilateral or collectively integrated---unilateral OCOs cause cyber fratricide

Ion A. Iftimie 20, Eisenhower PhD Candidate Fellow, NATO Defense College, and Senior Advisor, European Union Research Center, George Washington University School of Business, “NATO’s needed offensive cyber capabilities”, NDC Policy Brief, No. 10, May 2020, http://www.ndc.nato.int/news/news.php?icode=1441

The lack of integrated offensive cyber A2/AD capabilities undermines both the unity of the Alliance and its mandate of defence and deterrence. On the former, the lack of coordination between Allies during unilateral cyber operations could lead to friction when resulting effects infringe on Allied cyber-physical infrastructures. It could also lead to cyber fratricide, when failure to properly attribute Allied digital personas occurs during these military operations. On the latter, while most Allies are developing offensive cyber capabilities, some remain unable to face the growing number of cyber threats unilaterally.

### UQ---NATO OCOs Now

#### NATO’s OCOs posture is being developed under the assumption Article 5 response to cyberattacks is unlimited

Patrick Tucker 19, Tech editor @ Defense One, 5/24/19, "NATO Getting More Aggressive on Offensive Cyber", Defense One, https://www.defenseone.com/technology/2019/05/nato-getting-more-aggressive-offensive-cyber/157270/

In the latest signal NATO is adopting a tougher posture against cyber and electronic attacks, Secretary General Jens Stoltenberg this week said that the defensive alliance will not remain purely defensive.

Stoltenberg told attendees at the Cyber Defence Pledge conference in London, “We are not limited to respond in cyberspace when we are attacked in cyberspace.”

NATO members have already “agreed to integrate national cyber capabilities or offensive cyber into Alliance operations and missions,” he said. But the parameters of a NATO response to cyber attacks remains undefined. In 2015, Stoltenberg said that a cyber attack against one member nation could trigger an Article 5 collective response by all members. Yet only once has a collective response ever been invoked, at the request of the United States following the attacks of September 11, 2001. NATO is a defensive organization, so what an offensive cyber posture looks like remains something of a mystery. An Article 5 response can take many different forms.

That’s the strength of the article, according to NATO Deputy General Secretary Rose Gottemoeller. However, while an Article 5 response can be unpredictable, it must be coordinated, which can be tricky with many different partners in possession of many different capabilities.

At an event in May, Gottemoeller said NATO was in the processes of establishing a new innovation board to “bring together all of the parts of and pieces of NATO that have to wrestle with these new technologies to really try to get a flow of information. Many of you having served in any international institution or government, you know how things can get stove-piped. So we are resolved to break down those stove-pipes, particularly where innovation is concerned,” she said.

#### US limitation shapes strategy

Patrick Tucker 19, Tech editor @ Defense One, 5/24/19, "NATO Getting More Aggressive on Offensive Cyber", Defense One, https://www.defenseone.com/technology/2019/05/nato-getting-more-aggressive-offensive-cyber/157270/

NATO is building a cyber command that is scheduled to be fully operational in 2023 and will coordinate and conduct all offensive cyber operations. Until then, whatever NATO does offensively, it will rely heavily on the United States and the discretion of U.S. commanders, according to Sophie Arts, program coordinator for security and defense at the German Marshall Fund, who explains in this December report.

“Yesterday’s remarks indicate that NATO’s leadership is thinking more seriously about buttressing the alliance’s deterrence posture in cyberspace and address threats that fall under the threshold of an Article 5 violation,” she told Defense One.

“This tracks recent shifts in strategy adopted by several NATO allies, including the United States, which integrate offensive cyber operations as an important tool to proactively address growing instances of cyber interference from hostile actors.”

But Arts points out there is no field manual for coordinating cyber offensive operations among individual allies, including big players in cyber like Estonia, the U.K. and the United States, who keep command and control over their assets.

In 2017, Gregory Edwards, then director of infrastructure services at NATO’s communication and information agency laid out what that might look like. “You could make a case-by-case decision” about responding to attacks, he said. “You need to have a policy that says, ‘if our operation is disturbed, we will take a specific action.’ The action will be listed. It will be listed what things the commander is allowed to do in that regard. It will be a specific action.”

### Link Wall---2NC

#### Limiting Article 5 in response to cyberattacks prevents NATO from successfully executing collective OCOs---

#### 1) Commitment---interpreting Article 5 broadly is why NATO is doing OCOs to degrade adversary capabilities---but there’s no need to counter-strike when attacks aren’t defined as threatening---that’s 1NC Iftimie

#### 2) Planning---limiting commitment prevents integration and coordination

Ion A. Iftimie 20, Eisenhower PhD Candidate Fellow, NATO Defense College, and Senior Advisor, European Union Research Center, George Washington University School of Business, “NATO’s needed offensive cyber capabilities”, NDC Policy Brief, No. 10, May 2020, http://www.ndc.nato.int/news/news.php?icode=1441

NATO Cyber Rapid Reaction teams are already equipped to conduct defensive cyber operations in support of member states if called upon. A mandate of cyber defence and security implies, however, that NATO also starts to engage in active military measures to deny, degrade, disrupt, deceive, or destroy an adversary’s offensive cyber capabilities. This requires the development of not only offensive cyber A2/AD capabilities by Allies, but also the restructuring of the NATO command structures, policies, processes (procurement, intelligence, operations, etc.) and engagements needed to integrate them by the Alliance. NATO coordination with both national and regional entities charged with cyber security aspects will, in particular, need to be enhanced. Many agreements already exist in the realm of defensive cyber at national and regional levels (as seen with the 2016 NATO-EU Technical Arrangement on Cyber Defence), but political consensus among Allies is missing on whether they should be expanded to incorporate the collective use of offensive cyber A2/AD capabilities.

#### 3) Signal of deterrence—access to a full range of capabilities across all operational domains is key

Ion A. Iftimie 20, Eisenhower PhD Candidate Fellow, NATO Defense College, and Senior Advisor, European Union Research Center, George Washington University School of Business, “NATO’s needed offensive cyber capabilities”, NDC Policy Brief, No. 10, May 2020, http://www.ndc.nato.int/news/news.php?icode=1441

Speaking at the Cyber Defence Pledge Conference in London in May 2019, NATO Secretary General highlighted that for deterrence to have full effect against state and non-state adversaries, NATO and its member states must be ready to use the full range of capabilities at their disposal, to include national offensive cyber capabilities. Deterrence is the act of diminishing an adversary’s intent by highlighting the excessive costs for the said adversary if it proceeds with an undesired action. In NATO’s case, deterrence is achieved by highlighting to an adversary the excessive costs delivered through military means in the event of an attack against Allies. For deterrence to be successful, the adversary must believe that NATO is ready and willing to impose these excessive costs across all operational domains, to include the cyber domain. This may call for Allies to develop offensive cyber capabilities and integrate them with NATO operations in order to collectively impose a high enough cost to deter adversaries from aggressive behaviour. To avoid escalation to total war and cyber fratricide during the fog of war, Allies must also agree on a list of Flexible Deterrent Options meant to allow for a gradual increase of pressure in the cyber domain, and then hopefully limiting the scope and intensity of conflict in this domain. NATO Flexible Deterrent Options in the cyber domain could include (as presented in Figure 1):

#### It's effectively deterring major cyberattacks now, but the plan derails it

Peter Ramjug 22, Journalist at Northeastern University, "Russia Hasn’t Launched a Massive Cyberattack on Ukraine Yet. Why Not?,” Northeastern University, 3/7/22, <https://news.northeastern.edu/2022/03/07/ukraine-russia-cyberattack/>

More than a week into war and Russia has yet to unleash a paralyzing, large-scale computer network attack on Ukraine. U.S. banks are bracing for retaliatory cyberstrikes that have yet to materialize. Even Volodymyr Zelenskyy, Ukraine’s president, continues to post videos.

What has happened to Moscow’s much-heralded cyber-warfare capabilities?

For starters, “they’re not as sophisticated as many people make them out to be,” says Northeastern’s David Wesley, who teaches graduate-level courses in global strategy and culture in the D’Amore-McKim School of Business. “It’s actually the West that is crippling the Russian computer systems.”

Microsoft, in the span of just a few hours, detected and thwarted a data-wiping attack on Ukraine’s network days after the war started. American enterprise rushing to the rescue in times of war was reminiscent of how Ford quickly pivoted its assembly lines during World War II to build tanks, jeeps, and airplanes.

Russia may also be reluctant to start a cyberwar for fear of getting attacked back, adds Luis Dau, associate professor of international business and strategy.

“They don’t want a war on two fronts if they don’t have to,” he says. “They’re finding the war on Ukraine harder than they were expecting.”

Western governments and companies—and the Ukrainian government itself—have beefed up their computer defenses since 2017, when a sinister ransomware program known as NotPetya infiltrated the servers of Maersk, the Danish cargo-shipping giant. The program destroyed servers and computers around the globe.

Had it not been for a lone company server in the African nation of Ghana that lost power and thus wasn’t connected to the rest of the network, the situation could have been much worse. “That’s what saved Maersk but it was by accident,” says Wesley.

“Instead of $300 million, it would have been billions of dollars in damage,” he adds.

Two years later, in August 2019, Ukrainian officials launched the new Ministry of Digital Transformation, which is working on cryptocurrencies, blockchain, and offensive hacking capabilities.

“We are creating an IT army,” the ministry’s 31-year-old leader tweeted over the weekend. It directed cyber devotees to a Telegram channel—“itarmyofurraine”—that instructed followers on how to disable Russian websites. Russia’s largest stock exchange as well as a government-owned bank and the Russian Foreign Ministry were taken offline after being targeted by Ukrainian hackers.

Ukrainian ministry officials have also been working with the Anonymous hacking collective to take down Russian sites.

“If you go to almost any Russian website, they’re offline,” says Northeastern’s Wesley. “So the threat against Russia of cyberattacks is much higher now than it is against us.” But, he warns, “that doesn’t mean the threat isn’t there. It’s still really serious.”

Periodic web outages have been reported in Ukraine since hostilities began, but nothing approaching the size and devastation of the Maersk attack, one of the worst cyber breaches ever. Maersk employees reportedly noticed “Ooops your files are encrypted” messages appearing on their laptops before screens systematically went black one-by-one company-wide.

Wesley, Dau, and Alexandra Roth, an executive professor of international business and strategy at Northeastern, authored a case study to be used in international strategy courses to teach students about responding to global threats such as cyber warfare and regional disputes.

The June 2017 Maersk incident was likely collateral damage from an attack on Ukraine, which “has long been a testing ground for Russia’s cyber capabilities, and it was no coincidence it all started on the Ukrainian Independence Day,” Roth says.

Most computer network attacks, they say, have the greatest impact on antiquated operating systems such as the one Maersk was using. At a minimum, companies should have a broad approach that includes regular upgrades and patches.

Ignoring those steps could be costly.

Maersk executives were focused on issues such as inflation, trade, and fluctuating energy prices, but “failed to recognize that a cyberattack posed a far greater threat on its critical infrastructure,” the professors wrote in the case study.

The U.S. banking system wouldn’t make the same mistake.

It has been guarding its networks for years, investing massive sums on technology and people to build a wall around its most important data.

Even with those precautions, big institutions such as JP Morgan, Citigroup, and Bank of America have seen a wave of recent cyberattacks that they describe as a subtle but intensified assault, the New York Post reported. The attacks have ramped up since the U.S. imposed sanctions against Russia over the invasion of Ukraine.

But it’s not the big banks that have to worry about a Russian-fueled security breach, say Northeastern professors. It’s the smaller regional banks, credit unions, and hospitals.

“It’s an existential crisis for these smaller organizations,” Wesley says. “The larger ones are much better protected.”

Elon Musk, the South African-born billionaire founder of Tesla and SpaceX, has been outspoken about the invasion of Ukraine. He has come to Ukraine’s defense by shipping Starlink satellite internet stations to keep communications lines open.

Musk warned that Russian forces could still target the terminals.

“Starlink is the only non-Russian communications system still working in some parts of Ukraine,” Musk tweeted, “so probability of being targeted is high. Please use with caution.”

That goes back to the Northeastern professors’ beliefs that the combined efforts of Western technology makes Russia no match for the West.

“Our capabilities are much stronger than many people believe,” says Wesley.

The big question now surrounding a digital attack on Ukraine revolves around NATO’s Article 5, which is based on a collective defense mindset if one country is targeted, says Roth.

“So if a critical infrastructure gets hurt and if it causes physical damage similar to a conventional kinetic attack, then this is pretty clear that NATO will step in,” she says, something that may make Moscow think twice. Ukraine is not a member of NATO, but several of its neighbors are.

### Link Wall---Collective Key

#### Collective action is key to OCO success

Paul M. Nakasone 20, Commander of U.S. Cyber Command, Director of the National Security Agency, and Chief of the Central Security Service, Michael Sulmeyer, Senior Adviser to the Commander of U.S. Cyber Command, 8/25/20, "How to Compete in Cyberspace: Cyber Command's New Approach", Foreign Affairs, https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity

For all their power and results, however, cyberspace operations are not silver bullets, and to be most effective, they require much planning and preparation. Cyber Command thus works closely with other combatant commands to integrate the planning of kinetic and nonkinetic effects. Cyber Command’s capabilities are meant to complement, not replace, other military capabilities, as well as the tools of diplomacy, sanctions, and law enforcement. And they are often used in cooperation with foreign military partners, who bring different skills and techniques to the table. The West’s united front against the Soviet Union kept the Cold War cold; likewise, today, the United States and its allies are building unity of purpose to promote respect for widely held international norms in cyberspace.

### Link Wall---AT: Resiliency Turn

#### OCOs are better than declaratory policies at incentivizing build-up of resiliency

John Carlin 18, former assistant attorney general for the National Security Division at the Justice Department where he did lead the investigation on the Sony attack, currently chairs Morrison And Foerster’s global risk and crisis management team, interviewed by James A. Lewis, Director and Senior Fellow, Strategic Technologies Program, Center for Strategic and International Studies, 3/19/18, "Responding to Russia: Deterring Russian Cyber and Grey Zone Activities", CSIS, <https://www.csis.org/analysis/responding-russia-deterring-russian-cyber-and-grey-zone-activities>

MR. CARLIN: And I don’t want to underestimate that it’s important to have a declaratory policy. But I would firmly agree with Jim. We had one. We declared it. We’ve declared it now multiple times in the context of specific actions, and then not acted. And that has a – the inverse effect of encouraging future action. So I think less time right now on figuring out the exact words of a go-forward declaratory policy, and more focus on putting points on the board and executing a response to the actions that have already taken place in violation of numerous statements from two administrations that really agreed on very little – very little else.

#### The best defense is a good offense

Paul M. Nakasone 20, Commander of U.S. Cyber Command, Director of the National Security Agency, and Chief of the Central Security Service, Michael Sulmeyer, Senior Adviser to the Commander of U.S. Cyber Command, 8/25/20, "How to Compete in Cyberspace: Cyber Command's New Approach", Foreign Affairs, https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity

This doctrine of persistent engagement reflects the fact that one-off cyber operations are unlikely to defeat adversaries. Instead, U.S. forces must compete with adversaries on a recurring basis, making it far more difficult for them to advance their goals over time. For example, publicly releasing adversary malware obtained during hunt forward missions to the cybersecurity community makes that malware less effective because defenses can be tuned to detect and defeat it. Additionally, cyber effects operations allow Cyber Command to disrupt and degrade the capabilities our adversaries use to conduct attacks.

#### Resiliency takes too long

Jim Miller et al 18, president of Adaptive Strategies, member of the Defense Science Board at the Atlantic Council, previously co-chaired the Task Force of Cyber Deterrence, being interviewed by James A. Lewis, Director and Senior Fellow, Strategic Technologies Program, Center for Strategic and International Studies, 3/19/18, "Responding to Russia: Deterring Russian Cyber and Grey Zone Activities", CSIS, <https://www.csis.org/analysis/responding-russia-deterring-russian-cyber-and-grey-zone-activities>

MR. LEWIS: No, I think you need to split it into two parts. And so on the resilience side, I’m a little gloomier, in that I don’t – ten years is probably an optimistic estimate. So I do think – so I used to make fun of deterrence, and I still do at some levels, but I think you have to convince potential attackers – and we have four – that the risk of doing something to U.S. critical infrastructure is outweighed by the cost. And that’s part of what we’re talking about today, is how do we identify costs that could apply to people?

On the social media side, I think there’s this question of what does intermediation look like? What does the ability to impose new standards on the new media look like? And, you know, some people have said, well, Facebook needs to go out and hire 3,000 editors. They probably don’t need to do that, but how do we encourage people to begin to identify the false information. That’s probably something you can do with technology. But how do we do it in a way that’s respectful of freedom of speech? And so it’s a very intentionally complicated issue, because no U.S. government agency has the authority to go and say: This is – this is fake news. This is false. So it’s something that we’ll have to either change the laws or find incentives for the companies.

MR. LEDGETT: I do think that there’s a role for the government in terms of helping identify the provenance of a story and helping to identify – you know, the first time this story appeared was in this place, to our knowledge. And so that’s input to a process that I agree the government can’t run. But I think that – and, John, you would be the expert on this. But I think that, you know, they could add a paragraph to the 39-paragraph end user license agreement that nobody reads that says: Hey, we are going to exercise our judgement and we’re going to flag, you know, things that we believe are suspicious or don’t look factual. And you agree to let us do that.

MR. LEWIS: How would you break – how would you avoid a tit for tat cycle? What would you do to – this is not going to be a one-move game, right? So we’ve experienced things. I think we all agree we should do something back. And I’m fairly confident that other side will not say, OK, we give up. So we are going to get into an iterative process here. How do we control that? And I don’t know if escalation dominance is the right way to think about it. That’s a nice nod to Herman Kahn. But what is it we do to get out of the cycle of just tit for tat? And you’ve seen this in – certainly in some of the terrorist cases, certainly in the Israeli experience. It doesn’t do you any good to get into response – a counter-response cycle.

MR. MILLER: I agree with that. And it’s true within cyberspace. It’s because, as was noted earlier, we are more vulnerable than Russia in cyberspace. That does not necessarily need to be the case forever. I do think 10 years is probably on the optimistic side for hardening, but it’s not the optimistic side for increasing our offensive capability, which is – which is, I’ll say, non-trivial, even today. One of the challenges we need to just have in the foremost of our mind as we think about U.S.-Russia tit for tat is that the high end of the escalation ladder is thermonuclear war, right? And so taking steps to show that we have limited aims, even though we’re responding strongly, keeping open channels of communication, taking note of fire breaks.

### Impact---Terror

#### Terror scenario

Ion A. Iftimie 20, Eisenhower PhD Candidate Fellow, NATO Defense College, and Senior Advisor, European Union Research Center, George Washington University School of Business, “NATO’s needed offensive cyber capabilities”, NDC Policy Brief, No. 10, May 2020, http://www.ndc.nato.int/news/news.php?icode=1441

NATO adversaries in the cyber domain also include non-state actors, such as terrorist organizations. The US and the UK have conducted several successful offensive cyber operations against those entities. These offensive cyber operations had a significant force multiplier effect, in conjunction with conventional actions on the ground, at sea, in the air and from space, that contributed to the defeat of Daesh in both Iraq and Syria.10 Today, most Allies are building offensive cyber capabilities needed to deny adversaries the freedom of maneuver in the cyber domain.

The use of area denial weapon systems in the cyber domain

Anti-Access/Area Denial (A2/AD) weapon systems have traditionally been used by NATO and its member states to prevent an adversary’s freedom of maneuver on land, sea or air. In the geographic domains, these capabilities include land mines, missiles (cruise, ballistic, surface to air, anti-ship, etc.), submarines, electronic warfare, and even Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) weapons. In the cyber domain A2/AD is achieved through offensive cyber operations.

Those operations have already been used for the purpose of achieving A2/AD by NATO member states in the cyber domain. This is the case of the US-led Operation Glowing Symphony (OGS), where “the United States Cyber Command reportedly acquired administrator passwords to [Daesh] websites. The passwords enabled deletion of digital content, including videos used for recruitment, from cyber infrastructure located in at least five countries outside actively hostile areas of Iraq and Syria. Similar digital content reportedly resided on cyber infrastructure in as many as 30 other States. Changing the passwords reportedly locked IS administrators out of the websites”.11 OGS restricted Daesh’s freedom of maneuver on networks physically residing in Iraq and Syria (which were controlled by the terrorist group), but also worldwide, where a NATO member state (the US) achieved denial of service effects against Daesh.

OGS disrupted Daesh propaganda through content removal from servers residing in multiple countries and through restricting access to physical infrastructure needed to store digital data. Combined with operational successes against ISIL on the ground, OGS actions resulted in propaganda efforts being significantly reduced on several global social media platforms, including Twitter. One particular offensive cyber operation acted, ipso facto, as an A2/AD platform where a NATO member state restricted access to physical networks critical for Daesh recruitment, training, radicalization, fundraising, and command and control.

### Redlines Bad---1NC

#### The plan’s redlines incentivize adversary probing that escalates

Z’hra M. Ghavam 16, Lieutenant Commander, United States Navy, “NATO’s Preparedness for Cyberwar,” Naval Postgraduate School, September 2016, <https://www.hsdl.org/?abstract&did=801548>, p. 46-48

NATO’s publicly declared policy on cyber threats is consciously and purposefully vague.207 Why? Strategic ambiguity has its benefits. According to the Atlantic Council panel, there is no “redline” or “determined threshold” that would automatically define a cyber act as an act of war.208 Leaving the rules undefined affords NATO ample room in which to operate. For a 28-member multinational organization that operates on the principle of consensus, time and latitude for solidifying strategic-level decisions are critical. If NATO publicized a cyber redline, it would box the Alliance into a corner. This kind of policy could embolden cyber offenders and provoke massive intrusions that target NATO’s networks at just below this threshold. Having a defined redline could also invite nefarious cyber actors to cross it to test NATO’s resolve, damage its reputation as a leader in Euro-Atlantic security, and undermine the credibility of its Article 5 commitments.

Following the Wales Summit in 2014, NATO affirmed its stance on law and cyberspace while refusing to address cyber redlines:

Our policy also recognizes that international law, including international humanitarian law and the UN Charter, applies in cyberspace. Cyber attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm, therefore, that cyber defense is part of NATO’s core task of collective defense. A decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis.209

### Redlines Bad---2NC

#### The plan’s redline cause adversary probing that escalates---Russia and other actors will target just below the threshold, knowing that it definitely won’t cause Article 5 activation AND they’ll cross it to test resolve---that’s Ghavam

#### Ambiguity deters aggression by introducing uncertainty into adversary’s calculus---clarity causes provocations that go nuclear

James Joyner 10, Managing Editor of the Atlantic Council, “NATO's Cyber Threat”, The National Interest, 7/2/2010, https://nationalinterest.org/print/commentary/natos-cyber-threat-3590

That seems reasonable enough and is certainly a matter that deserves discussion within NATO. Indeed, I have it on good authority, it’s in fact being discussed frequently. But, while it makes sense for the allies to draw up contingency plans and reinforce their cooperation and capabilities in this burgeoning arena, we should stop short of formally declaring what precise set of circumstances would allow Article 5 to be invoked.

First, doing so would put the members in a bind. A cyber attack might technically meet the theoretical definition put forth in advance without the actual circumstances generating consensus for any number of reasons. Perhaps the aggrieved party will be perceived to have provoked the attack by belligerence—belligerence that would actually be encouraged by an a priori declaration of support.

Or perhaps the risks of retaliation simply outweigh the damage done by the attack because of complicating circumstances. This is hardly unthinkable given that the most probable nation-state aggressors are Russia and China.

Regardless, the allies would then be forced to choose between the credibility of NATO and their own short-term interests. It’s an untenable position far more likely to harm the alliance and its members than to ward off the cyber threat.

Second, there’s tremendous value in strategic ambiguity. This was commonly understood during the Cold War, when the United States refused to declare that it would not engage in first use of nuclear weapons. While our leaders almost certainly had no intention of launching a first strike, they knew that declaring this formally would make a conventional attack—which could be expected to escalate to a nuclear war—more likely.

In the cyber case, drawing a bright line for potential adversaries virtually invites actions just short of casus belli. By instead simply declaring that there may be circumstances in which NATO will consider a cyber attack on one of its members an attack on all—but not spelling out what those circumstances may be—those contemplating such an attack will have an additional risk factor to deter them.

The North Atlantic Council should simply come to an understanding that the charter’s 1947 language requiring an “armed attack” to invoke collective defense is dated and that flexibility is needed for emerging threats. Plus, they should agree to increase cooperation in this arena and streamline the process by which consultation under Article 4 can take place.

#### It also causes future overreaction---NATO will be forced into conflict when adversaries go beyond

Ken M. Jones 15, Master’s Degree from the Naval Postgraduate School, “Cyber War: The Next Frontier for NATO”, Calhoun: The NPS Institutional Archive, March 2015, https://core.ac.uk/download/pdf/36737331.pdf

Finally, NATO needs to maintain ambiguity on what justifies an Article 5 response. As mentioned previously, ambiguity has served NATO well. A set threshold for when NATO will invoke an Article 5 response to a cyber-attack on a member country is not necessary. This ambiguity has historically served the alliance well, as demonstrated by the 9/11 attacks. If the alliance had said weapons were only include guns, bullets, tanks, and bombs, it would have set a threshold precluding a NATO response to attacks that turned four planes into improvised missiles. The larger issue of ambiguity is that there is no set definition of what constitutes an armed attack and what circumstances dictate a collective response, as per Article 5. Remaining ambiguous on the severity threshold of a cyber-attack allows the alliance to act in cases of future cyber-attacks that cause severe damage, but also allow NATO to refrain from over-reacting, even if an event is a cyber, or kinetic, attack as per a definition. It would be a mistake to set a threshold for attacks that cannot currently be anticipated.

#### The plan accelerates Russian cyber probing---adversaries will test redlines and circumvent escalation thresholds

Łukasz Kulesa 19, Deputy Head of Research at the Polish Institute of International Affairs (PISM). "The Future of Deterrence: Effectiveness and Limitations of Conventional and Nuclear Postures." https://carnegieeurope.eu/2019/11/28/future-of-deterrence-effectiveness-and-limitations-of-conventional-and-nuclear-postures-pub-80440

NATO needs to be careful about defining and signaling its redlines. Making these boundaries too specific could embolden adversaries to intensify their actions below NATO’s declared threshold of response. Being deliberately ambiguous and raising the fear of retribution may be more useful for encouraging adversaries’ self-restraint.

At the same time, NATO should aim to deter specific types of particularly threatening unconventional activities. These include major and sophisticated cyber attacks against allies’ military forces and critical military and civilian infrastructure, proxy military and special forces operations, and state-sponsored terrorism. NATO could declare that such activities may lead it to invoke Article 5 and respond in various ways, including asymmetrically (for example, the response to a cyber attack may not involve only cyber capabilities).

The alliance must be able to identify early whether and when unconventional and hybrid gray-zone actions have become a more substantial and coordinated campaign. In such a case, NATO should aim to deter the adversary from escalating further. This requires increasing the alliance’s capacity to share early-warning intelligence and pool national intelligence-gathering, investigation, and attribution capabilities. NATO should not shy away from attributing ongoing operations to state adversaries, relying on national data as needed. The alliance and its members should be prepared to use direct channels of communication and other means to deliver immediate deterrence signaling in specific cases.

On the Southern flank, NATO faces state actors that use unconventional tactics and proxy forces (for example, Iran and Syria); state collapse and the emergence of ungoverned spaces in Libya, Yemen, and parts of the Sahel; and the activities of a range of nonstate actors, from loose groups to terrorist and criminal networks to highly organized quasi-state structures like Hezbollah. Cooperation with regional partners in addressing these threats will be vital. NATO’s primary task, as elsewhere, should be to deter states in the region from using unconventional tactics against NATO and its allies, using signaling and attribution tools. When possible, the alliance should aim to affect the calculus of nonstate actors to prevent them from harming alliance interests. This may not work with jihadist groups but may be possible with actors motivated by political or economic interests.

### Redlines Bad---Russian SOI Impact

#### Russian cyber probes produce a European SOI

David Takacs 17, Associate Fellow at Slovak Security Policy Institute. "Ukraine‘s deterrence failure: Lessons for the Baltic States." DOI 10.1515/jobs-2017-0001

Russia and its revisionist behaviour present the Baltic States with a multitude of threats, making deterrence a top priority in the Baltic Region. Not only does Moscow wish to extend its sphere of influence to include what it describes as ‘near abroad’, it must carefully protect its own model of ‘sovereign democracy’ at home. Prior to Russian involvement, Ukraine was getting close to signing an association agreement with the European Union (EU) and it was feared that ‘democratic change in brotherly Ukraine could spread to Russia’. Transforming Ukraine to a western democracy was seen as a threat to the Russian regime and was thus stymied at its source (Snegovaya, 2014). However, the Baltic States have already been fully integrated into NATO and the (EU) and have been stable democracies for over two decades now. So what is the nature of the threat that Russia presents to the Baltic States?

Putin is using hybrid tactics as a means of achieving his objectives of a politically restructured Europe. These include massive pro-Russian propaganda and misinformation campaigns, using economic levers, intimidation, or the employment of cyber warfare elements. In Ukraine in 2014, Russia has once again demonstrated its resolve to use both military and non-military means to create and fuel conflicts in pursuit of its wider geopolitical interests. The Kremlin is busily trying to regain its sphere of influence over nations that were formerly part of the Soviet Union, and the Baltic States’ governments are continuously being reminded to stay alert. In addition, NATO frontier allies face much more significant threats due to their proximity to the potential aggressor (Grygiel and Mitchell, 2016, p. 166). Thus, what NATO needs most to deter Russia is ‘to demonstrate robust political solidarity’ within the alliance (NATO Parliamentary Assembly Report, 2015, pp. 4-6). There has been a significant increase in Russian probing activities to gauge NATO’s commitment to the Baltic States over the past two years. Grygiel and Mitchell (2016, p. 43) define Russian probing as a ‘lowmintensity and low-risk test aimed at gauging the opposing state´s power and will to maintain security and influence over a region’. In case of the Baltic States, probing is aimed at the US and the strongest European countries, their power and their will to back up their most exposed allies. As mentioned by Grygiel and Mitchell (2016, p. 122), ‘there is a strong correlation between the existence of alliances in a given region and the effectiveness of deterrence against a threatening power’. Building on the allies’ fear of abandonment and US fear of entrapment in local conflicts, Russia is aiming to hinder their relationships which could ultimately provide Moscow with more room for probing and manoeuvring in the Baltic Region.

Hybrid or conventional?

#### Global war

Dr. Hal Brands 18, Henry A. Kissinger Distinguished Professor of Global Affairs at the Johns Hopkins School of Advanced International Studies, Charles Edel, Senior Fellow and Visiting Scholar at the U.S. Studies Centre at the University of Sydney and is the author of Nation Builder: John Quincy Adams and the Grand Strategy of the Republic, The Disharmony of the Spheres, https://www.commentarymagazine.com/articles/hal-brands/the-disharmony-of-the-spheres/

To see this, just work backward from the present. During the Cold War, a bipolar balance did help avert actual war between Moscow and Washington. But even in Europe—where the spheres of influence were best defined—there were continual tensions and crises as Moscow tested the Western bloc. And outside Europe, violence and proxy wars were common as the superpowers competed to extend their reach into the Third World. In the 1930s, the emergence of German and Japanese spheres of influence led to the most catastrophic war in global history. The empires of the 19th century—spheres of influence in their own right—continually jostled one another, leading to wars and near-wars over the course of decades; the Peace of Amiens between England and Napoleonic France lasted a mere 14 months. And looking back to the ancient world, there were not one, but three Punic Wars fought between Rome and Carthage as two expanding empires came into conflict. A world defined by spheres of influence is often a world characterized by tensions, wars, and competition.

The reasons for this are simple. As the political scientist William Wohlforth observed, unipolar systems—such as the U.S.-dominated post–Cold War order—are anchored by a hegemonic power that can act decisively to maintain the peace. In a unipolar system, Wohlforth writes, there are few incentives for revisionist powers to incur the “focused enmity” of the leading state. Truly multipolar systems, by contrast, have often been volatile. When the major powers are more evenly matched, there is a greater temptation to aggression by those who seek to change the existing order of things. And seek to change things they undoubtedly will.

The idea that spheres of influence are stabilizing holds only if one assumes that the major powers are motivated only by insecurity and that concessions to the revisionists will therefore lead to peace. Churchill described this as the idea that if one “feeds the crocodile enough, the crocodile will eat him last.”

Unfortunately, today’s rising or resurgent powers are also motivated—as is America—by honor, ambition, and the timeless desire to make their international habitats reflect their own interests and ideals. It is a risky gamble indeed, then, to think that ceding Russia or China an uncontested sphere of influence would turn a revisionist authoritarian regime into a satisfied power. The result, as Robert Kagan has noted, might be to embolden those actors all the more, by giving them freer rein to bring their near-abroads under control, greater latitude and resources to pursue their ambitions, and enhanced confidence that the U.S.-led order is fracturing at its foundations. For China, dominance over the first island chain might simply intensify desires to achieve primacy in the second island chain and beyond; for Russia, renewed mastery in the former Soviet space could lead to desires to bring parts of the former Warsaw Pact to heel, as well. To observe how China is developing ever longer-range anti-access/area denial capabilities, or how Russia has been projecting military power ever farther afield, is to see this process in action.

The reemergence of a spheres-of-influence world would thus undercut one of the great historical achievements of U.S. foreign policy: the creation of a system in which America is the dominant power in each major geopolitical region and can act decisively to shape events and protect its interests. It would foster an environment in which democratic values are less prominent, authoritarian models are ascendant, and mercantilism advances as economic openness recedes. And rather than leading to multipolar stability, this change could simply encourage greater revisionism on the part of powers whose appetite grows with the eating. This would lead the world away from the relative stability of the post–Cold War era and back into the darker environment it seemed to have relegated to history a quarter-century ago. The phrase “spheres of influence” may sound vaguely theoretical and benign, but its real-world effects are likely to be tangible and pernicious.

Fortunately, the return of a spheres-of-influence world is not yet inevitable. Even as some nations will accept incorporation into a Chinese or Russian sphere of influence as the price of avoiding conflict, or maintaining access to critical markets and resources, others will resist because they see their own well-being as dependent on the preservation of the world order that Washington has long worked to create. The Philippines and Cambodia seem increasingly to fall into the former group; Poland and Japan, among many others, make up the latter. The willingness of even this latter group to take actions that risk incurring Beijing and Moscow’s wrath, however, will be constantly calibrated against an assessment of America’s own ability to continue leading the resistance to a spheres-of-influence world. Averting that outcome is becoming steadily harder, as the relative power and ambition of America’s authoritarian rivals rise and U.S. leadership seems to falter.

### Redlines Bad---AT: Deterrence Fails

#### Deterrence works and stops attacks before they happen

Maud Quessard 20 Université de Paris I – Panthéon – Sorbonne, Paris, “Cyber dissuasion et guerres de l’information : l’administration Trump à l’offensive” Chaire Grands Enjeux Stratégiques Contemporains 2020, accessed via : <https://natolibguides.info/cybersecurity/articles>, Translated by Joseph Estrada.

\*\* IRA == l’Internet Research Agency de Saint Petersburg

Questioned in march 2018 during his confirmation hearing at the senate about the reprisals that adversaries of the United States can fear after attacks, cyber or informational, general Nakasone clearly put forward that adversaries do not fear eventual reprisal (the deterrent effort would be insufficient or ineffective). To overcome this, he officially applies a concept inherited from the American special forces “forward defense,” put in the open in the war on terror, and that consists in carrying out preventative actions in being permanently present in foreign computer systems. It should be clear that one must be prepared for offense to make defense of national territory effective.

Today, the Cyber Command endowed with new prerogatives by the Executive (in National Memorandum 13, still confidential) and by Congress would carry out preventative cyber operations targeted on strategic foreign sites (Russian, in priority). These would not be the subject to the prior approval of the white house, which allows an augmented speed of response. The objective of these (disconnecting the IRA, carrying out an intrusion into the Russian GRU), made responsible for DNCleaks, carry out threatening targeted messaging campaigns against officials or foreign military) would be to dissuade all states considered threatening to democracy and American national security. For some people observers, it would be a question of practicing a "cyber cold war" by using everything the available cyber and informational "deterrence" arsenal.

And this, all the more so as with the proliferation of hybrid conflicts in Europe such as in Asia, many middle powers allied with the United States are under attack cyber, Russian or Chinese, which target their defense infrastructures. These attacks often support other forms of threats, operating in the "gray zone". This is the case since 2012, for the Philippines, Malaysia, Vietnam or Taiwan, which with conflicts over maritime borders facing China, suffer provocations Chinese in their territorial waters, doubled by cyber attacks on their civil and military infrastructures facing which they found themselves destitute. These vulnerabilities led them to seek help from the American partner to be able to train their own cyber units10 . For the United States, the affirmation of an offensive cyber posture may be seen by its allies as an attempt to maintain a comparative advantage in the cyber space as its status as hegemon is put in question.

Thus, the American intrusion carried out against Russian electricity infrastructures in June 2019 was publicly presented as a way to prevent a blackout (massive power cuts) in some pivotal American states, during the campaign presidential election of 2020.11 For those responsible for US cyber offensive operations, the challenge now is to digitally infiltrate hostile systems even before they can attack national territory. The objective is also to make believe in a balance of power, to increase deterrence as in the days of the nuclear age. For as much, the idea is to avoid for all actors any damage reaching targets civilians (such as hospitals) to avoid escalation.

## Innovation DA

### FYI---What is Smart Defense?

Marios Efthymiopoulos 19, PhD from the University of Crete in Security and Strategic Affairs on NATO issues and NATO-Russia relations, Chairman of the Board of Advisors of Strategy International, 6/24/19, "A cyber-security framework for development, defense and innovation at NATO", Journal of Innovation and Entrepreneurship, Volume 8, Article 12, https://innovation-entrepreneurship.springeropen.com/articles/10.1186/s13731-019-0105-z

Throughout the attempt to achieve a truly cooperative defense, “Smart Defense” stands out on renewing operational and tactical effectiveness; an innovation and business-led orientation for political, tactical, and operational alliance and coordination. It is all about specialization of forces including the element of resilience of forces mainly through technological agility.

Smart defense is prioritized as a method of innovative approach. Reflective toward efficiency and efficacy. Needs to meet NATO forces command and structure as attributed for force resilience of 2020, through the following steps: (1) sound strategic structuring and planning; (2) good operational coordination in exercises and in the field; (3) specialization of force structure, command, and operations; (4) achieving collective defense, through collective efforts; (5) burden sharing; and (6) technological advancements, considering the threats and challenges of the twenty-first century.

2018 was a year of much needed strategic and tactical resilience; smart defense stands out as a request for geo-political capability and capacity building, so as to implement operational preparedness and effectiveness, reflective in operations both on a regional and global scale of operations.

In 2019, the security environment seems politically and militarily hybrid, symmetrical but also asymmetrical, where the cost of human capital is limited, through the optimum use of technology provided. Duplication of operational efforts is limited yet the challenges are still reflective to the volatility of the security environment and threats that we live at.

Member states hold constant joint operational strategic centers of training and operations; on and about among others, ballistic missile defense, intelligence, surveillance, reconnaissance, cyber-defense and security, maintenance of readiness, training and force preparation but also agile deployment bases for effective engagement and now in cyber-security. All aforementioned should be expected to continue work with minimum cost, namely human casualties yet delivering high level of technology operational efficiency and constant preparedness that is both beneficial and practical and of tactical need to succeed against hybrid threats.

### OFF

#### NATO’s “Smart Defense” policy for cybersecurity creates policy resilience to hybrid threats---solves the case while preserving e-innovation

Marios Efthymiopoulos 19, PhD from the University of Crete in Security and Strategic Affairs on NATO issues and NATO-Russia relations, Chairman of the Board of Advisors of Strategy International, 6/24/19, "A cyber-security framework for development, defense and innovation at NATO", Journal of Innovation and Entrepreneurship, Volume 8, Article 12, https://innovation-entrepreneurship.springeropen.com/articles/10.1186/s13731-019-0105-z

Resilience as methodology: NATO’s strategic aim

Resilience is a method. A dedication to the goal. It is therefore an aim. Terminologically is announced in security-led strategies yet also business-led strategies. It holds a completely sound operational aim. To deliver and stick to the requested. It is brand name that defines strategy through which it results to operational capacity that sustains and grows; at the level of NATO, with the capacity to apply in diverse fields of operations adding value, to an already robust policy decision and operational capacity building and actions; at the level of cyber-security policy resilience to the framework is a “strong-hold” policy to deliver a protection mechanism and method.

Resilience’s framework acknowledges the will for preparedness so as to counter a possible integrative part of possible emerging crises. It is seen as an innovative strategic management policy procedure and tool. Strategically, it applies to operational capacity building, both civil and military. It is an element of acknowledged standardization of procedures. In the defense sector, when forces are deployed, they need flexible and effective means of countering threats; while in the field of cyber-security, they need agility in operational network centric operations, and constant accurate flow of information.

Strategic resilience in cyber-security requires flexible adaptability to new challenges. Its strategic resilience works as a tool for closeness, mitigation, and/or negotiation; it allows for cooperation among allies or members.

NATO’s vigilance and resilience in security-led affairs including cyber-security defines strategic plans and re-assesses risks that will allow us to think entrepreneurial and innovative. For NATO members, Heads of State, and Governments, cyber-security creates a modern administrative and operational format and framework of the alliance at a virtual level that is flexible and e-oriented, reflective to the market needs for security and stability, while augmenting market e-innovation and while adapting to new affordable methods of economic and socio-economic growth. NATO acquires protection mechanisms while its operations and memberships enlarge while operational challenges are upgraded and updated. NATO needs to provide militarily and technologically agile and interoperable forces with added value, through civilian capabilities (NATO’s Cyber-Defense Policy, 2011).

Resilience in security-led affairs through innovation and entrepreneurship therefore should be a leveled adaptation process for NATO; a phase to consequently strategize and draw new scenarios for cyber-security among others. This comes through operational result processes of training and experiences, when countered in an effective manner with lessons to be learned constantly in adaptable new circumstances against any forms of cyber-attacks.

Resilience becomes thus a policy orientation for NATO’s “Smart Defense” clause. NATO boosts on military innovation and methods of operational support and deliverables and protection mechanisms, while remaining relevant as a political military organization, a regional and global asset value to security and strategy application at a time of vast changes and challenges.

#### The plan undermines our tech edge

Camille Grand 20, NATO’s Assistant Secretary General for Defence Investment, Matthew Gillis, Defence Investment Staff Officer at NATO HQ, "Alliance capabilities at 70: achieving agility for an uncertain future", NDC Policy Brief No. 01, Jan 2020, <http://www.ndc.nato.int/news/news.php?icode=1408>

Secondly, the pace of change has accelerated at a tempo that risks outpacing our ability to exploit and, as necessary, counter the technological advancements on the horizon. Many of these technologies are driving towards faster and more distributed decision-making, which in turn bumps up against the sometimes bureaucratic and conservative nature of NATO’s machinery and decision making. Posturing the Alliance to fully embrace these technologies will require an adapted mindset and culture of delegating authority and accepting ambiguity.

One case for improvement is in the area of NATO processes, particularly those that manage procurements, standardization, and capability life cycles. We often strive for perfection in our future requirements, and engineer our processes around numerous decision gates and complicated management structures. The result is a capability that can be over budget, late, and obsolete when delivered. NATO has taken some healthy steps in this direction with the adoption of a new model for governing common funded capabilities with fewer decisions and streamlined oversight. But continued efforts are needed.

Industry also has a substantial role to play in this area. Our traditional defence industrial base should not be complacent with a business model that can be slow, cumbersome, and risk averse. In what Klaus Schwab has defined as the “fourth Industrial Revolution”, the changes on the horizon “herald the transformation of entire systems of production, management, and governance”1 while entirely upending existing industrial value chains. The success of Allies’ industries will depend on more acceptance of risk, greater investment in research and development, and an adapted mindset towards partnering with players outside the traditional defence sphere.

#### The impact is great power war

Jim Talent et al 19, Senior Fellow, Bipartisan Policy Center, Former U.S. Senator (R-MO), Robert O. Work, Distinguished Senior Fellow, Center for a New American Security, Former Deputy Secretary of Defense, 12/3/19, "The Contest for Innovation: Strengthening America’s National Security Innovation Base in an Era of Strategic Competition", Report of the Task Force on 21st-Century National Security Technology and Workforce, The Ronald Reagan Institute, https://www.reaganfoundation.org/media/355297/the\_contest\_for\_innovation\_report.pdf

The United States has entered an era of long-term competition with revisionist powers. A key aspect of this competition will revolve around a contest for technological superiority waged between the national innovation bases of the respective competitors. The outcome of this competition will determine not just American national security but also how the nations of the world interact—and whether a free and open political and economic system will remain the foundation of those interactions.

After a long post-Cold War focus on rogue regional powers and nearly two decades of continuous warfare in the Middle East and a focus on rogue regional powers, the United States now faces a new defining national security challenge: a long-term strategic competition with a resurgent Russia and a rising China.

Russia seeks to reestablish itself as a global power. While Russia is able to compete with the United States militarily in certain domains, its economic outlook and long-term demographic prospects are grim. Accordingly, it is unlikely to develop and nurture a true national innovation ecosystem. Given these disadvantages, Russia is limited to acting as a geostrategic spoiler seeking to undermine and weaken the United States, its alliances, and its global interests.

China, on the other hand, is already challenging the United States economically, militarily, and politically. China’s economy has surpassed that of the United States in terms of purchasing power parity and could, under some scenarios, pass the U.S. GDP in absolute terms in the mid- to late 2020s. Under the leadership of the Chinese Communist Party, China defines its vital national interests in ways that are irreconcilable with both the interests of the United States and the values of self-determination and individual freedom to which we and our allies are committed. China’s global expansion, from both a trade and military perspective, is challenging the United States in virtually every region of the world.

In pursuit of its goal of reshaping the world order, China aims to supplant the United States as the world’s leading technological power by 2030. China has articulated a distinct strategy of statedriven innovation, defined by its concept of “military–civil fusion,” to lead the world in cutting-edge technologies that might allow it to leapfrog the United States both economically and militarily.

That strategy presents a two-fold challenge for the United States. Economically, the challenge is to sustain American prosperity and access to markets on equal terms with other nations against China’s ambition to control the economic sectors that will determine national primacy in the decades ahead.

Militarily, the fundamental mission of the U.S. government (USG) is to deter a great-power war and, if deterrence fails, to prevent escalation of the conflict and end the war on terms favorable to the United States and its allies. An important key to this mission is achieving and maintaining military–technical superiority. However, over the last several decades, China—and, to a lesser extent, Russia—has invested heavily in advanced military capabilities specifically aimed at overcoming the technological lead of America’s armed forces.

As a result, the conventional overmatch that the United States has relied upon to undergird its deterrence posture since the end of the Cold War is eroding. The balance of power in East Asia has already shifted substantially in China’s direction. If this trend continues, effective deterrence in that region will likely fail, leaving the United States to face the unattractive alternatives of accepting aggression against its interests or its allies or triggering armed conflict with the People’s Liberation Army (PLA), with all the attendant risks of escalation.

### Overview---2NC

#### Tech dominance is key to winning great power wars—the foundation of military strength is economic strength---there’s a huge first adopter advantage for emerging tech that will determine who wins the wars of the future

#### The DA accesses a better internal link to tech innovation than the aff---NATO needs a tech innovation pipeline that can provide more defense at less cost with least delay---but that requires an agile bureaucracy willing to make big bets to incentivize the creation of entirely new markets of defense tech---an Alliance wide approach is better than a fragmented uncertain strategy

#### Framing issue---maximize innovation---the more the better---we don’t have to win the aff ends all innovation---just that they erode the pace, scope, and coordination of developments

#### Tech dominance is key to future wars---hypersonics, biotech, and AI

Charles Lutes 19, director of the Office of Defense Coordination at Lawrence Livermore National Laboratory, previously the director of the Center for the Study of Weapons of Mass Destruction at the National Defense University in Washington, D.C., currently pursuing a Ph.D. in Public Policy from The George Washington University, “U.S. Defense Strategy and the Innovation Imperative”, Getting Innovation Right, Center for Global Security Research, Lawrence Livermore National Laboratory, Sept 2019, https://www.osti.gov/servlets/purl/1635772

The point of departure for any contemporary analysis of the means and ends of innovation for national security should be the 2018 National Defense Strategy (NDS).1 The strategy describes a complex and dynamic security environment marked primarily by a renewal of rivalry among the major powers and with it new forms of strategic competition and new forms of strategic conflict. Among the dynamic elements it highlights is the technological dimension: strategic competition with Russia and China is characterized by a seemingly relentless drive to develop new technologies— advanced computing, big data analytics, artificial intelligence, autonomy, directed energy, hypersonics, and biotechnology. Multiple simultaneous technological revolutions are likely to significantly impact the character of war. The competitor that best harnesses these technologies will have the advantage in fighting and winning the wars of the future. The NDS exhorts the nation to foster a competitive mindset and emphasizes the need to “out-think, out-maneuver, out-partner, and out-innovate” our competitors and potential adversaries.

It is not surprising that the NDS focuses on innovation as a key to out-competing adversaries during a period of rapid technological change. At the same time, the NDS hints that technological innovation is a necessary, but not sufficient condition, for outinnovating the competition. As technology advances, the nation’s military must also seek to innovate its operational concepts and doctrine, as well as its organizations. Each is explored below.

#### Coordinating tech innovation solves all global challenges---saves humanity

Daniel **Araya 20**, PhD, Public Policy, University of Illinois at Urbana-Champaign, Senior Partner with the World Legal Summit and Senior Fellow with the Centre for International Governance Innovation, 9/1/20, "Is The Venus Project The Next Stage In Human Evolution?", Forbes, https://www.forbes.com/sites/danielaraya/2020/09/01/is-the-venus-project-the-next-stage-in-human-evolution/#1d09e43c5c35

A seismic shift is under way. Against the backdrop of rising temperatures, collapsing ecosystems, and the threat of species extinction, technologies like artificial intelligence (AI) and robotics are now moving to transform the global order. Indeed, for the first time in our history, we have the tools and technologies to guide and shape our evolution. But what will this future look like?

I recently spoke with Roxanne Meadows and Nathanael Dinwiddie of The Venus Project to better understand their thoughts on the future. As they explain, the status quo is no longer working. Climate change, social inequality, and technological innovation are now disrupting a market-driven society. The key to resolving these global challenges, they suggest, is rooted in a Resource Based Economy.

The term “Resource Based Economy” was first coined by Jacque Fresco, the founder of The Venus Project. Fresco believed that a Resource Based Economy could support the scientific integration of automating technologies (AI and robotics) and engineering systems in providing the highest possible living standards. Meadows and Dinwiddie suggest that this kind of economy is the next stage in human evolution. But what do they mean?

1. What is The Venus Project?

Meadows and Dinwiddie: The Venus Project is a non-profit organization that presents a new socio-economic model utilizing science and technology. For the past 40 years, we have maintained a 21-acre research center in Venus, Florida. We propose a new scientific foundation in transcending humanity’s current problems by testing a new social design for organizing our society as a global “operating system”.

Taken as a whole, the Venus Project fills the egregious gap between the sciences and the humanities by combining a social philosophy of the future with technical knowledge applied at a global scale to solve the problems of the human condition. Our methodologies are designed to realize the full potential of science and technology to achieve social betterment for all living systems— without exception. Our approach to social organization calls for changes in governance, economics, urban planning, education, human relationships, language, and values.

2. We appear to be in the early stages of a massive economic depression. What is your sense of what is happening politically and economically right now?

Meadows and Dinwiddie: We are witnessing an unprecedented political polarization and economic disruption around the world today. The status quo is no longer working. Many people are now beginning to understand how dysfunctional the management of nations, peoples, and resources has been. Human needs and the needs of our environment are far too complex to be managed by political means, arbitrary economic direction, or an elite without the relevant understanding of science and technology.

Compounding this problem, nature operates as a closed-loop system, but we do not. We extract resources without replenishing them, accumulate waste materials without recycling them, and we pollute our air, water, and food crops for the need to maintain competitive profit margins. There are many other factors converging at once besides the pandemic, all of which contribute to the system’s unrest.

3. Younger generations seem disaffected with Capitalism. Could you describe your vision of a post-scarcity society?

Meadows and Dinwiddie: The Venus Project recognizes that if we utilize a global systems approach as a basis for organizing and managing resources, we can design a much more humane environment for all. Our goal is to advance the health and the protection of the ecosystem, as opposed to the accumulation of wealth, property, and power. We do not have enough money to fulfill the needs of the world’s people, but we do have enough resources, if wisely managed. Ultimately, it is not money that people need, but unencumbered access to the necessities of life and self actualization.

Accomplishing this is a technical and engineering challenge requiring massive coordination by transdisciplinary teams of engineers and scientists in managing the Earth’s resources within its carrying capacity. This kind of scientific endeavor would eliminate the vicious rivalries over scarce resources and, in turn, generate very different behavior amongst people.

Briefly, this is what Jacque Fresco, founder of The Venus Project, termed a “Resource Based Economy”. This is a necessary step for humanity’s evolution. It could be thought of as a new science, a science of Earth Management where, by necessity, all of Earth’s resources become the common heritage of all the world’s people.

4. How does the Venus Project differ from Socialism or Communism?

Meadows and Dinwiddie: Rather than worker revolts and the forcible overthrow of the system (Communism), or the redistribution of capital (Socialism), The Venus Project approaches social change as a process of guided evolution. In our view, the challenges before us are a matter of engineering and design. The Venus Project calls for an experimental analysis of a new social system. This system is unlike any communist revolution, utopian commune, or coup d’état tried in the past.

In our view, the fundamental issue limiting social management in the past has been the lack of an effective data-driven methodology for evaluating and improving the system’s functioning. Full-scale blanket application of social policies to vast geographic areas— be it through revolution or legislation— without a means for evaluating their effectiveness, follows from an approach heavy in ideology but short in scientific method. The Venus Project calls for iterative prototyping of cities that we take as the unit of analysis in validating or falsifying hypotheses. All of this begins with testing a prototype, not a revolution.

Although Karl Marx did envision a society wherein money, private property, and social hierarchy were abolished, he could not begin to imagine how to implement this system at a technical level. In contrast to Communism, The Venus Project calls for the total redesign of cities (transportation, distribution, manufacturing, recycling, infrastructure) to produce abundance of goods and services. This is achieved through automation and optimized infrastructural efficiency.

5. What role does technology and automation play in The Venus Project?

Meadows and Dinwiddie: For the first time in history, we have the tools and technology to guide and shape our evolution. To accomplish this, The Venus Project advocates the humane and intelligent use of technology and the methods of science directed toward the well-being of all people and the environment which sustains all life.

In our view, technology and automation should be strictly used for social betterment and to eliminate repetitive, dangerous and monotonous work. If automation displaces a job, for example, that means all people would gain more access to the products those machines produce. The necessities of life are distributed without a fee with the aim of expanding to all goods and services. Consequently, there is no threat resulting from technological labor displacement. On the contrary, technology and automation have the potential for enhancing the world’s standard of living, enabling people to learn, spend time with their families, travel, and confront the new frontier of challenges in improving the resilience of the system as a whole.

6. How do you envision utilizing AI in decision-making?

Meadows and Dinwiddie: Applying the methods of science and technology (including AI) to the operation of the world’s societies will lead to a substantially more reliable functioning of support systems than we have today. Homelessness, starvation, war, and environmental degradation are consequences of today’s political and economic approaches to decision-making. A Resource Based Economy operates within a unified systems approach that utilizes the methods of science and AI to arrive at the most appropriate decisions at any given time. Unlike today’s implementation of technology, this new approach would be carefully carried out with the utmost human and environmental concern. The real-time influx of quantitative and qualitative data would provide real-time feedback, enabling humanity to constantly observe and continually improve the operation of the system over time.

7. What are the future goals of The Venus Project?

Meadows and Dinwiddie: At present, we are focused on formalizing and systematizing the body of work of The Venus Project’s founder, Jacque Fresco. In an age that is sorely lacking an approach updated to current knowledge and capability, we enter uncharted territory with the methods of science to help us through. This is the crucial job that no one has attempted, until now.

In the short term, we are focused on a systems approach to organize a holistic understanding of the natural world and human culture. This involves understanding economics and human social systems in the broader contexts of Earth processes and ecosystems, and communicating this understanding through books, videos, the internet, podcasts, transmedia storytelling, and course curricula.

In the mid-term, we aim to fulfill the desperate need for the strategic coordination of consilience by synthesizing the knowledge of academia and the know-how of industry. This network of intelligence will produce a transdisciplinary research agenda, research program, and global theory of change. Constructing a new planning center will function as a living lab and think tank devoted to designing the first prototype city.

In the long term, The Venus Project hopes to see the construction of new prototype cities for the purpose of testing the hypothesis of a holistic, technical design-solution for a social system. Iterations of these prototypes will form a worldwide network of cities. The study of these cities will function as the basis for a science of Earth management, the models of which guide the intelligent allocation of resources for the purpose of optimizing civilization to adapt and evolve in relationship with an Earth ecology.

There is a lot to consider and we welcome participation in the development of such a system.

### Overview---Turns Case---NATO/Russia

#### Innovation provides the adaptability NATO needs to meet future strategic challenges

Julian Lindley-French 20, Senior Fellow at the Institute for Statecraft in London, ““NATO@70”: still adapting after all these years”, NATO at 70: No Time to Retire, NDC Research Paper, NATO Defense College, No. 08, Jan 2020, http://www.ndc.nato.int/news/news.php?icode=1414

Future adaption: what are the most likely evolutions of the Alliance looking forward?

The complexity of NATO’s future adaptation challenge must not be under-estimated. The modernisation of Russia’s armed forces is part of a new form of complex strategic coercion that employs systematic pressure across 5Ds of disinformation, destabilisation, disruption, deception and implied destruction. Moscow’s enduring aim is to use the implicit threat of force to keep the Western allies permanently strategically, politically and militarily off-balance and the threat of overwhelming force as a form of strategic extortion racket focused on those at the margins of the Alliance. As a consequence, future adaptation and the Alliance concept of deterrence and defence will require an entirely new and innovative concept of protection and projection.

The nature of future war must also be seen within the context of the emerging complex strategic coercion that Russia is pioneering. Technology-led cross-domain warfare will see the battlespace become an integrated air, sea, land, space, cyber, information (including electronic warfare) and knowledge super-domain for the conduct of operations. Faced with such threats transatlantic political cohesion and Alliance military interoperability will be vital. The Alliance and its member states must be in the vanguard of the Revolution in Military Technology that is now underway. Artificial intelligence, quantum computing and machine-learning, nano-technologies, drone and other semi or fully autonomous delivery systems are now appearing in a battlespace that stretches from the depths of the oceans to outer-space, across all landmasses, and within and between changing societies and communities.

Adapting NATO to meet the strategic challenges of the twenty-first century must thus be the priority for “NATO@70”. If not, there is a very real danger the Alliance will lack the nimbleness to meet strategic change and technological developments, and ultimately fail as a consequence. There is also a danger that Alliance cohesion will progressively fade if such ambitions are not properly enunciated through a new Strategic Concept that enshrines at its heart a new form of flexible response. Above all, European words must be matched by European deeds through further organisational and internal reform to enable a properly agile and modernised Alliance that would give meaning to the 360-degree approach and enable the Allies to strike a balance between technology, capability and affordability

### Overview---Turns Case---Hybrid Threats

#### Smart defense solves hybrid threats

Marios Efthymiopoulos 19, PhD from the University of Crete in Security and Strategic Affairs on NATO issues and NATO-Russia relations, Chairman of the Board of Advisors of Strategy International, 6/24/19, "A cyber-security framework for development, defense and innovation at NATO", Journal of Innovation and Entrepreneurship, Volume 8, Article 12, https://innovation-entrepreneurship.springeropen.com/articles/10.1186/s13731-019-0105-z

NATO cyber-security policy should never stop transforming, while technology progresses and threats expand to a new and deeply digitized world of insecurity starting with the case with the cyber-attacks in Estonia in 2007 (Rehman, 2013). Past events in Estonia showed early on a strong smart cyber-defense “umbrella” which is certainly still needed by 2018, in which agility and resilience needs to be achieved.

There is a need of a resilient cyber-security strategic policy, a methodological and operational approach for a continuously standardized practical operational preparedness so as to constantly be able to counter cyber-attacks of hybrid or non-hybrid nature. Innovative methodology and ideologies are needed to process such a policy approach. There is a need for clear innovation and entrepreneurial understanding of what constitutes cooperation in cyber-security efficiency knowledge acquiring information and cooperation between public-private institutions and agencies.

A strategic cyber-security policy when applied will allow for the 30 member states to counter with more agile ways any emerging crises. This will efficiently manage processes and purposes for operations against any methods of electronic warfare. Interoperability of forces for joint use in cyber-defense is expected to be achieved through an adaptability and standardization process period. NATO should “e-volve” as should Alliance “e-networked” States. NATO should innovate and manage. NATO should administer change on methods of smart resilience in defense through cyber-security policy, strategically and operationally.

#### Agility and adaptability are key

Marios Efthymiopoulos 19, PhD from the University of Crete in Security and Strategic Affairs on NATO issues and NATO-Russia relations, Chairman of the Board of Advisors of Strategy International, 6/24/19, "A cyber-security framework for development, defense and innovation at NATO", Journal of Innovation and Entrepreneurship, Volume 8, Article 12, https://innovation-entrepreneurship.springeropen.com/articles/10.1186/s13731-019-0105-z

Operationally, national and cooperative forces need to be continuously agile and technologically advanced. In an asymmetrical world, which is complete with unforeseen challenges and threats, we need forces with flexibility, adaptability, operational and strategic command structure, based on high technologically sophisticated information “coming in,” but also being used while in training or through active operations.

On a theoretical scale, the current article requests a cyber-security strategic framework adoption of resilient adaptability and interoperability policy in the framework of safety and defense. The article considers that understanding the realities of threats is by definition a natural innovation and as we move ahead, we structure and operate a single strategy on cyber-security against a virtual threat from wherever it comes from. Its long-term resilience may be more complex as operational capacity needs to constantly develop and adapt into the convergence of societal structures, and methods; where socio-economic, technological, defense even health, and education issues are affected.

When theory on cyber-security, resilience, and operational capacity will be applied at NATOs level, it will enable allies and members, jointly, to create a true policy and strategy for cyber-security resilience against hybrid virtual threats. The methodology on how to is presented through this current article.

### UQ---Smart Defense---2NC Solves Case

#### The DA is a status quo gradualism counterplan with an external impact of tech dominance

#### Smart Defense solves the case now---it’s a defense posture to hybrid threats that uses bottom-up, business-led input to determine how we should respond---but broad Article 5 interpretation is key---it incentivizes tech innovation in order to stay prepared against all hybrid threats

#### Smart Defense solves clarifies NATO’s response to hybrid threats---avoids over and under reactions

Marios **Efthymiopoulos 19**, PhD from the University of Crete in Security and Strategic Affairs on NATO issues and NATO-Russia relations, Chairman of the Board of Advisors of Strategy International, 6/24/19, "A cyber-security framework for development, defense and innovation at NATO", Journal of Innovation and Entrepreneurship, Volume 8, Article 12, https://innovation-entrepreneurship.springeropen.com/articles/10.1186/s13731-019-0105-z

Associating smart defense with cyber-resilience: “engagement through policy adaptation”

As fiscal austerity measures are applied and cutbacks are in effect, according to the Chicago Council on Global Affairs, NATO allies have to decide on methods to approach NATOs political agenda decisions. Allies must enhance capacities and capabilities to implement new and innovative methods of tactical management for the benefit of security toward the Alliance space (Chicago Council on Global Affairs, 2012). According to the Atlantic Council, “…The Alliance, given its new strategic landscape, currently finds itself in, requires a new strategy. NATO’s current three core tasks—collective defense, crisis management, and cooperative security—are ‘tasks’ but not strategies—they do not identity the full spectrum of ends, ways, and means, and therefore do not tell the Alliance and its members either what to do or the risks involved. NATO has been working diligently but without great clarity or common agreement as to its end goals (NATO’s Cyber-Defense Policy, 2011)”.

Heads of States and Governments do listen and observe, but are not keen in stepping in the extra mile; to therefore consult and call on NATO to hold Summit meetings, to negotiate or mitigate current issues, and to elaborate and concentrate more on economic, political, military and management innovation and efficiency of administrative cooperation in all policy regulated fields of NATO.

A strategic framework policy on “Smart Defense,” which is yet to be achieved by 2020, may render a cheaper cost for the total sharing of burden by member states, while attracting more elements or variables where technology can be used to minimize costs. Surely, not all members share the same burden to this day by are reflective to all countries security defenses when it comes to cyberspace.

While a policy on smart defense lowers overall long-term cost, and if burden sharing is actually increased but equaled to lower levels of fiscal sharing, long-term results will show, that in fact, less cost will be achieved and cyber-innovative methods can help mitigate possible costs.

While cyber-security becomes a core, NATO policy for smart defense and resilience attracts attention to stake holders. Through evolving and constant communication and marketing perspectives, social media and workshops, and conferences, cyber-defense should continue to be promoted and have a clear aim. Reflecting on the needs for a global element of cyber-security against current and emerging challenges, exchange of scientific information and operational processes promote such ideology, where experts from around the world exchange information and discuss the risk assessments and how to manage.

Cyber-security then works as a “decree of specialization, which now requires adaptation if not done so already for each member state”, politically, strategically, tactically, and operationally but also legally. Cyber-security must and should always be provided as a methodological tool for operational success of NATO against current and emerging threats. It is and will always be a tool for a joint framework of cooperation, globally.

As smart defense is being upgraded and developed, cyber-defense “…not a conception but a real-politic issue… (Efthymiopoulos, 2008b)”, should remain an element of specialization policy, a key for concrete strategic engagement of all resilient member states. It will emerge to become a policy of innovative unity among states (political) yet also business continuity (strategic orientation) about the future of NATO (The entrepreneurial and managerial side of things).

NATO’s strategic approach post Warsaw and Brussels of 2017 and 2018 Summits is estimated to reflect a much need realistic plan of operations and engagement in the field of cyber-security and defense. NATO should continue to be collective to be a force projector and force protector. It should not limit its role and actions but should allow and seek out enlarged cooperations tailored to the global and regional needs to counter the existing challenges or emerging challenges, considering that as aforementioned challenges are now borderless.

Cyber-security and technological progress within NATO are synonymous. They can therefore be seen as the core of collaboration on smart defense, to be finalized and achieved by 2020 standards. Cyber-security being technologically advanced is resilient to changes and is innovative as a method as it was never been done before at NATO until the date that it was presented to. It does provide adaptable technological architecture and posture, which will be discussed below considering the opportunities but also challenges. It will provide robust deliverables with minimum human capital, fiscal but requests technical deliverables.

### UQ---Smart Defense---AT: UQ Overwhelms

**It's going to be finalized this year---but the aff undermines efficiencies by creating gaps in coverage**

Marios **Efthymiopoulos 19**, PhD from the University of Crete in Security and Strategic Affairs on NATO issues and NATO-Russia relations, Chairman of the Board of Advisors of Strategy International, 6/24/19, "A cyber-security framework for development, defense and innovation at NATO", Journal of Innovation and Entrepreneurship, Volume 8, Article 12, https://innovation-entrepreneurship.springeropen.com/articles/10.1186/s13731-019-0105-z

By 2008, seven Alliance countries according to the Memorandum of Understanding on the cyber-defense center, supported Estonia to get full operational capability (Germany, Italy, Latvia, Lithuania, Slovakia, and Spain), which lead to an evolution period. By 2016, NATO Allies are expected to discuss further and finalize the framework, logistics, and operations, elements of cyber-resilience and procedures on the policies, when considering threats and challenges in a changing environment. NATO is yet to decide on the resilience policy, as hybrid warfare is developing, at a time when smart defense of NATO nations are expected to achieve the goals and aims which are to be seen by the year 2020.

The cyber-attacks in Estonia of 2007 are still today the biggest and most organized electronic attack, with a duration period of several weeks, provided NATO with a motive and multipurpose task for years to come. NATO’s leadership was in fact correct in its judgment that (1) such an operational center and policy was needed, (2) its operational center would constantly be evaluating and evaluated, and would research on prospective evolutions in technology, malware, and cyber-security (3) that NATO requires resilience when considering the current or future threats and challenges.

The inauguration of its Cooperative Cyber-Defense Centre of Excellence (CCDCOE) in Tallinn Estonia in May 2008, led to a mission, which holds a clear vision and statement. It is yet to be “politically ratified” and adopted as a key core policy by Allies. Its raison d’être as stated is “to enhance the cooperative Cyber-Defence capability of NATO and NATO nations, thus improving the Alliance’s interoperability in the field of cooperative Cyber-Defence,” therefore reflecting on the key core elements to counter hybrid threats and be constantly resilience to strategic requests and needs. The vision is for the CCDCOE to become “a specialized and expertise center for NATO in cooperative cyber-defense” (CCDCOE, Training Catalogue, n.d.).

The domain of the cooperative cyber defense center in the framework of cooperative security within NATO focuses in the fields of research which include:

“Legal and policy elements”

Concepts and strategy

Tactical environment

Critical information infrastructure protection (NATO, 2016c)

The Centre’s core policy created an outcome of research and policy-orientation, as already analyzed. It was presented primarily as a first outcome, then accepted by the Supreme Commander Allied Command Transformation (SACT), deriving from a request of NATO HQ (Headquarters) and by the North Atlantic Council (NAC) level. This included Doctrine and Concept Development, Awareness and Training, Research and Development Analysis, and Lessons learned and finally Consultation.

In July 2018 during the Brussels NATO meeting, the Heads of States and Governments agreed to the opening of the cyberspace center as part of the new NATO command structure reform that provides more agility and assurances of operational preparedness, while ensuring force command operations and agility (Efthymiopoulos, 2013). The agreement includes a creation of policy and action reflecting key core issues including a framework policy for the cyberspace operations center of NATO to learn and coordinate in operations how to counter emerging challenges.

Results: NATO innovates with reflection to cyber-security

In terms of cyber-security, the Centre for Excellence in Tallinn continues to portray and project NATOs need for a methodological cyber-resilience policy. At NATO Brussels summit, cyber-security became operational. Therefore, NATOs cyber-defense policy and smart efficient methods while also requested for more interoperability agility and security resilience in the field of cyber-security becomes a core policy.

The attempt as an idea and method to reach out on cyber-security agility of forces for operations is not a new one. On February 6th and 7th 2009, NATO’s Science for Peace and Security (SPS) sponsored a workshop. It foresighted the possibility of cyber-security framework. Something we commend through this article: a framework strategy for operational and efficient cyber-security to become a core policy of resilience at NATO. The 2009 workshop titled “Operational Network Intelligence: Today and tomorrow” aimed at adaptation knowledge procedures considering the evolving and fast growing technology. It spoke about innovation and entrepreneurship. It talked about methodological approaches that may bring allies together, while bring cooperative sides together in investment through R&D opportunities.

Its overall purpose therefore was to introduce the possibility of innovation: “rethink present strategies and identify urgent measures to be taken in order to minimize the strategic and economic impacts of cyber-attacks” (NATO, 2009b). This was the level of anticipation at the time; considering future correlation of smart-defense with the policy of cyber-defense at its core. In 2019, innovation seems to be a sound but lone option; a process where through cooperative security and military and technological entrepreneurship NATO can move forward.

In 2019, considering the risk assessments on hybrid threats and challenges (Davis Jr., 2015), the need for better civil awareness and readiness, at a time of much needed cooperative defense, Allies have to decide for a robust long-term planning innovative and entrepreneurial strategy for current and future operations of NATO. Keeping in mind the need for strong success in field operations, including success in and at a multi-dimensional level of operations against all threats while making operations to be cost efficient with minimum human casualty numbers.

NATO increasingly recognizes that organized cyber-attacks seek to take advantage of “gaps” in the “system social and market matrix.” Therefore, it should be a request from member states to examine the increasing need for coordination of human factors related to the issues of electronic warfare, operational network, intelligence, and cyber-defense, whether for training, scientific exchange, and or operations (NATO Review, 2015).

NATO is currently using people involved in e-systems, security, IT engineers, researches, officers dealing with network operations and operational centres, as well as professional and academics, among others including military specialists. Specialists in the field on both a strategic and tactical levels should continue to be systematically involved at organized levels of research, sharing, discussion, and exhibition of outcomes, which will in turn enrich the abilities, capabilities, and capacities of rendering current smart-defense and cyber-security as a key and successful resilient and collaborative defense policy to NATO.

### UQ---Smart Defense---AT: No Smart Defense Now

#### Smart Defense is coming now---their evidence is outdated and doesn’t assume allied perception

Marios Efthymiopoulos 19, PhD from the University of Crete in Security and Strategic Affairs on NATO issues and NATO-Russia relations, Chairman of the Board of Advisors of Strategy International, 6/24/19, "A cyber-security framework for development, defense and innovation at NATO", Journal of Innovation and Entrepreneurship, Volume 8, Article 12, https://innovation-entrepreneurship.springeropen.com/articles/10.1186/s13731-019-0105-z

As previously noted, cyber-security capabilities in a smart and resilient way is the “operational goal.” NATO members prepare well and also at joint levels. NATO’s Smart Defense,Footnote1 a policy framework for defensive tactical advice and operations, used to be the method that among others branded the need for a cyber-security policy. A cyber-resilience of NATO, which was adopted during the Warsaw Summit in July 2016 and reflective to the July NATO summit in 2018, expects allies to take continued actions through standardized procedures of protection effectiveness and also innovative openness and entrepreneurial attraction through NATOs respective institutions, centers of excellence, agencies, and its new cyberspace operations center that is to be inaugurated in Mons Belgium.

What is well known through policy analysis is that NATO military forces should reach to appropriate operational and tactical levels, so as to operate in and around “article and non-article 5 operations” (Sendmeyer, 2010)—meaning not only defensive-clause operations but also in counter-offensive operations (NATO, 2008b). Cyber-protection and cyber-security methods are needed, when defense of allies is associated with possible threats or challenges such as the one of ISIS.

#### Their evidence is snapshot, Smart Defense will soon be evident

Marios Efthymiopoulos 19, PhD from the University of Crete in Security and Strategic Affairs on NATO issues and NATO-Russia relations, Chairman of the Board of Advisors of Strategy International, 6/24/19, "A cyber-security framework for development, defense and innovation at NATO", Journal of Innovation and Entrepreneurship, Volume 8, Article 12, https://innovation-entrepreneurship.springeropen.com/articles/10.1186/s13731-019-0105-z

In specific, a cyber-security strategy for NATO will enhance its innovation and creativity core of operations and methodologies against any kind of virtual threats. It will set standards, policy procedures, and recommendations. NATO’s strategy of cyber-security through its new Cyberspace Operations Centre, in Mons (Belgium) as decided in the Brussels Summit of July 2018 (Cyber-Space Operations Center Mons Belgium, 2018) unfolds options and opportunities, innovation, and entrepreneurship in operations efficiency and capabilities application. Current technological advancements and dynamisms through innovation and sustainable futuristic advancement will soon be evident.

### UQ---Tech Innovation

#### NATO’s proving its capable of innovative tech development now

Camille Grand 20, NATO’s Assistant Secretary General for Defence Investmen, Matthew Gillis, Defence Investment Staff Officer at NATO HQ, "Alliance capabilities at 70: achieving agility for an uncertain future", NDC Policy Brief No. 01, Jan 2020, <http://www.ndc.nato.int/news/news.php?icode=1408>

Blueprints for the future?

The future outlook for disruptive technology is not entirely negative. Two new initiatives show exceptional promise to invert traditional capability development models, while seizing upon the opportunities offered by new technology. They demonstrate vividly how NATO adapts.

The first is the Maritime Unmanned Systems Initiative. Here, 14 Allies have committed to a cooperative framework for developing and integrating unmanned systems into NATO’s defence architecture.2 The project is aimed at bringing autonomy and unmanned capability to bear in support of tedious and dangerous jobs at sea, including anti-submarine and counter-mine warfare. Beyond leveraging new technology, the project is also leveraging a “start up” mindset for agility and lean approaches. The project has benefi ted from experience drawn from industry, academia, and government, including Coca Cola and the Pentagon’s Defense Innovation Unit. This model has already paid dividends: less than a year after the fi rst commitment was taken, the largest-ever exercise of NATO unmanned underwater, surface and air vehicles took place off Portugal.3

The second initiative is the Alliance Future Surveillance and Control capability. In a novel example of obsolescence management, NATO leaders have committed to cooperate towards defi ning a replacement for NATO’s AWACS fl eet in anticipation of its retirement around 2035. The project launched in 2016 with a fundamental re-evaluation of NATO’s future needs, eschewing any assumptions that AWACS would simply undergo a “likefor-like” replacement. The project has since arrived at capability requirements that drive for an integration of surveillance and C2 across multiple domains. Allied industries have now been challenged to offer ideas on how NATO’s requirements could be fulfi lled by 2035. Up to six concepts are being sought in order to encourage a wide variety of innovative solutions, including those that leverage emerging and disruptive technologies.

Both of these projects are in their early steps. Nevertheless, their models are contesting the traditional approaches to defence acquisition by embracing disruptive technology, tapping into industry expertise, and leaving space for future capability growth. These projects offer promise for the future adaptability and agility of NATO capability development, and as such deserve close attention and support.

### Link Wall---2NC

#### Commitment---fully embracing emerging tech requires a defense posture that accounts for the uncertainty of future developments---broad acceptance of risk increases the demand for new tech innovations

Marios Efthymiopoulos 19, PhD from the University of Crete in Security and Strategic Affairs on NATO issues and NATO-Russia relations, Chairman of the Board of Advisors of Strategy International, 6/24/19, "A cyber-security framework for development, defense and innovation at NATO", Journal of Innovation and Entrepreneurship, Volume 8, Article 12, https://innovation-entrepreneurship.springeropen.com/articles/10.1186/s13731-019-0105-z

In twenty-first century security affairs, NATO forces are required to be well prepared for possible rules of engagement at all levels and dimensions. They should be able to counter symmetrical and asymmetrical battles, threats or challenges, hybrid or non-hybrid. At the level of cyber-security and cyber-resilience and preparedness, scenarios, of possible attacks and battles, can be anticipated. Along the lines of the new cyber-space operations center, NATO should prepare operational methods for action, whether this is for defense or cooperation for cyber-space.

The use and necessity today of technology is limitless. So is the virtual world of defense and security, where technology and cyber-defense merge. These are the tools for action. Technology plays a key role in a global reach. Yet so does NATO, through the framework of a limitless technology applied in military operations. NATO uses technology to train, prepare, ready, deploy, and operate its forces. Technology for NATO works as tools with which the Alliance protects and defend, yet also is capable to counter-assault, with counter-measures where and when is needed, required, or decided.

Since the adoption of the NATO Cyber-Defense policy (NATO’s Cyber-Defense Policy, 2011), NATO trains its military and civilian assets for possible action against possible threats. NATO is constantly training its forces in cyber defense training can be achieved through national, bilateral even multilateral levels of NATO, through the association of member states, at the level of Centres of Excellence, such as the NATO Cyber-Defense Centre for Excellence (CCDCOE) (NATO, n.d.) and now through the Cyberspace Operations center in Mons Belgium. Training and exercises are now anticipated to expand and enlarge. So are multinational operations held through remote areas and locations. NATO is now to get more engaged in the field of cyber-defense, in both operations and tactics. It is anticipated within the Alliance that NATO is well prepared, both for current and future challenges, countering multiple and multileveled dimensions of cyber-attacks. Yet, it also holds an open option, if necessary, to conduct counter-offensives to prevent further escalation of cyber or military actions (Hughes, 2009).

NATO Missions, “will continue to require agile and interoperable, well-trained and well-led military forces” (Carayannis, Campbell & Efthymiopoulos, 2014). This new technological and operational environment through cyber-defense provides NATO with a new level of technological possibilities, new tools for use against possible threats but also protective “cyber-objectives.” Allies have an added policy, mission, and value. Ongoing and constant transformation through its operational and capacity building resilience, aims to reach in updated capabilities and political excellence, in 2016. NATO aims for well-coordinated missions in cooperation with and/or participation with other international organizations, when prompted to react on international threats or challenges. As such, NATO has the ability to continue to be a force and security provided in future potential of, what we may call it, the “online” security protection initiative against all possibly known threats.

NATO seeks excellence, in achieving the best smartest way to protect but also counter-attack. By “nature,” NATO exists to prevent and defend member states from attacks. Through smart ways and agile training, NATO can counter most known ways of interface (whether virus or virtual) attacks or even e-spying attempts.

#### Decision-making framework---centralizing decision gates through complicated management structures ensures capabilities will be over budget, late, and obsolete when delivered---government limitations get in the way of ‘business-led’ innovations

Marios Efthymiopoulos 19, PhD from the University of Crete in Security and Strategic Affairs on NATO issues and NATO-Russia relations, Chairman of the Board of Advisors of Strategy International, 6/24/19, "A cyber-security framework for development, defense and innovation at NATO", Journal of Innovation and Entrepreneurship, Volume 8, Article 12, https://innovation-entrepreneurship.springeropen.com/articles/10.1186/s13731-019-0105-z

During the year 2018, there was a new security cultural security comprehension; it is considered as multi-leveled and multi-dimensional. In 2018’s NATO summit of July, allies evaluated current developments in cyber-security considering challenges, threats, but also opportunities. Evaluated current strategic and geopolitical challenges. They upheld methodological preparedness for network defense and operations and declared under the new NATO command structural reform the setting up of a cyberspace operations center, as part of the adapted command structure. Allies now request for more awareness and openness, innovation methods, and capacity building in cyber-security, considering changes in the market economy, more tangible and operational capacity building through R&D companies. Any decision, considering the changing nature of security and strategic market, should be “business-led” innovative-led, promoting sustainability and growth, market methods to uphold NATO’s relevance, while keeping the public informed. The public is keen on understanding the operational usefulness of the alliance, at a time of inside and outside NATO members’ landscape threats and challenges.

Defense capacity building for the twentieth century requires a modern way of thinking. It is about encouraging cooperative defense at the level of expected outcomes considering global but also regional risk assessments. NATO is still to enhance but also maintaining military capacities and military capabilities.

The new strategic concept of NATO requests the alliance to move forward. Twenty-first century needs and challenges require agility and compatibility of forces and force command at all levels, including network-centric operations and defense.

NATO forces, force command, technology, and methodological approach in military elements and standards cannot be or remain static. They need to technologically advance, progress methodologically innovate, to accommodate for the increasing need for multi-dimensional ways of security and defense. NATO needs to have interoperable, capable, and well-equipped technologically agile forces considering innovation and entrepreneurial thinking in a period of technological advance.

#### Line drawing---static methodologies prevent constant tech upgrades needed to stay prepared for future threats that are impossible to anticipate

Marios Efthymiopoulos 19, PhD from the University of Crete in Security and Strategic Affairs on NATO issues and NATO-Russia relations, Chairman of the Board of Advisors of Strategy International, 6/24/19, "A cyber-security framework for development, defense and innovation at NATO", Journal of Innovation and Entrepreneurship, Volume 8, Article 12, https://innovation-entrepreneurship.springeropen.com/articles/10.1186/s13731-019-0105-z

In an emerging globalized world, where complexity may become a key characteristic in strategy and security, resilience will become an integrated part of NATOs policy orientation and application. New vulnerabilities and threats continue to emerge. Political pressure will require NATO leaders to take decisions about the organization’s future. Yet all agree that NATO is a necessity. As such, NATO should become more open, more adaptable, and more flexible. With more burden sharing, better smart budgeting, long-term planning, and operational application and continued success, NATO should continue be re-branded as an adaptive security organization that does more to offer security and strategic alignment to truly current but also future challenges and threats, that we may not yet anticipate or think of.

In the not so long past, such similar actions reaffirmed by the Heads of States, included among others, the Treaty of London in 1990 Summit, to the 1994 Summit in Brussels, and in 1999 over its 50th year anniversary Summit in Washington, to the immediate decisions taken in 2001 after the terrorist acts in the USA (NATO, 2001b) to its 60th anniversary, which was held in Strasbourg and Kiehl accordingly in April 2009 to the Chicago Summit of 2012 and the Wales Summit of 2014, which added value to the Alliance and Allies reaffirming NATOs long-term necessity but now also strategic resilience to multi-dimensional challenges and threats.

Vulnerabilities and threats considering multidimensional challenges such as cyber-security require NATO to be truly, strategically and operationally agile. It requires NATO to be adaptable to conditions unforeseen.

Considering technological advancements, we are yet to acquaint ourselves, our institutions, governments, and international organizations with true phenomena of a new, yet networked global society. In this borderless society, where electric grids, information, or installations failures may have in the past solely affect a country, now affect a region and possibly a larger area. Our abilities are limitless to point out challenges and face them. We also have the ability to innovate through methodological approaches and security cooperation utilizing the constant upgrade of technology. However, when decisions come to being, this may not be easy.

### Link Wall---General

#### Collective defense is the foundation of Smart Defense---limiting our commitment hurts resiliency, duplicates efforts, and prevents interoperability

Marios Efthymiopoulos 19, PhD from the University of Crete in Security and Strategic Affairs on NATO issues and NATO-Russia relations, Chairman of the Board of Advisors of Strategy International, 6/24/19, "A cyber-security framework for development, defense and innovation at NATO", Journal of Innovation and Entrepreneurship, Volume 8, Article 12, https://innovation-entrepreneurship.springeropen.com/articles/10.1186/s13731-019-0105-z

NATO’s concept of cyber-defense in 2019

It was NATO’s Military Committee decision to adopt a “Cyber-Defense Concept” (Efthymiopoulos, 2008e). The Committee’s aim was and still is to deliver business continuity and military resilience. As NATO is a provider of collective defense and as a collective organization in a globalized and currently unsafe e-world, it needs to be agile. In an environment of insecurity, the Alliance’ delivers new policy results. Taking into perspective new forms of asymmetrical threats, such as cyber-attacks.

Historically, the 2002 Prague Summit first marked NATO’s tasking authority committee with regards to all activities that should be held in relations to cyber-defense. As technical achievements were delivered, so policy-makers delivered policy results on cyber-defense. That is why, Allied leaders during the Riga Summit of 2006 acknowledged the need to include these as is stated on its decisions at the Press Communiqué: (1) to protect NATO’s operational information systems, and (2) to protect its allied countries from any e-, or in other words cyber-attacks by new forms and means developed by NATO’s Allied Command Transformation (ACT) In Norfolk Virginia.

The output of the informal Meeting of the Ministers of Defense in October 2007 of NATO (NATO Defence Ministers Meeting, 2007) gave way to the inauguration of NATO’s Center for Excellence (COE), which at a later stage got accredited to have become the Allied Command Transformation on cyber-defense, named as Cooperative Cyber-Defense Centre of Excellence, CCDCOE (NATO, 2008a). It was based on the concept and early understanding of cyber-resilience for NATO’s future policies in countering challenges and threats, as was agreed by NATO’s Military Committee.

The central and final decision-making role over the policy of cyber-defense however is the North Atlantic Council (NAC), which accordingly is led by Heads of State and Governments. This is the highest deciding political authority which decides, creates, and overviews policy. It also evaluates, considers, and adopts NATO’s policies and activities with regards to political and military affairs or standing issues on challenges and threats, among others. Below the NAC, is NATO’s Consultation Control and Command Agency (NC3A) (NATO NC3A, 2002) now transformed to the NCIA agency (NATO, 2008a) and the NATO Military Authorities (NMA). The latter authority has implementation as its major task (NATO’s Cyber-Defence policy, 2008).

The implementation of NATO’s cyber-defense policy is considered as the second most important decision by now, once the decisions are taken by the NAC. The “Concept of Cyber-Defence” “adds practical action programmes, to fit within the overarching policy” (NATO, 2009a). The “Cyber-Defence Management Authority” that is tasked upon its policy concept “brings together the key actors in NATO’s Cyber-Defence activities.” Its aim is to manage and support all NATO communication and information networked systems and individually allies upon request (NATO, 2008c).

NATO’s policy creation and activity is “encouraged” by Allies. The aim is to adapt the alliance to the new strategic and security environment that is “hybrid” and thus the creation of the cyberspace operations center in Mons in Belgium. To engage as many as possible governments, industry-related market companies, and individuals. In accordance to its best practice policy, NATO considers that its “operational forum” can and should be considered as the best joint operational cooperation between states and market, as to also avoid duplication of efforts and use the necessary global knowledge to achieve interoperability of force action and command also in cyber-space.

Practically, in military policy, implementation, or operational areas, NATO has adopted “three phases of practical activity and cooperation”: the initial phase includes a NATO Computer Incident Response Capability (NCIRC). It was established as “interim operating capability” for NATO to build up on both security risk and manage the element of cyber-threats. Its second phase involved an ever more realistic and pragmatic perspective that required the coordination of all initial “offering” states to the attempt to establish a cyber-center (under the NATO agreement between states of a voluntary national contribution—VNC), in bringing the NCIRC to a full operational capability (NATO, 2008c).

New and innovative policies were adopted. They were proposed and came to effect (well-known procedure of internal NATO working process) until the adoption of “MoU”; a memorandum of understanding was drafted and proposed to NATO, by a sponsoring state which would establish a center for cyber-training, in this case in Estonia.

From that point on, it became an administrative decision of the Allies, that once the aforementioned stages would be put into effect, then a third phase would come into existence. Needless to say, this third phase was a complete implementation and rule-based operational procedure that would soon enough bring about into existence NATO’s request for technological agility and resilience, which is finalized at the Warsaw Summit of July 2016. It consists of incorporating—lessons learned—from the prior two phases as using new and latest cyber-defense measures (use of new technology and getting more knowledge on the security environment), in order to enhance cyber-defense posture. Once the third phase was evaluated, the Allied Command Transformation (ACT) decided, to accredit the operational center—in this case the Cooperative Cyber Defense (CCD) COE (Estonia), what is called as a “Centre of Excellence”. In turn, this resulted to the inauguration of the CCDCOE by May 2008.

#### Limiting Article 5 commitment to hybrid threats undermines cyberdefense integration

CDR Wiesław Goździewicz 16, Legal Advisor NATO Joint Force Training Centre, “From Riga to Wales. NATO’s Road to Collective Cyberdefence”, NATO Road to Cybersecurity, The Kosciuszko Institute, https://ik.org.pl/wp-content/uploads/nato\_road\_to\_cybersecurity\_the\_kosciuszko\_institute\_2016.pdf

The Wales Summit Declaration8 was a major step forward in acknowledging the challenges posed by complex cyberattacks. It was the first official document in which the Member Nations of the Alliance confirmed the possibility of a cyberattack to cross the threshold of an armed attack and thus become the basis for invoking Article 5 of the North Atlantic Treaty. It was reiterated that cyberthreats and attacks would continue to become more common, sophisticated, and potentially damaging. In Paragraph 72, the Alliance Nations declared that:

“Cyberattacks can reach a threshold that threatens national and EuroAtlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm therefore that cyber defence is part of NATO’s core task of collective defence. A decision as to when a cyberattack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis.”

This clearly demonstrates the Alliance’s view whereby cyberattacks can cross the threshold of an armed attack, allowing individual or collective self-defence to be invocated under both Article 51 of the UN Charterand Article 5 of the North Atlantic Treaty. Moreover, for the first time since NATO took on the topic of cyberdefence in 2006, it was explicitly stated that cyberdefence became part of the Alliance’s collective defence tasks and efforts.

The Member Nations adopted the Enhanced Cyber Defence Policy (ECDP) which reaffirms the principles of the indivisibility of Allied security and of prevention, detection, resilience, recovery, and defence and clearly states that “(…)the fundamental cyber defence responsibility of NATO is to defend its own networks, and that assistance to Allies should be addressed in accordance with the spirit of solidarity, emphasizing the responsibility of Allies to develop the relevant capabilities for the protection of national networks.” The ECDP recognises the applicability of international law to cyber operations, including the International Humanitarian Law (IHL) or the Law of Armed Conflict (LOAC).

The Nations committed themselves to further develop their national cyberdefence capabilities and enhance the cybersecurity of their networks, upon which the Alliance depends. NATO’s top priority for cyberdefence is the protection of NATO-owned communications and information systems (CIS); however, the Alliance will assist the Nations in defending their national networks considered critical for NATO’s missions. For this purpose, the Alliance cooperates with national authorities to ensure an appropriate level of cyberdefence of national CIS. Such cooperation is being formalised in Memoranda of Understanding (MOUs) signed between the Cyber Defence Management Board and the respective nations. Cyberdefence MOUs are based upon a template developed in the Cyber Defence Action Plan in line with the principles of the ECDP. They set the foundations for mutual support in the area of cyberdefence, including information sharing, participation in training and exercises as well as the provision of reciprocal assistance in the form of intelligence and “manpower” (CIS specialists and cyberdefence experts). The Czech Republic was the first NATO Nation to sign such a MOU on 12 October 2015.9 Assistance to Allies may be provided by one of the Rapid Reaction Teams formed by the NCIA as part of the Alliance’s collective cyberdefence capability.10

The Wales Summit Declaration further provided for a continued integration of cyberdefence into NATO operations and operational and contingency planning, as well as the enhancement of information sharing and situational awareness among Allies. The key role of partnerships in addressing cyberthreats was stressed.

Also the ECDP requires NATO to include cyberdefence aspects in the defence planning process. This has been achieved by implementing respective cyberdefence annexes in Operations Plans (OPLANs) developed for real-life operations, training and exercises as well as contingency plans. The training and exercise programme has grown to include cyber-specific exercises such as Cyber Coalition and Locked Shields. In addition, an extensive cyberdefence play has been incorporated into more “classic” training and exercises, including the biggest NATO exercise over the last decade – Trident Juncture 15 and Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise (CWIX), to which the Joint Force Training Centre has been the proud host for the last five years.11

One of the most important aspects of the NATO ECDP is cooperation in broad terms: with NATO Nations (as described above), Partner Nations, international actors such as the UN and the EU, industry and academia. Cooperation with industry has been formalised in the NATO Industry Cyber Partnership (NICP), which was founded and endorsed by the Alliance based upon the conclusion that NATO and industry faced shared risks in cyberspace, and that addressing these challenges required new frameworks for action. Within the NICP framework, the NCIA has launched the cybersecurity incubator concept tasked to develop a new model for NATO-industry cooperation with the aim to decrease the time required for NATO to develop its cyber response capabilities, based upon the results of research and development programmes already run by industry and academia.

There are many other cooperation frameworks such as the Cyber Information and Incident Coordination System (CIIS), a web-based application developed for sharing cyberdefence information within a trusted community and available to all NATO Nations and Partner Nations as well as commercial organizations.

NATO does not develop offensive cyber capabilities. Although the Alliance focuses on defence against cyberattacks, it does not preclude particular Member Nations from developing their own national offensive cyber capabilities. In fact, there are nations who openly admit they pursue such capabilities involving “(…)countering (disorganising, jamming and destroying) the sources of threats (active defence and offensive actions) (…)”.12 As a matter of fact, NATO Rules of Engagement13 in Series 36 (Information Operations) envisage the possibility of conducting offensive computer network operations (namely Computer Network Attacks – CNAs); however, none of these offensive ROEs have been authorised so far by the North Atlantic Council in operations or exercises.

This short text hopefully illustrates how NATO’s approach to cyberdefence has evolved over the last decade to culminate in a clear and unambiguous declaration that cyberattacks can trigger the invocation of Article 5. While the Alliance is committed to assist Allies in their defence efforts, it encourages the Member Nations to develop their own cyberdefence capabilities in the spirit of Article 3 of the North Atlantic Treaty. This evolutionary approach should be continued to ensure the adaptation of the Alliance’s cyberdefence policy to new trends in cyber operations, including the development of response options to e.g.:

1) cyber actions amounting to armed attacks;

2) the possibility of a broader application of cyber means and methods of warfare in future conflicts;

3) terrorist acts with the use of cyber means.

Adaptability and flexibility as well as a broad range of response options are a must in the world where the vulnerabilities of critical infrastructure are no secret and neither is the reliance of countries on critical infrastructure which in many cases is shared between two or more countries.

### Link Wall---Baltics

#### Baltic participation in tech innovation to counter hybrid threats drives multilateral adoption throughout Europe

Justinas Mickus 19, Associate Analyst of Vilnius Institute for Political Analysis, and Piret Kuusik, International Centre of Defence and Security Junior Researcher, October 2019, “The Baltic Risk Landscape,” https://efpi.icds.ee/wp-content/uploads/sites/18/2019/11/Mickus-Kuusik\_The-Baltic-Risk-Landscape\_October-2019.pdf

To an extent, then, the developed expertise in combatting cyber threats can and already has enabled the Baltic states to set multilateral standards and craft collective policy solutions in the field. And yet, with the increasingly widespread appreciation of hybrid and next-generation threats, the comparative advantage the Baltics have today will likely decrease in the future. Should Baltic politicians wish to further pursue leadership in cyber and hybrid security, they will require further policy innovation (a similar note could be made about the self-declared Baltic expertise on Russian/Eastern Neighborhood questions more broadly).

The Baltics, certainly, may also focus on other areas in which they play a unique role and boast unique expertise. Today, individual Baltic states have made significant inroads in developing notable expertise in e-governance (Estonia) or fintech (Lithuania). Survey respondents from Latvia and Estonia also demonstrate high appreciation for and diverse understanding of the impact the rising pace of technological change is likely have on Baltic politics. For both sets of respondents, this trend ranks among the top three and is connected with various economic, societal, and security risks (by contrast, increasing cyber-dependence is primarily through the security lens).

Whether they choose to further develop their hybrid and cyber capabilities or expand their focus to different fields, the Baltic states stand to benefit from international cooperation. As continuous policy innovation requires new inputs, seeking diverse international partnerships can greatly augment the policy instruments currently employed by the Baltic states. For example, should the Baltic governments focus on the trend of ageing population (among the experts surveyed, it ranked as the most important trend in the Baltic region), the could consult the expertise and experience of Japan, which has recently developed an ambitious strategy of tackling the transformation into a digital society for an ageing population.11

ACTIVE AND CONSTRUCTIVE MEMBERSHIP

Unique expertise alone is not sufficient for small states to shape the international order with the use of postwar institutions – there is a difference between being a one-issue state and the leader on the issue. Small states must simultaneously be active and constructive partners to other members of the core group of the postwar order. As their institutional innovations need the assent and backing of greater powers to have any tangible effect, fostering stable and productive partnerships with key allied powers to secure their buy-in is a necessary tactic for small states.

#### NATO’s hybrid warfare planning is concentrated in the Baltics.

Eoin Micheál McNamara 2016, PhD researcher at the University of Tartu where he has lectured in transatlantic relations, associate fellow at the Latvian Institute of International Affairs in Riga, “Securing the Nordic-Baltic region,” 17 March 2016, https://www.nato.int/docu/review/articles/2016/03/17/securing-the-nordic-baltic-region/index.html

Russia’s illegal annexation of Crimea in March 2014 and its military actions in Ukraine have led transatlantic policy-makers to reassess collective defence arrangements across what is frequently referred to as NATO’s “eastern flank”. Extending north partially beyond the “eastern flank” is a region that comprises eight Nordic and Baltic states, which have become increasingly interdependent in security terms. The region is of rising importance in the context of Europe’s changing security order – and defence and deterrence is set to be high on the agenda at NATO’s summit meeting in Warsaw, Poland, in July.

NATO has a strong role in coordinating closer security ties between the region’s states. Finland and Sweden are not members of the Alliance and are therefore not covered by NATO’s collective defence clause. However, the Allies are working closely with both countries – two of NATO’s most active partners – to assess security in the Baltic Sea region, to expand exchanges of information, including on hybrid warfare, coordinating training and exercises, and to develop better joint situational awareness.

The prospects are positive for improved NATO-Nordic-Baltic defence cooperation, yet a number of important challenges need to be overcome. The region will test NATO’s flexibility in strengthening defence ties among its members and crucial partner states.

#### Bolstering hybrid response in the Baltics is the first step towards broader NATO/EU adoption

Andrew Radin 17, political scientist at the RAND Corporation, 2017, “Hybrid Warfare in the Baltics: Threats and Potential Responses,” https://www.rand.org/content/dam/rand/pubs/research\_reports/RR1500/RR1577/RAND\_RR1577.pdf

Improving the response to potential Russian covert action can be thought of in three phases: detecting and attributing Russian action, strengthening the capacity of the Baltics to respond, and formulating an effective and appropriate EU and NATO response.

Better intelligence gathering and coordination and a clearer understanding of the signs of Russian covert aggression can help bolster defenses against active subversion. U.S. Air Force assets, such as unmanned aerial vehicles and ground-based radars, could be beneficial at filling gaps in these countries’ existing intelligence, surveillance, and reconnaissance capabilities, both for covert action and conventional warfare.7 NATO is also currently undertaking several initiatives to improve intelligence and coordination related to Russian covert action, including developing shared indicators and warnings, NATO Force Integration Units (NFIUs), and combined exercises. Although NATO has made progress in developing institutions for intelligence sharing, NATO’s structures and processes for intelligence sharing remain cumbersome and dependent on often-reluctant nations to share.8 Given NATO’s slow progress in this area, further developing bilateral intelligence sharing between the Baltic countries and the United States or other NATO countries could be valuable. Additional research could also contribute by identifying the signs and mechanisms of past instances of large-scale Russian covert activities in Georgia, Crimea, and eastern Ukraine. So far, there is little open source information about how to differentiate between “everyday” Russian exercises and influence operations and the start of a large-scale campaign mirroring the operation in Crimea. More clearly identifying the modus operandi of Russian agents would help to separate out the cases that justify a NATO deployment and those that might not.

The capacity of the Baltic countries to counter covert action can certainly be improved. U.S. special operations forces have conducted extensive engagement with their Baltic counterparts, to the point that there is a sense of saturation, especially given the small size of the Baltic special operations forces. Additional research may be beneficial to help identify gaps in the Baltic countries’ capacity, including within civilian agencies, and to conduct targeted missions that could offer more focused benefits. Support for the Baltic states to counter covert action may also strengthen their ability to resist Russia in the event of an invasion.9 The U.S. Air Force may be able to directly assist with the development of technical capabilities for border control, air and maritime domain awareness, and intelligence gathering, including assistance with acquiring unmanned aerial vehicles, radars, and other sensors. Another specific area where the United States may be able to offer assistance is in planning exercises and war games to improve contingency planning and coordination, especially in Latvia.

Finally, the United States, NATO, and the Baltic countries can do more to think practically through how a response to Russian covert action would proceed. The 2014 Wales Summit focused on the development of greater “responsiveness” through the Readiness Action Plan and the creation of the Very High Readiness Joint Task Force (VJTF). However, it remains uncertain how these new, more responsive forces would be employed if there was warning of a significant Russian covert (or conventional) military action in the Baltics.10 While the development of the VJTF and implementation of the Readiness Action Plan is complex and will take time, it is highly beneficial for the United States and other NATO allies to think through on a practical level how a high-readiness forces would deploy and be employed in the Baltics, and how they would coordinate its actions with the Baltic security forces.

### Innovation IL---K2 Tech Edge

#### NATO innovation is key to maintaining the tech edge against competitors while preserving shared Allied values

Rob Murray 20, head of the Innovation Unit in NATO’s Emerging Security Challenges Division, MSc, ISR Management, University of Lincoln, MBA, The University of Chicago Booth School of Business, MA, International Policy and Diplomacy, Staffordshire University, 9/1/20, "Building a resilient innovation pipeline for the Alliance", NATO Review, https://www.nato.int/docu/review/articles/2020/09/01/building-a-resilient-innovation-pipeline-for-the-alliance/

Sceptics will say this would present big tech with too many opportunities for mergers and acquisitions and thus create monopolistic risk. They might be right and clearly incentives for all parties would need to be found. But, if we are to win the technological adoption race built upon liberal democratic values, we need to use every advantage we have.

To utilise, adopt and scale these technologies effectively, we must have at the forefront of our minds the need to work at the speed of relevance rather than the speed of approval. This means new ways of financing technologies, interacting with tech firms both big and small, and much more agile acquisition models, which carry the empowerment and incentives to those responsible for equipping the Alliance. Such a cultural shift will not be easy – but innovation rarely is.

As we look towards NATO 2030 and heed Eisenhower’s words of achieving both security and solvency, while noting that the foundation of military strength is economic strength, a resilient innovation pipeline that leverages our comparative advantage, creativity and capital will be critical to the Alliance maintaining its technological edge built on shared Allied values.

### Innovation IL---NATO-Led Key

#### NATO is key to innovation---fragmenting efforts won’t means we lose the tech edge to competitors

#### NATO focus has a stronger effect on innovation priorities

Rob Murray 20, head of the Innovation Unit in NATO’s Emerging Security Challenges Division, MSc, ISR Management, University of Lincoln, MBA, The University of Chicago Booth School of Business, MA, International Policy and Diplomacy, Staffordshire University, 9/1/20, "Building a resilient innovation pipeline for the Alliance", NATO Review, https://www.nato.int/docu/review/articles/2020/09/01/building-a-resilient-innovation-pipeline-for-the-alliance/

But before we get to commercialisation, we need to create the direction of what it is we wish to see commercialised. Technological disruptive innovation does not just happen. It starts with a mission-oriented vision, where measuring risk is impossible and only uncertainty reigns. It requires bold moves that will signpost the future; the confidence to place big bets on technology not yet invented; and an ability to pick winners – all of which must be underpinned by persistent engagement, encouragement and enlightenment. Since the end of the Second World War, only one entity has taken-on such uncertainty: Allied governments (see image below).

Step 1: agree innovation priorities among Allies

The first step towards fixing the fragmentation of Allied disruptive innovation is for Allies, through the NATO framework, to focus on agreed innovation priorities. This will allow them to pick winners and invest public patient capital – the private sector is unlikely to invest venture capital as the risk is simply too high (nations tend not to go out of business and can take on such uncertainty). This direction and investment will help to maintain NATO’s overarching technological edge. Indeed, as Keynes and Weber argued, the ability to make things happen that otherwise would not needs a combination of technological, policy and bureaucratic skills matched by investment

#### Networking is key to maximize innovation

Rob Murray 20, head of the Innovation Unit in NATO’s Emerging Security Challenges Division, MSc, ISR Management, University of Lincoln, MBA, The University of Chicago Booth School of Business, MA, International Policy and Diplomacy, Staffordshire University, 9/1/20, "Building a resilient innovation pipeline for the Alliance", NATO Review, https://www.nato.int/docu/review/articles/2020/09/01/building-a-resilient-innovation-pipeline-for-the-alliance/

Step 2: leverage the comparative advantage of the Alliance

If Allies are to achieve most defence at less cost with least delay built with wisdom and efficiency, then it is logical to leverage those natural advantages that geography and skill sets afford NATO member states. A network of the finest universities across the Alliance should be established and resourced to allow cutting-edge multinational research to take place across multiple disruptive technologies simultaneously. Perhaps Stanford could lead on relevant AI research, while Delft and the University of Chicago partner on quantum; maybe Imperial College London looks at biotechnologies with Johns Hopkins University, while Tallinn University centres its efforts on next generation cyber defences; and the École Polytechnique and Massachusetts Institute of Technology examine future telecommunication needs.

The point is Allies will need to leverage such networks of universities in conjunction with national government research labs to provide maximum innovation coherence. The diversity of multinational, multi-disciplined defence and security innovation research teams, which NATO can engender, is a huge asset and is the Alliance’s competitive advantage.

#### Solves foreign ownership concerns

Rob Murray 20, head of the Innovation Unit in NATO’s Emerging Security Challenges Division, MSc, ISR Management, University of Lincoln, MBA, The University of Chicago Booth School of Business, MA, International Policy and Diplomacy, Staffordshire University, 9/1/20, "Building a resilient innovation pipeline for the Alliance", NATO Review, https://www.nato.int/docu/review/articles/2020/09/01/building-a-resilient-innovation-pipeline-for-the-alliance/

Utilise, adopt and scale

Where the first stage of NATO’s innovation pipeline should centre on the creation of disruptive innovative technologies, stage two is all about their utilisation and adoption at scale.

Utilisation

This is where initial public venture capital (VC) entities, such as in-q-tel, NSSIF, DefInvest and SmartCap, can help ‘crowd in’ trusted private venture capital to provide safe financing to NATO’s fledgling start-ups, thereby minimising their susceptibility to nefarious foreign direct investment. This issue is impacting many start-ups as they raise funds and carries implications when they wish to export their products but may not be able to, due to unfriendly foreign ownership and technology transfer concerns raised by Allied governments.

In addition to Venture Capital entities supporting the trusted financing of Allied start-ups, innovation accelerators – in combination with elite universities, and supported by Allied defence professionals (operators, investors and procurement experts) – can help provide the necessary ‘polish’ to start-ups and their value propositions. This will create the necessary ecosystem to maximise the likelihood of commercial success. The United States’ Air Force Ventures is an interesting model of this approach, which helps to acquire new start-up products at speed without being bogged down by acquisition bureaucracy.

#### Startups need NATO to get off the ground

Rob Murray 20, head of the Innovation Unit in NATO’s Emerging Security Challenges Division, MSc, ISR Management, University of Lincoln, MBA, The University of Chicago Booth School of Business, MA, International Policy and Diplomacy, Staffordshire University, 9/1/20, "Building a resilient innovation pipeline for the Alliance", NATO Review, https://www.nato.int/docu/review/articles/2020/09/01/building-a-resilient-innovation-pipeline-for-the-alliance/

Adoption

But even when dual-use disruptive innovation is commercialised, turned into prototypes and the product/market fit is achieved, the challenge of getting initial contracts from customers (both government and commercial) remains. Cash is king for young companies, as they do not have the financial reserves to work through long acquisition processes often associated with Allied governments. If start-ups cannot close deals in a matter of weeks and months rather than quarters and years, then they would not attempt to (opportunity cost).

Now, some commentators may argue: Why spend so much time discussing start-ups? Traditional large armaments companies can be innovative. Why go through all this effort for tiny companies that may or may not make it?

The reason is simple: the competition and creativity generated by start-ups is good for the Allied defence ecosystem. Allied open democracies and open educational models bring about levels of creativity which other forms of government are unable to do. This maximises disruptive innovation efforts and, as such, forces incumbents (large companies) to compete with new, fresh thinking – it builds resilience.

Such creativity and disruption is NATO’s competitive advantage. Therefore, NATO needs to adapt its acquisition models to accommodate start-ups, their timelines and their potential. This fundamentally means our acquisition professionals should be empowered to take measurable risk. As one Ally’s legislative body recently remarked: “Defence stakeholders must integrate the risk culture, which is the only way to both enable innovation in defence and to very quickly capture dual or civilian innovation. Acculturation to innovation is a priority.”

Scaling

If we have managed to commercialise new technology, adopt it quickly as a prototype and now wish to scale, how might this be done? Big tech could have a role to play here. In May, it was reported that, in the first quarter of 2020, Facebook, Apple, Amazon, Alphabet and Microsoft spent over 29 billion US dollars on research and development (R&D). That is more than the entire 2020 NASA budget and represents a 17 per cent increase on the same time period last year.

In November 2018, the US Congressional Research Service noted: “In 1960, the United States accounted for 69% of global R&D, with U.S. defense-related R&D alone accounting for more than one-third of global R&D (36%). Additionally, the federal government funded approximately twice as much R&D as U.S. business. However, from 1960 to 2016, the U.S. share of global R&D fell to 28%, and the federal government’s share of total U.S. R&D fell from 65% to 24%, while business’s share more than doubled from 33% to 67%. As a result of these global, national, and federal trends, federal defense R&D’s share of total global R&D fell to 3.7% in 2016.”

Big tech has the resources and wherewithal to be able to scale new technologies at speed. They could partner with successful start-ups, perhaps through a joint venture or an Alliance-wide public-private partnership, to provide those scale-up skills that start-ups lack (for example, compliance, legal support, production on mass, intellectual property protection) without necessarily acquiring these young companies.

### Innovation IL---AT: Gov Innovation Fails

#### Gov innovation works

Rob Murray 20, head of the Innovation Unit in NATO’s Emerging Security Challenges Division, MSc, ISR Management, University of Lincoln, MBA, The University of Chicago Booth School of Business, MA, International Policy and Diplomacy, Staffordshire University, 9/1/20, "Building a resilient innovation pipeline for the Alliance", NATO Review, https://www.nato.int/docu/review/articles/2020/09/01/building-a-resilient-innovation-pipeline-for-the-alliance/

As the image above shows, governments have done this before and the technologies created (internet, GPS, touchscreen et al, which fed into the building of the iPod and iPhone) have had a huge impact on the way we live. However, for all those successes, there will have been many failures and this is where Allies will need to get comfortable. To quote one anonymous Allied defence innovator: “if our success rate begins to go above 35 per cent, I start to worry. It means we’ve stopped taking big enough risks.” Indeed, obvious research areas Allies might collaborate on include the follow-on to 5G or the technology needed to enable total supply chain assurance, for example.

#### Yes capabilities

Rob Murray 20, head of the Innovation Unit in NATO’s Emerging Security Challenges Division, MSc, ISR Management, University of Lincoln, MBA, The University of Chicago Booth School of Business, MA, International Policy and Diplomacy, Staffordshire University, 9/1/20, "Building a resilient innovation pipeline for the Alliance", NATO Review, https://www.nato.int/docu/review/articles/2020/09/01/building-a-resilient-innovation-pipeline-for-the-alliance/

In aggregate, the Alliance has an abundance of world-class academic institutions, the finest scientific researchers, amazingly creative start-ups and a mature well-resourced financial eco-system. These constitute the core ingredients, which, when combined and focused, can solve dual-use, ‘tough-tech’ problems – that is, challenges facing both defence and non-defence sectors, such as augmented reality and quantum computing.

#### Yes incentive

Rob Murray 20, head of the Innovation Unit in NATO’s Emerging Security Challenges Division, MSc, ISR Management, University of Lincoln, MBA, The University of Chicago Booth School of Business, MA, International Policy and Diplomacy, Staffordshire University, 9/1/20, "Building a resilient innovation pipeline for the Alliance", NATO Review, https://www.nato.int/docu/review/articles/2020/09/01/building-a-resilient-innovation-pipeline-for-the-alliance/

A dual-use model is important for disruptive defence innovation because when we eventually get to commercialising such tough-tech breakthroughs, Allies will need start-ups and tech firms to maximise the reach of their products by looking at ‘total addressable problems’ rather than ‘total addressable markets’. In other words, we should not want start-ups building the next wave of technology to have governments as their only customer. We want such technologies to benefit society too and therefore have civil, commercial use. Such commercial use then drives the subsequent development of said technology, pulling the government-side along with it, which means better products and technology all round – building defence with wisdom and efficiency.

Indeed, dual-use potential will help align the incentives of our researchers, entrepreneurs and finance communities as the prospective commercial upside (problem) will be big enough for them to undertake the investment of commercialisation. The geopolitical advantage such disruptive innovation fosters (picking winners via big bets on the next breakthrough) will also be large enough to allow for its creation via early stage patient public sector capital investment.

### Innovation IL---Commitment Key

#### Commitment generates urgency---motivation gaps risk military failure

Paul Bernstein 19, a distinguished research fellow at the Center for the Study of Weapons of Mass Destruction (WMD Center) of the National Defense University in Washington, DC, ““Innovating” Versus “Out-Innovating”: Innovation as a Form of Strategic Competition”, Getting Innovation Right, Center for Global Security Research, Lawrence Livermore National Laboratory, Sept 2019, https://www.osti.gov/servlets/purl/1635772

Second, we need a sense of urgency and the means to accurately assess what others are doing. Russia and China are committed to developing leading-edge military technologies and fielding “high-tech forces” in part because they see U.S. dominance as an existential threat. They are highly motivated. It is not clear the United States is as sharply motivated, which creates the potential for a focus or commitment gap. Closing any such gap is something leadership should pay attention to; otherwise it may take a crisis or a military failure to generate the necessary sense of urgency.

### Innovation IL---Integration Key

#### Integration is key---we need to incorporate all elements of innovation to outcompete great powers

Paul Bernstein 19, a distinguished research fellow at the Center for the Study of Weapons of Mass Destruction (WMD Center) of the National Defense University in Washington, DC, ““Innovating” Versus “Out-Innovating”: Innovation as a Form of Strategic Competition”, Getting Innovation Right, Center for Global Security Research, Lawrence Livermore National Laboratory, Sept 2019, https://www.osti.gov/servlets/purl/1635772

Third, we need an integrated approach. A dynamic approach to innovating for operational advantage requires taking account of all forms of innovation, determining the appropriate mix for the types of conflicts the armed forces are likely to engage in and the specific operational challenges they will need to overcome. Innovation encompasses not only technology but also operational concepts and organization/ process. Military innovation and transformation leaders have long argued against an overemphasis on technology at the expense of other factors. Typically it is some combination of technology, concepts, and organization that provides a basis for breakthroughs. Often we are reminded of this when an adversary demonstrates it.

High-end regional war is generally the default lens through which we view requirements for innovation and it may be true that the bulk of defense innovation will be directed at this problem. But the spectrum of conflict also includes hybrid warfare (a mix of regular and irregular armed conflict) and coercive activities short of armed conflict (“political warfare”)—modes of conflict that are not entirely new, but whose contemporary manifestations are indeed novel and for which the United States generally seems poorly prepared. We cannot dismiss the requirements for innovation in these aspects of great power competition, not least because they may lead us down pathways much different from those shaped by the demands of highend regional war.

The following matrix may be useful as a very simple way to visualize the “battlespace” for innovation.

It is worth noting here that political warfare may be somewhat anomalous when considered as an arena of great power competition. In this domain, the goal of the United States and its partners is not to out-innovate adversaries so as to build the more advanced toolkit for political subversion, social division, economic warfare, and coercion. Rather, the West’s goal is to greatly improve the ability of liberal states to reduce their vulnerability to such strategies and actively resist them. This is a somewhat different context for innovation, but an important one given the strategic stakes.

### Innovation Impact---China AI

#### China AI competition escalates

Calum Chace 20, co-founder of the Economic Singularity Foundation, global keynote speaker about AI, MBA, Cranfield University, 6/30/20, "Thucydides And The Dragon: Artificial Intelligence And Sino-US Rivalry", Forbes, https://www.forbes.com/sites/calumchace/2020/06/30/thucydides-and-the-dragon-artificial-intelligence-and-sino-us-rivalry/#1c7a93d94fc1

From Cold War to Code War?

The most dangerous source of conflict could be China’s determination to catch up with and then surpass America as the leading developer of AI, our most powerful technology. Some fear that the Cold War between the two nuclear superpowers could be followed by a Code War between its two AI superpowers.

Taiwanese venture capitalist Kai-Fu Lee, a former Google and Apple executive, argues that China will overhaul the US in AI because it has more hard-working and aggressive entrepreneurs and researchers, and also because it has a disregard for privacy which allows its researchers to amass more data. “If data is the new oil, China is the new Saudi Arabia”, as one critic put it.

It is true that the 9-9-6 work ethic (72 hours a week) makes Chinese startup scene a highly competitive one. Many Chinese students no longer want to stay in the US when they finish their degrees in computer science. They are keen to return home and get rich there.

Do Chinese people care about privacy?

It is also true that China’s attitude to privacy distinguishes it from the US, and even more from Europe. The Social Credit system being pioneered today has the potential to become a level of government surveillance that would make Big Brother jealous. This is happening partly because the communist party wills it so, and resistance is pretty much impossible for most citizens. It is also partly because corruption is endemic and severe in China, and levels of trust outside family networks are low. A system which punishes anti-social behaviour swiftly and effectively is less resisted in China than it would be elsewhere.

But we should not over-state the extent to which being oblivious to privacy issues is a killer app. China watcher JJ Ding argues that Chinese people do care about privacy, and that the government knows it cannot take their acceptance for granted. The US tech giants still have a significant lead in technology and expertise, and they still have momentum. AI is increasingly a duopoly between China and the US, not an emerging Chinese hegemony.

The US managed to avoid the utter disaster of full-scale military confrontation with the Soviet Union, and in many ways its relations with China are much closer, which should make confrontation less dangerous. The US economy is less open than those of most developed countries – trade accounts for 27% of US GDP, compared to 61% for the UK, and 33% for China. But the US and Chinese economies are far more entwined than America’s ever was with the Soviet Union. GM sells more cars in China than in the USA and Canada combined, and Apple, Qualcomm and most other large US companies are similarly exposed.

Avoiding the splinternet: a role for Europe

Trump’s populist attacks on Huawei won’t kill it, although they could certainly curb its growth, and perhaps shrink it for a while. In the longer run they could easily have the perverse effect of damaging the US tech sector: China may decide that America is an inherently untrustworthy partner, and make the very heavy investments of time and treasure required to wean itself off US suppliers, and build its own chip industry, for instance. They could lead to “the splinternet”, a fracturing of the world’s technology ecosystem into two distinct communities, which would make global co-operation harder, and provoke mutual fear and suspicion.

War between China and the US (or NATO) is the worst possible outcome, but at this stage it still looks unlikely. Both the US and Chinese governments must walk a tightrope between pursuing their legitimate grievances on the one hand, and provoking outright hostility and communications breakdown on the other. This requires wisdom and diplomatic skills which are not prominently on display in both Beijing and Washington at the moment.

It would help if there were three AI superpowers, not just two. AI is not a race, as there is no finish line, and unless the internet splinters completely, the advances made by any party help everyone. But at the moment, Europe is barely involved. That ought to change, and soon.

### Innovation Impact---China Quantum

#### China quantum competition escalates

Arthur Herman 19, director of the Hudson Institute's Quantum Alliance Initiative, 11/10/19, "The Quantum Computing Threat to American Security", Wall Street Journal, https://www.wsj.com/articles/the-quantum-computing-threat-to-american-security-11573411715

Google announced last month that it had achieved "quantum supremacy," demonstrating the potential of a new kind of computer that can perform certain tasks many orders of magnitude faster than the most advanced supercomputers. It's a crucial moment for America's national security, which depends on winning the race to do what quantum computers will do best: decrypt the vast majority of existing public-key encryption systems.

Google reports that its quantum computer, dubbed Sycamore, solved a mathematical calculation in 200 seconds that would take a supercomputer 10,000 years. IBM, a quantum competitor, asserted that Google's claim of supremacy is overblown, and that the world's most powerful classical computer, the Summit OLCF-4 at Oak Ridge National Laboratory, could have done the same calculation in 2.5 days—roughly a thousandfold difference rather than 1.5 trillionfold. Still, quantum computers are no longer science fiction.

To process information, digital computers use bits, essentially switches that can be either off or on, corresponding with the binary digits, 0 and 1. Quantum computers employ "qubits," which use the probabilistic nature of quantum physics to represent any combination of 0 and 1 simultaneously, enabling them to encode more complicated data.

Their computing power grows exponentially as the number of qubits expands. Sycamore's 54-qubit chip allowed it to outcompute the best supercomputer. A 2,000- to 4,000-qubit quantum computer would render most public-key encryption architectures—used for applications from banking and credit cards to the power grid—obsolete. They rely on numbers too big for conventional computers to factorize, but which a quantum computer could.

Building quantum computers is a very heavy lift. They require hugely expensive infrastructure to stabilize the qubits at temperatures near absolute zero. They also generate high error rates, or "quantum noise," for which researchers have to compensate. Developers are probably years away from the large-scale code-breaking quantum computer everyone worries about—although once scientists and engineers start using quantum computers to build the next generation of quantum computers (since modeling complex systems like themselves is one of their strengths) the timeline could quickly shorten.

Beijing is America's chief quantum-computing rival. It spends at least $2.5 billion a year on research—more than 10 times what Washington spends—and has a massive quantum center in Hefei province. China aspires to develop the code-breaking "killer app," which means protecting U.S. data and networks from quantum intrusion is a vital security interest.

Congress enacted the National Quantum Initiative Act late last year, which commits an additional $1.25 billion over five years—still a fraction of China's effort. In addition to more money, the U.S. needs a three-phase national-security strategy to protect and defend American data, networks and infrastructure from future quantum attack.

First, dramatically increase efforts to develop encryption methods based on algorithms large and complex enough to foil quantum intrusion. The National Institute of Standards and Technology is working to set a comprehensive standard for these quantum-resistant algorithms so they can be deployed by 2024, but companies in the U.S., Canada and elsewhere are already building algorithms and other protective tools.

Second, use quantum technology itself to create the "unhackable" networks of the future. The same particles that make quantum computing possible can provide randomized and unhackable keys for encrypted transmissions, in the form of quantum random number generators and quantum key distribution, a method of securing information shared between two parties. Dismissed as a fantasy a few years ago, quantum cryptography has spawned companies in the U.S., Switzerland, South Korea and Australia, which are deploying the first components of a new quantum-based information-technology infrastructure. Eventually this will include satellites using quantum keys to transmit encrypted data.

Here again China has moved quickly. It launched the world's first quantum satellite in 2016 and shocked the world by creating a quantum-encrypted intercontinental video link from space to a China-Austria study group in Vienna. China has also created a 1,263-mile ground link between Beijing and Shanghai using quantum-encrypted keys between relay stations, which offers an ultrasecure network for transmitting sensitive data, including for China's military and intelligence services.

Third, require that all U.S. data and networks, including future 5G technology, be made secure from quantum attack while devoting resources to build the hack-proof quantum communication networks of the future. That will require working with America's closest allies, several of which are making key breakthroughs in the same quantum and postquantum technologies.

Promoting such cooperation has been a core mission at the Quantum Alliance Initiative, which convened a consortium of companies and universities from the U.S. and allied countries to develop global standards for quantum random number generators and quantum key distribution late last year. But no one can do all this alone, not even Google plus IBM plus Microsoft and the other big companies working in quantum computing. Leadership from the federal government is more imperative than ever. Google's breakthrough proves that the threats, as well as the opportunities, of quantum technology are real—and that quantum is poised to become the national-security issue of the 21st century.

## ADV CP

**OFF**

**The United States federal government should**

**-emphasize its Article 5 commitment to NATO member states in response to Russian gray zone aggression**

**-re-establish consistent communication avenues with Moscow over gray zone activities**

**-reinvigorate efforts to extend New START and expand the agreement to include the cyber domain and future weapons**

**Hotlines and communication are key---clarification alone has no deterrent effect**

Whitney L. **Cissell 20**, MA thesis in Security Studies, Naval Postgraduate School, Army Major, Nuclear Nonproliferation Officer, March 2020, "DETERRENCE IN THE DANGER ZONE: HOW THE UNITED STATES CAN DETER RUSSIAN GRAY ZONE CONFLICT", https://calhoun.nps.edu/handle/10945/64844

2. Communication

Communication between the United States and Russia is at an all-time low since the end of the Cold War, yet it is a critical element in the framework of deterrence, especially at the sub-conventional level, where the cost of action is low and attribution is difficult. An effective deterrence strategy relies on Washington’s re-establishing consistent communication avenues with Moscow. These avenues must include both strategic and sustained communication, each of which has formal and informal components. Effective communication allows the United States to employ a dual-pronged deterrent strategy utilizing deterrence by denial and deterrence by punishment through focusing its punitive efforts on key gray zone actions while reserving resources for denial efforts, such as resiliency and information operations. Douglas Lute explains, “It’s not enough for the U.S. to have these threats and believe them; in fact, that has no deterrent effect. The critical thing is to communicate them in a clear, unambiguous, and consistent way with Russia.”261 U.S. threats will not be credible if they promise an escalation that Russia is not likely to believe.262 Identifying gray zone activities that the United States will not tolerate and communicating these limits to Russia bolster the credibility of the punitive threat assigned to those actions.

**Extending New START stabilizes the gray zone**

Whitney L. **Cissell 20**, MA thesis in Security Studies, Naval Postgraduate School, Army Major, Nuclear Nonproliferation Officer, March 2020, "DETERRENCE IN THE DANGER ZONE: HOW THE UNITED STATES CAN DETER RUSSIAN GRAY ZONE CONFLICT", https://calhoun.nps.edu/handle/10945/64844

a. Formal Diplomacy

Formal diplomacy between the United States and the Soviet Union, and now Russia, has been a stabilizing force in the bilateral relationship since the Cold War and, furthermore, has contributed to the safety and security of the international security environment. Treaties and confidence-building measures that modify behavior set the standard for how states conduct business, and develop trust. The Open Skies Treaty, the Comprehensive Test Ban Treaty, and arms control have been staples of the U.S.–Russian relationship. While some diplomatic measures are still in place, or followed even if they have not been ratified, the erosion of formal diplomacy in recent years has reduced the trust and communication between the United States and Russia, causing a destabilizing effect on deterrence, specifically in the sub-conventional level.

To deter Russian gray zone aggression, many subject matter experts suggest reinvigorating efforts to extend New START. The treaty between the United States and Russia, which entered into force in February 2011, sets “measures for the further reduction and limitation of strategic offensive arms.”283 The treaty also provides confidencebuilding measures that encourage transparency such as on-site inspections, data exchanges, notifications, and the exchange of predicted yearly numbers of ballistic missiles (both sea and land based).284 Panetta suggests, “The U.S. should not only reignite interest in extending the New START treaty, but also in developing an improved agreement for the future, one that possibly includes the cyber domain and future weapons.”285 Since the dissolution of the INF in 2019, the bilateral New START is the last remaining formal arms control measure between the United States and Russia and is key in keeping formal diplomatic relations afloat.

**Comm Plank---Solvency---Deterrence**

**Communication solves deterrence---it’s a foundational condition necessary for success---provides Russia with assurances and alternative options, while forwarding human relationships**

Whitney L. **Cissell 20**, MA thesis in Security Studies, Naval Postgraduate School, Army Major, Nuclear Nonproliferation Officer, March 2020, "DETERRENCE IN THE DANGER ZONE: HOW THE UNITED STATES CAN DETER RUSSIAN GRAY ZONE CONFLICT", https://calhoun.nps.edu/handle/10945/64844

A. NECESSARY CONDITIONS FOR A DETERRENT STRATEGY

A necessary condition for deterrent success that is specific to the sub-conventional level and the current security environment is a shift in the deterrence mindset away from zero tolerance of deterrence failure toward a cumulative deterrence posture that focuses on maintaining overarching credibility via tailored responses to targeted gray zone activities when deterrence and denial fail. Additionally, for any deterrent strategy to be applied, the foundational conditions of deterrence must be in place, including communication and diplomacy to provide assurances and alternate options to an adversary. Leon Panetta asserts, “Communication with adversaries is imperative to have. It serves to forward human relationships that are critical in the ability to create dialogue and keep open lines of communication.”255 Since the end of the Cold War, these conditions have deteriorated between the United States and Russia, and restoring them is essential.

**Comm Plank---Solvency---Accidents**

**Hotlines solve accidents**

Whitney L. **Cissell 20**, MA thesis in Security Studies, Naval Postgraduate School, Army Major, Nuclear Nonproliferation Officer, March 2020, "DETERRENCE IN THE DANGER ZONE: HOW THE UNITED STATES CAN DETER RUSSIAN GRAY ZONE CONFLICT", https://calhoun.nps.edu/handle/10945/64844

In addition to diplomatic and military communication, communication during a crisis is critical in the maintenance of a deterrent posture. Just after the Cuban Missile Crisis, the United States and the Soviet Union signed a 1963 memorandum of understanding that established a direct link between the two states. The “hotline,” as it was called, was “a quick communication link between heads of states . . . designed to reduce the danger of an accident, miscalculation or a surprise attack.”275 The hotline was used multiple times throughout history and has since been transitioned to the Nuclear Risk Reduction Center, where its role has been expanded to include providing an communication between the United States and Russia for “the exchange of notifications under treaties, goodwill notifications, and for emergency communication during a major fire in the U.S. Embassy in Moscow.”276 Although the hotline was established to prevent crisis and escalation to nuclear war, it has proven an effective means of communication during both crisis and stability between Washington and Moscow. Robert Gates, former CIA director and defense secretary, stated that the hotline is a critical tool “as long as these two sides have submarines roaming the oceans and missiles pointed at each other.”277

In today’s context, where most of the conflict between great powers is conducted below the level of conflict for which the hotline was created, the hotline’s utility can be expanded as a tool to re-establish communication and broaden communication to include immediate gray zone issues. Considering the increased risk of miscalculation based on the current lack of communication and the ability for gray zone operations to escalate, a crisis hotline is a rational and effective communication avenue that is already established and can be immediately utilized to kick-start communication. The communication can even start within the parameters of the existing framework of the NRC to encourage discourse and submit proposals or grievances over the extension of New START.

**Comm Plank---AT: Russia Says No**

**Russia says yes---military communication proves**

Whitney L. **Cissell 20**, MA thesis in Security Studies, Naval Postgraduate School, Army Major, Nuclear Nonproliferation Officer, March 2020, "DETERRENCE IN THE DANGER ZONE: HOW THE UNITED STATES CAN DETER RUSSIAN GRAY ZONE CONFLICT", https://calhoun.nps.edu/handle/10945/64844

Despite the plummeting political relations between the United States and Russia, military communication has remained, even if in a limited fashion. Military contact has served as a mainstay of communication between the states since 2014 and the expulsion of many Russian diplomats. At the top levels of military leadership, the chairman of the Joint Chiefs of Staff, U.S. Army General Mark Milley, and the Russian chief of the General Staff, General Valery Gerasimov, continue a limited but regular dialogue. Ulrich Kühn argues, “NATO should aim to re-establish . . . communications channels with the Russian General Staff at the working level.”273 The top-level interaction is a positive foothold in U.S.–Russian communication; however, more frequent communication is needed. Recently, the interaction between the top levels has increased, including a physical meeting in Switzerland “aimed at increasing communication between their nations to reduce risks in conflict areas.”274 Efforts are in place to improve military communication and could be enhanced through the replacement of the Russian liaison at SHAPE and by acting on Kühn’s suggestion of re-establishing working-level military communication. These improvements to military communication could set the framework of positive relations between the states to usher in future consistent diplomatic communication, which is crucial for deterrence.

**New START Plank---Solvency---Deterrence**

**Reinvigorating New START discussions pacifies tensions---it convinces Putin gains aren’t zero-sum and that de-escalation is mutually beneficial**

Whitney L. **Cissell 20**, MA thesis in Security Studies, Naval Postgraduate School, Army Major, Nuclear Nonproliferation Officer, March 2020, "DETERRENCE IN THE DANGER ZONE: HOW THE UNITED STATES CAN DETER RUSSIAN GRAY ZONE CONFLICT", https://calhoun.nps.edu/handle/10945/64844

3. Diplomacy

Through diplomacy, it is possible for the United States and Russia to build lasting cooperation through formal agreements, mutual interests, and established codes of conduct. This section explores both formal and informal diplomacy followed by a discussion of U.S. and Russian common interests detailing specific categories in which diplomacy could be renewed. However, diplomacy must be a first-line option supported by credible threats of denial and punishment. Anthony Cordesman explains, “The one thing that you cannot do is use diplomacy as a substitute for countermeasures.”278 It is critical to recognize that every effort spent toward diplomacy can help stabilize U.S.–Russian relations at the nuclear and conventional level. Improved stability at these levels can alleviate tension and reveal where instability is still present at the sub-conventional level.

Washington must operate from a place of strength to affect Putin’s cost–benefit analysis through deterrence by denial, supported by punishment, while also giving him a diplomatic alternative. Brad Roberts explains that during his time with the Obama administration, it was clear that “President Putin concluded that there was a fundamental conflict of interest with the United States, that it was a zero-sum game. The U.S. was pursuing interests against Russia that were simply unacceptable to President Putin, and as such, he reconceived a relationship of enduring conflict.”279 As described in earlier chapters, the United States attempted to demonstrate that Putin had taken too dark a view of American interests and through diplomatic opportunities sought to pursue mutual interests and pragmatic cooperation in various areas; however, the efforts failed. Roberts explains that this conflictual relationship does not have to be inevitable: “It is a matter of political calculus emanating from a particular person at a particular time.”280 This would suggest that to restore diplomatic cooperation with Russia, Putin’s decision calculus must be influenced to convince him that it is in his best interest.

Cordesman illustrates that “the U.S. tends to deal with Russia in terms of the sticks and often does not have a well-defined set of carrots.”281 Cordesman goes on to explain that a necessary addition is “offering a well-defined alternative in terms of cooperation where the U.S. and Russia both benefit.”282 Operating a deterrent strategy solely on punishment threats is dangerous because, although it is imperative to signal to Russia that there are penalties for misbehavior, the United States must also signal assurance for compliance. With established communication, diplomacy will facilitate not only that acceptable alternative but also aspire to build formal and informal agreements that bound sub-conventional conflict, decrease the risk or escalation, and provide insight toward an adversary’s intent.

**New START Plank---AT: Fails/Won’t Happen**

**Even if New START isn’t extended, the CP still solves gray zone deterrence by spurring future agreements, correcting misperceptions, and avoiding accidents---the unilateral commitment is sufficient**

Whitney L. **Cissell 20**, MA thesis in Security Studies, Naval Postgraduate School, Army Major, Nuclear Nonproliferation Officer, March 2020, "DETERRENCE IN THE DANGER ZONE: HOW THE UNITED STATES CAN DETER RUSSIAN GRAY ZONE CONFLICT", https://calhoun.nps.edu/handle/10945/64844

Even if New START is not extended, discussions over the treaty’s contents could be used to spur discussion on a new arms control treaty or, at the very least, a broader discussion and effort toward multilateral arms control. Kühn explains that discussions about arms control are “particularly important since the strategic nuclear dialogue between Washington and Moscow effectively petered out after the New START entered into force in 2011.”286 Kühn suggests, “Reconvening NATO–Russian talks about military strategy and nuclear doctrine, which had been ongoing prior to Russia’s annexation of Crimea, could help dispel misperceptions and thus avoid inadvertent escalation.”287 As the timetested formula for risk reduction is deterrence plus diplomacy, Kühn’s suggestion to reconvene NATO–Russian communication, combined with U.S.–Russian efforts toward New START or a similar treaty, would likely bolster deterrence of the gray zone.

These efforts to reinstate formal diplomacy would emphasize the U.S. resolve toward diplomacy and simultaneously signal to Russia that the use or threat of tactical nuclear weapons is not in its interest as a state.288 By addressing the unacceptable use of tactical nuclear weapons in the context of arms control, Washington has a forum to address the issue while it reaffirms the nuclear taboo and communicates to Moscow that any use of a nuclear weapon will be met with grave U.S. and international consequences. This reaffirmation of non-use drives the U.S.–Russian conflict back to the sub-conventional level, allowing the United States to focus resources and diplomacy efforts on the gray zone.

In a situation where the United States and Russia do not extend New START, formal diplomacy could be achieved through a unilateral approach. To show commitment and a willingness for diplomacy, the United States could make a public commitment to data exchanges and inspections in line with what would have occurred if New START had been extended. The United States could also make a public commitment to maintaining the limited number of weapons designated by New START. These commitments would foster an environment ripe for continued formal negotiations of a future arms agreement between the United States and Russia as well as open the path to informal diplomacy between the states.

**Perm---AT: Do Both**

#### Causes mixed signals which escalate conflict

Alexander **Klimburg 20**, a non-resident senior fellow at the Atlantic Council, 2/4/20, "Mixed Signals: A Flawed Approach to Cyber Deterrence", Survival, Global Politics and Strategy, Volume 62, Issue 1, <https://www.hcss.nl/news/mixed-signals-flawed-approach-cyber-deterrence>

Adopting a policy of genuine transparency would have a much-needed stabilising effect by limiting the threat of inadvertent escalation or loss of escalation control. Such a policy should feature multilevel discussions, with varying levels of confidentiality, about strategic cyber capabilities and their command and control, alongside ongoing international discussions on norms of restraint.54 The obvious benefits of this approach explain why the United States’ closest allies and partners have almost unanimously advocated for it. Any covert cyber activities that impair these discussions, rather than advancing them, should remain just that – covert. Otherwise, mixing signals in the cyber domain is a recipe for serious adverse effects that threaten to undermine the security not just of the United States, but of all liberal democracies and of the internet itself.

## Case Answers

### No Cyber Impact---1NC

#### Cyberwar won’t escalate

Erica Longergan & Keren Yarhi-Milo 22, Lonergan is an assistant professor in the Army Cyber Institute at West Point and a research scholar at the Arnold A. Saltzman Institute of War and Peace Studies at Columbia University; Yarhi-Milo is the Arnold A. Saltzman Professor of War and Peace Studies in the political science department and the School of International and Public Affairs, “Cyber Signaling and Nuclear Deterrence: Implications for the Ukraine Crisis,” War on the Rocks, 4/21/22, <https://warontherocks.com/2022/04/cyber-signaling-and-nuclear-deterrence-implications-for-the-ukraine-crisis/>

The Limited Escalation Risks of Cyber Operations

But all of this focus on cyber operations causing nuclear escalation may be misplaced and, more importantly, distract policymakers from the dangers of a more plausible scenario: the use of ambiguous cyber signals during nuclear crises. Specifically, the nature of cyber operations reduces their inherent escalatory potential, particularly when compared to other ways a state could attack an adversary’s nuclear forces or command, control, and communications systems, like a direct counterforce strike or employing anti-satellite weapons. But their misuse as a signaling tool could do more harm than good.

First, successfully conducting cyber operations against strategic targets, like nuclear systems, is harder than the conventional wisdom might suggest. It requires a means of gaining access to a particular system and developing an exploit to cause a desired effect — and then maintaining persistent (and stealthy) access to be able to conduct an offensive operation at the desired time. Moreover, the overall outcome may be unpredictable and net less-than-desirable results.

Second, even if a state is able to conduct these kinds of operations, they typically prefer to do so in secret — and this mitigates some escalation concerns. That’s because, to cause an escalatory response, a state like Russia would have to uncover a cyber operation during a particular time period — such as while the Ukraine conflict is unfolding. For example, Russia would have to detect a cyber operation against a nuclear command and control system to cause Putin to perceive a “window of vulnerability,” perhaps assessing that it is part of a U.S. or NATO counterforce strategy to disable Russia’s ability to retaliate with nuclear weapons. But the likelihood of these circumstances arising is low because — unless a state is trying to signal with a cyber capability — it will try to keep these kinds of sensitive operations secret. Therefore, the chances of such an operation being discovered at a particular time period are relatively small.

Finally, even if, hypothetically, Russia was to discover a cyber operation taking place, the likelihood of it leading to escalation is low. This is due to the virtual nature of cyber “weapons” — they rarely cause destruction in the physical world, let alone permanent damage. For example, even Russia’s 2015 cyber attack against Ukraine’s power grid, an important example of a strategic cyber attack against civilian critical infrastructure, only resulted in service disruptions for a few hours. During the current conflict, Russia-linked actors have so far been stymied in using cyber operations for strategic impact, such as the failed cyber attack by the group Sandworm against Ukraine’s power grid.

Taken together, this reasoning suggests that, in practice, cyber operations may not rise to a level that would cause a state like Russia to actually fear the integrity of its nuclear command, control, and communications systems, creating few reasons to escalate to the level of nuclear employment.

### No Cyber Impact---2NC

#### OCOs won’t escalate

Heine Sørensen 19, Senior Lecturer at the Institute for Strategy at the Royal Danish Defence College, and Dorthe Bach Nyemann, Senior Lecturer at the Institute for Strategy, Royal Danish Defence College, Represented Denmark in the Research Project Entitled “Countering Hybrid Warfare I-II” Within the Framework of the Multinational Capability Development Campaign (MCDC), US Joint Forces Command, “Deterrence by Punishment as a Way of Countering Hybrid Threats – Why We Need To Go ‘Beyond Resilience’ in the Gray Zone”, Multinational Capability Development Campaign, March 2019, https://tinyurl.com/y6cko3at

The Flipside of Deterrence by Punishment – the Fear of Escalation

One of the greatest reservations against communicating a willingness to take punitive actions concerns the risk of escalation and increased tension due to a more assertive or offensive posture. Yet when looking into possible responses – retaliation in cyberspace, for example – a number of “self-dampening” mechanisms appear to be in place that may be applicable to many types of responses.30 One example is the requirement to establish some level of attribution of aggression on which to base a response. As discussed above, while attribution is rarely impossible, it can be a time-consuming and technically-challenging endeavor. In a high-stakes scenario the time taken to get attribution as right as possible means there will be plenty of time to think twice about actions and consequences, and to lean on diplomatic measures in parallel. An example of a self-dampening mechanism related to the cyber domain is the large investment required to develop credible offensive capabilities. Moreover, an offensive cyber capability is a transitory tool31. The ability to access a computer system or network to cause harm or damage is only temporary and dependent on a very rapid and ongoing patching of vulnerabilities. At the same time, wielding the cyber instrument despite the downside of “burning” the capacity might have a de-escalatory effect by communicating capability and credibility to the opponent with a view to discouraging future hostile attacks. Targeting in any domain – including cyberspace – must also follow relevant rules, law and due-process which will self-limit the range of targets and actions available.

A final “escalatory showstopper” is related to the challenge of identifying and developing targets of adequate strategic significance – not too much, not too little – to achieve the desired effect. Responding to hybrid aggression by applying “middle range” punitive actions that are proportionate to the aggression threatened or suffered will also self-limit the escalatory potential. It is unlikely to be in the interest of any hybrid aggressor to pursue an escalatory spiral above and beyond where they were looking to compete in the first place: on the hybrid level. Nevertheless, one way to mitigate the risk of escalation – while enhancing civilian oversight and interagency coordination – would be to establish rules of engagement for punitive actions on the hybrid level32 . This would provide decision-makers with common guidelines to pursue punitive actions that fall below the “use of force threshold”. Moreover, this could actually bolster the credibility of punitive actions by signaling to hybrid aggressors the intent to take pre-prepared punitive actions when deemed necessary: in other words, a “playbook” for countering hybrid threats.

#### High level cyber operations are empirically denied---ample past predictions have never come to pass

Andreas Wenger & Myriam Dunn Cavelty 22, Wenger is professor of international and Swiss security policy at ETH Zurich and director of the Center for Security Studies (CSS), Switzerland; Cavelty is deputy head of research and teaching at the Center for Security Studies (CSS), ETH Zurich, Switzerland, “Conclusion,” Cyber Security Politics, 1st ed., Routledge, 01/18/2022, pp. 239–266 DOI.org (Crossref), doi:10.4324/9781003110224-18

In a world of rapid socio-technical transformation and increasing fragmentation of political power and authority, cyber security has firmly established itself as one of the top national security issues of the 21st century. Managing cyber insecurities will most likely further increase in complexity and political significance in the next decade, co-produced by an acceleration of the ongoing socio-technical transformations, on the one hand, and the changing dynamics of the related political responses, on the other. The first part of the book recorded the ongoing geographic expansion of cyberspace into outer space, anticipated how emerging technologies will increase the interconnectedness of infrastructures and services, and projected how in a context of ever tighter coupled and integrated socio-technical systems cyber threat narratives will inevitably expand to more policy fields at both the national and international levels. The second part of the book discussed how in cyberspace state actors need to find the right balance between restraint and exploitation, why they need to uphold their efforts to control the risk of escalation, and why governments increasingly share responsibility with actors from economy and society.

The current state of cyber security politics is very much a reflection of the interplay between the underlying forces of great power competition and the dynamics of socio-technical and socio-economic globalization processes. From the interplay of these two processes emerge the two key factors – multidimensional uncertainty and socio-political ambiguity – that characterize the current context of cyber security politics at both the national and international levels, as highlighted in Figure 16.1. Multidimensional uncertainty plays a key role in the emergence of cyber insecurity as a wicked problem and shapes – and is shaped by – the ambiguity of cyber security politics.

The ambiguity of cyber security politics encompasses the two dimensions of cyber security outlined in the introductory chapter (Dunn Cavelty and Wenger 2022): First, the international dimension of cyber security politics concentrates on how state actors shape and use cyberspace in accordance with their strategic goals, while at the same time struggling to uphold the stability of their strategic relationships. In Figure 16.1, the interactive search for an acceptable balance between

[FIGURE 16.1 OMITTED]

the strategic utility of and the strategic stability in cyberspace is represented in the upper left (possibilities of (geo)political (mis)use) and lower right (conflictive / cooperative government responses) corners. Second, the broader dimension of cyber security politics focuses on how state, industry, and societies negotiate their respective roles in governing cyberspace, while at the same time competing in the tech innovation process that affects the continued transformation of cyberspace. In Figure 16.1, the interactive search for norms of responsible behavior in an uncertain and ambiguous socio-technical and sociopolitical context is represented in the lower left (fragmented trans-sectoral/transnational governance responses) and upper right (emerging digital technologies) corners.

This concluding chapter, building on the individual contributions to this book, highlights four key debates that together encapsulate the complexities and paradoxes of the current thinking about the future of cyber security politics from a Western perspective. The first section asks how much political influence states can achieve via cyber operations and what context factors condition the (limited) strategic utility of such operations. A second section discusses the role of emerging digital technologies in cyber security politics and notes how the dynamics of the tech innovation process reinforce the fragmentation of the governance space around them. A third section asks how states attempt to uphold stability in cyberspace, and in their strategic relations more general, highlighting three interconnected challenges – escalation, deterrence, and intelligence – of this interactive quest. A fourth and final section focuses on the shared responsibility of state, economy, and society for cyber security and calls attention to the continuing renegotiation processes about their respective roles in an increasingly trans-sectoral and transnational governance space.

The strategic utility of cyber operations

The debate about the strategic utility of cyber operations arises in a context characterized by the interplay between the rapid emergence of new digital technologies and the politics of their use and misuse. Over time, the debate evolved considerably, as cyber security issues transformed from a technical risk management issue discussed by a limited circle of experts into a key challenge of national security debated at the highest level of governments (Dunn Cavelty 2008; Dewar 2018). In its early stages, the debate focused on “doomsday” cyberattack scenarios that centered on the strategic exploitation of increasingly interconnected and vulnerable infrastructures (Clarke and Knake 2010). As out-of-the-blue cyber war failed to make its expected appearance, experts began to shift their attention to the political and strategic implications of low-level cyber conflict (Baezner 2018; see also Rid 2012; Lindsay 2014/15), on the one hand, and to the increase of computer network attack campaigns linked to covert state involvement (Dunn Cavelty 2015), on the other.

At the current point in time in the history of cyber security politics the empirical picture is characterized by “dogs that did not bark” at the high end of conflict and persistent cyber operations and instability at the low end of conflict (Schulze 2020; Harknett and Smeets 2020; Lupovici 2021). Within this context, the chapters in this volume point to three interconnected aspects of the enduring debate about the strategic utility of cyber operations: A first subsection concentrates on the difficulty of achieving a controlled strategic effect under multidimensional uncertainty. The focus here is on explaining why most cyber operations so far seem not very escalatory and appear unlikely to result in visible changes in the existing balance of power between great powers. A second subsection focuses on the utility of cyber operations as a tool of subversion and mild sabotage. Here the focus is on understanding how the ambiguity of involved actors and the opaqueness of cyber operations can be manipulated in specific strategic contexts by some powers for asymmetric influence. A third subsection deals with the assumed asymmetrical vulnerability of democracies to disinformation as the latest cyber threat focus in Western (security) politics. Here the debate centers on the question if a strategic effect can be achieved via cyber influence operations that aim at undermining social cohesion and trust in democratic political institutions.

#### Gray zone cyber conflict won’t escalate

Andreas Wenger & Myriam Dunn Cavelty 22, Wenger is professor of international and Swiss security policy at ETH Zurich and director of the Center for Security Studies (CSS), Switzerland; Cavelty is deputy head of research and teaching at the Center for Security Studies (CSS), ETH Zurich, Switzerland, “Conclusion,” Cyber Security Politics, 1st ed., Routledge, 01/18/2022, pp. 239–266 DOI.org (Crossref), doi:10.4324/9781003110224-18

The power to subvert: manipulating “gray zones” while minimizing the risk of escalation

Most cyber operations take place below the threshold of war, Marie Baezner and Sean Cordey (2022) note in their chapter. Mapping the practical use of such operations in a series of cyber conflict case studies, they confirm that especially influence operations fall into a zone which goes beyond conventional diplomacy and stops short of conventional war, which Lucas Kello describes as “unpeace” (Kello 2017). Taking this empirical puzzle as a starting point for their analysis, the chapter asks why some actors see such operations as attractive and efficient tools of power projection and influence. The (limited) strategic utility of cyber (influence) operations, the two authors conclude, depends on the characteristics of the strategic context and the operational environment in which they are employed and on the nature of the strategic actor employing such operations.

At a strategic level, the increasingly pervasive use of cyber (influence) operations in international affairs reflects the current dynamics of great power competition. Together, the increasing costs of conventional war and the realities of economic interdependence create incentives, especially for great powers, to gain asymmetric influence through cyber operations, in particular in their spheres of interest, without however unduly undermining the strategic stability of great power relations. At an operational level, the use of cyber influence operations reflects an operational environment that is characterized by legal ambiguity and political contestation, opacity of the parties involved and blurred boundaries between the private and public domains. Referring to the concept of and literature on “gray zones”, Baezner and Cordey argue that revisionist powers use cyber operations as tools to operate below the threshold of armed combat to gain an asymmetric advantage in their relationship with other political actors, especially in view of the global (military) dominance of the United States.

Based on a series of case studies, Baezner and Cordey note that the following operational assumptions about cyber (influence) operations seem to make them attractive tools for many to intervene in gray zone conflicts. First, the majority of the cyber technologies used in such contexts are widely available at relatively low cost. Patriotic hackers or opaque criminal groups with ties to domestic or foreign elites use them opportunistically for disruption and mild sabotage rather than for destruction. Second, cyber espionage and influence operations are increasingly used to influence the information environment of a conflict and gain an asymmetric advantage. They work in tandem with a wider set of economic, political, and military coercive tools. Third, the legal uncertainty surrounding intelligence operations allows state actors to avoid formal condemnation and uphold a posture of plausible deniability. The opaqueness of actors and operations makes it unlikely that a verdict of attribution would be as transparent and credible as to justify a military response.

#### It doesn’t spill out to cross-domain kinetic force AND is limited to just stop intrusions

Erica D. Borghard 19, Assistant Professor in the Army Cyber Institute at the United States Military Academy at West Point, and Shawn W. Lonergan, Assistant Professor of International Relations in the Department of Social Science at USMA, “Cyber Operations as Imperfect Tools of Escalation”, Strategic Studies Quarterly, Fall 2019, p. 123-124

However, there are important empirical reasons to suspect that the risks of cyber escalation may be exaggerated. Specifically, if cyberspace is in fact an environment that (perhaps even more so than others) generates severe escalation risks, why has cyber escalation not yet occurred? Most interactions between cyber rivals have been characterized by limited volleys that have not escalated beyond nuisance levels and have been largely contained below the use-of-force threshold.5 For example, in a survey of cyber incidents and responses between 2000 and 2014, Brandon Valeriano et al. find that “rivals tend to respond only to lower-level [cyber] incidents and the response tends to check the intrusion as opposed to seek escalation dominance. The majority of cyber escalation episodes are at a low severity threshold and are non-escalatory. These incidents are usually ‘tit-for- tat’ type responses within one step of the original incident.”6 Even in the two rare examples in which states employed kinetic force in response to adversary cyber operations—the US counter-ISIL drone campaign in 2015 and Israel’s airstrike against Hamas cyber operatives in 2019—the use of force was circumscribed and did not escalate the overall conflict (not to mention that force was used against nonstate adversaries with limited potential to meaningfully escalate in response to US or Israeli force).7

We posit that cyber escalation has not occurred because cyber operations are poor tools of escalation. In particular, we argue that this stems from key characteristics of offensive cyber capabilities that limit escalation through four mechanisms. First, retaliatory offensive cyber operations may not exist at the desired time of employment. Second, even under conditions where they may exist, their effects are uncertain and often relatively limited. Third, several attributes of offensive cyber operations generate important tradeoffs for decision-makers that may make them hesitant to employ capabilities in some circumstances. Finally, the alternative of cross-domain escalation—responding to a cyber incident with noncyber, kinetic instruments—is unlikely to be chosen except under rare circumstances, given the limited cost-generation potential of offensive cyber operations. In this article, we define cyber escalation and then explore the implications of the technical features and requirements for offensive cyber operations. We also consider potential alternative or critical responses to each of these logics. Finally, we evaluate the implications for US policy making.

#### **It’s empirically proven**

Dr. Christian Leuprecht 19, Class of 1965 Professor in Leadership, Department of Political Science, Royal Military College and Adjunct Research Professor at Charles Sturt University; Ph.D, Queen’s, Joseph Szeman (an undergraduate student in Political Studies and History in his 4th year at Queen’s University), David Skillicorn (Professor in the School of Computing at Queen’s University, and Adjunct Professor at the Royal Military College of Canada), March 2019, “The Damoclean Sword of Offensive Cyber: Policy Uncertainty and Collective Insecurity”, Contemporary Security Policy

To date, no direct use of OCO capabilities has resulted in the outbreak of traditional conflict, perhaps owing to uncertainties in the novelty of the attacks, the difficulty of attribution, and the reluctance of national cyber actors to retaliate when the path of escalation is unclear (Rid & Buchanan, 2015). Most importantly, however, the actions of armed forces in democratic countries are constrained by the rule of law, which translates into multiple authorities to ensure responsible and acceptable use, and safeguard against escalation. The fine-grained control of OCOs compared to conventional military force provides a way to manage escalation without the direct use of physical or military assets, whose effect in sparking conflict is much better known. In other words, instead of reacting to an escalating conflict by deploying physical military assets to a region, an OCO can be employed covertly to incur more controllable costs on the adversary, with the benefit of plausible deniability (Hare, 2018). Depending on the type of OCO employed, if there is a reduction in tension, the effects of the OCO can be reversed or scaled back.

### No Cyber Impact---AT: OCOs Different

#### OCOs are stabilizing---their evidence is Russian propaganda

James A. Lewis 15, Director and Senior Fellow, Strategic Technologies Program, Center for Strategic and International Studies, "THE ROLE OF OFFENSIVE CYBER OPERATIONS IN NATO’S COLLECTIVE DEFENCE", Tallin Paper No. 8, A NATO CCDCOE Publication on Strategic Cyber Security, https://www.ccdcoe.org/uploads/2018/10/TP\_08\_2015\_0.pdf

Stabilising or Not

Dissimulation is an essential part of hybrid warfare, and Europe and the US face a propaganda barrage that is much more sophisticated than the clumsy Soviet efforts of the Cold War. Despite this clumsiness, a good portion of the Western public has found it persuasive. Similarly, those critical of NATO will find new complaints about aggression and militarisation credible. Russia has already complained that NATO’s defensive cyber doctrine is destabilising warmongering and part of a larger conspiracy to advance western hegemony.11 The Snowden revelations have lent a powerful impetus to Russian propaganda.

Behind the rhetoric lies both a desire to conceal their own use of cyber operations and a real fear that Russia’s decline leaves it vulnerable to new military technologies. The intent is to hamper and complicate any Western response to Russian efforts to regain control in Crimea and the “near abroad”. The Russian position is that NATO’s new cyber doctrine is destabilising as it threatens to use conventional or even nuclear responses (in the Russian description of the new policy towards low-level cyber attacks).

Any announcement by NATO relating to offensive cyber capabilities would be greeted with alarm and vitriol in Moscow. However, the effect on stability would likely be less pronounced. NATO-Russia relations are already in steep decline. It is possible that any NATO announcement would accelerate this, but it is also possible that Russia could recalculate the risk of further adventures if it were faced with a stronger defence. In terms of opponent attitudes, there is probably little effect. Russia, along with NATO’s other potential military opponents, is likely to overestimate both capabilities and coordination among NATO member states and underestimate NATO’s will to defend. This is an unhappy combination as it makes aggression against NATO seem less risky.

NATO’s decision on how cyber attacks could trigger Article 5, while greeted with complaints, had a stabilising effect. It made clear to potential opponents that cyber attacks are not risk-free. Similarly, a clear enunciation of how NATO would use offensive cyber capabilities as part of any defensive operation would also change opponents’ risk calculations in ways that would force them to consider how offensive actions, even if intended to be covert, are not free of risk or cost.

### No Russian Cyber---1NC

#### Russia won’t launch catastrophic cyber attacks

James Andrew Lewis 20, Senior Vice President and Director of the Technology Policy Program at the Center for Strategic and International Studies, “Dismissing Cyber Catastrophe”, Center for Strategic and International Studies, 8/17/2020, https://www.csis.org/analysis/dismissing-cyber-catastrophe

A catastrophic cyberattack was first predicted in the mid-1990s. Since then, predictions of a catastrophe have appeared regularly and have entered the popular consciousness. As a trope, a cyber catastrophe captures our imagination, but as analysis, it remains entirely imaginary and is of dubious value as a basis for policymaking. There has never been a catastrophic cyberattack.

To qualify as a catastrophe, an event must produce damaging mass effect, including casualties and destruction. The fires that swept across California last summer were a catastrophe. Covid-19 has been a catastrophe, especially in countries with inadequate responses. With man-made actions, however, a catastrophe is harder to produce than it may seem, and for cyberattacks a catastrophe requires organizational and technical skills most actors still do not possess. It requires planning, reconnaissance to find vulnerabilities, and then acquiring or building attack tools—things that require resources and experience. To achieve mass effect, either a few central targets (like an electrical grid) need to be hit or multiple targets would have to be hit simultaneously (as is the case with urban water systems), something that is itself an operational challenge.

It is easier to imagine a catastrophe than to produce it. The 2003 East Coast blackout is the archetype for an attack on the U.S. electrical grid. No one died in this blackout, and services were restored in a few days. As electric production is digitized, vulnerability increases, but many electrical companies have made cybersecurity a priority. Similarly, at water treatment plants, the chemicals used to purify water are controlled in ways that make mass releases difficult. In any case, it would take a massive amount of chemicals to poison large rivers or lakes, more than most companies keep on hand, and any release would quickly be diluted.

More importantly, there are powerful strategic constraints on those who have the ability to launch catastrophe attacks. We have more than two decades of experience with the use of cyber techniques and operations for coercive and criminal purposes and have a clear understanding of motives, capabilities, and intentions. We can be guided by the methods of the Strategic Bombing Survey, which used interviews and observation (rather than hypotheses) to determine effect. These methods apply equally to cyberattacks. The conclusions we can draw from this are:

* Nonstate actors and most states lack the capability to launch attacks that cause physical damage at any level, much less a catastrophe. There have been regular predictions every year for over a decade that nonstate actors will acquire these high-end cyber capabilities in two or three years in what has become a cycle of repetition. The monetary return is negligible, which dissuades the skilled cybercriminals (mostly Russian speaking) who might have the necessary skills. One mystery is why these groups have not been used as mercenaries, and this may reflect either a degree of control by the Russian state (if it has forbidden mercenary acts) or a degree of caution by criminals.
* There is enough uncertainty among potential attackers about the United States’ ability to attribute that they are unwilling to risk massive retaliation in response to a catastrophic attack. (They are perfectly willing to take the risk of attribution for espionage and coercive cyber actions.)
* No one has ever died from a cyberattack, and only a handful of these attacks have produced physical damage. A cyberattack is not a nuclear weapon, and it is intellectually lazy to equate them to nuclear weapons. Using a tactical nuclear weapon against an urban center would produce several hundred thousand casualties, while a strategic nuclear exchange would cause tens of millions of casualties and immense physical destruction. These are catastrophes that some hack cannot duplicate. The shadow of nuclear war distorts discussion of cyber warfare.
* State use of cyber operations is consistent with their broad national strategies and interests. Their primary emphasis is on espionage and political coercion. The United States has opponents and is in conflict with them, but they have no interest in launching a catastrophic cyberattack since it would certainly produce an equally catastrophic retaliation. Their goal is to stay below the “use-of-force” threshold and undertake damaging cyber actions against the United States, not start a war.

This has implications for the discussion of inadvertent escalation, something that has also never occurred. The concern over escalation deserves a longer discussion, as there are both technological and strategic constraints that shape and limit risk in cyber operations, and the absence of inadvertent escalation suggests a high degree of control for cyber capabilities by advanced states. Attackers, particularly among the United States’ major opponents for whom cyber is just one of the tools for confrontation, seek to avoid actions that could trigger escalation.

The United States has two opponents (China and Russia) who are capable of damaging cyberattacks. Russia has demonstrated its attack skills on the Ukrainian power grid, but neither Russia nor China would be well served by a similar attack on the United States. Iran is improving and may reach the point where it could use cyberattacks to cause major damage, but it would only do so when it has decided to engage in a major armed conflict with the United States. Iran might attack targets outside the United States and its allies with less risk and continues to experiment with cyberattacks against Israeli critical infrastructure. North Korea has not yet developed this kind of capability.

One major failing of catastrophe scenarios is that they discount the robustness and resilience of modern economies. These economies present multiple targets and configurations; they are harder to damage through cyberattack than they look, given the growing (albeit incomplete) attention to cybersecurity; and experience shows that people compensate for damage and quickly repair or rebuild. This was one of the counterintuitive lessons of the Strategic Bombing Survey. Pre-war planning assumed that civilian morale and production would crumple under aerial bombardment. In fact, the opposite occurred. Resistance hardened and production was restored.1

This is a short overview of why catastrophe is unlikely. Several longer CSIS reports go into the reasons in some detail. Past performance may not necessarily predict the future, but after 25 years without a single catastrophic cyberattack, we should invoke the concept cautiously, if at all. Why then, it is raised so often?

### No Russian Cyber---2NC

#### No Russian cyber:

#### They spy and coerce, but won’t launch catastrophic attacks because they know it’d be attributed and there’d be massive retal. Empirics prove high degree of control prevents inadvertent escalation and even if, there’s no impact due to hardening and resiliency---that’s Lewis

#### Everything is small, designed to avoid miscalc

Marie Baezner 17 and Patrice Robin, Cyber Defense Project (CDP) Center for Security Studies (CSS), ETH Zürich, “Cyber-Conflict Between the United States of America and Russia” https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/184547/Cyber-Reports-2017-02.pdf?sequence=1

On the other hand, both states might not desire further escalation, preferring to restrain the conflict to cyberspace. Each would follow the “tit-for-tat” logic and accuse each other while never reaching a tipping point where the conflict spills over to a conventional war. Such a tipping point would be linked to the intensity of the attack or the nature of the targets. Both nations would keep the cyberattacks small enough not to trigger a bigger reaction. The same would be observed on the choice of targets, with both avoiding certain critical or sensitive targets, for instance critical infrastructures. In order to contain the conflict in cyberspace, both states would have to demonstrate their restraint by selecting options with low risk of miscalculation (Lin, 2012, pp. 64–66). In the future, it might also be possible to see a deescalation in the form of the emergence of an international treaty or at least further bilateral treaties between the USA and Russia on cyberattacks. For example, during the last few years, businesses in the USA were often hacked and spied on by the Chinese military. These intrusions were mostly cyber-economic-espionage and were said to have supported the theft of billions of dollars’ worth of intellectual property (Bamford, 2016). In September 2015, the USA and China signed an agreement engaging both countries not to support or conduct cyber-theft of intellectual property. Moreover, the parties have made the commitment not to use cyberattacks against each other’s critical infrastructures in peace-time and to support the establishment of international behavioral norms in cyberspace (Rosenfeld, 2015). Both states also highlighted the fact that they could not control each individual in their country and therefore could not be held responsible for individual acts. Since then it seems that the number of attacks on commercial targets has diminished (Timm, 2016). Former President Obama suggested the creation of a position of cybersecurity ambassador to deal with bilateral or multilateral treaties concerning cyber-norms (Lee, 2016). For this kind of de-escalation to take effect, the termination of the conflict at hand must be the stated aim of both parties. A clear common understanding of the terms of agreement is required and must be based on trust-building efforts, as well as the assurance of mutual adherence. The difficulty of tracking the implementation of such agreements in cyberspace has been an obstacle preventing more states consenting to such solutions (Lin, 2012, pp. 62–64). Nevertheless, a dialogue on cyberspace already exists between the USA and Russia since July 2013. This cooperation includes Confidence Building Measures (CBM) such as the creation of working groups on the issue of ICT security, exchange of information between the two national Computer Emergency Response Teams (CERT), and the creation of a direct communication line to directly manage ICT incidents (Segal, 2016; The White House, Office of the Press Secretary, 2013). In October 2016, former President Obama used the latter to inform Russian President Putin that the USA was accusing Russia of interference in the election process (Ignatius, 2016). Furthermore, Russia and the USA take part in the UN GGE supporting the future establishment of international norms on actions in cyberspace. They stated that international law can be applied in cyberspace and therefore, the rules of proportionality and limited collateral damage should also be respected in cyberattacks (Ignatius, 2016; United Nations General Assembly, 2015). These examples demonstrate that even though the two states are involved in a “tit-for-tat” logic in their relations on a tactical level, there was still a dialogue on the strategic level, at least until 2015. The recent cyberattacks in USA and the election of Donald Trump as US President, bring new uncertainties.

#### They have zero interest in producing widespread damage

Dr. James Andrew Lewis 18, Senior Vice President at the Center for Strategic and International Studies, Ph.D. from the University of Chicago, January 2018, “Rethinking Cybersecurity: Strategy, Mass Effect, and States,” <https://tinyurl.com/y27xcqbb>, p. 7-11

Similarly, the popular idea that opponents use cyber techniques to inflict cumulative economic harm is not supported by evidence. Economic warfare has always been part of conflict, but there are no examples of a country seeking to imperceptibly harm the economy of an opponent. The United States engaged in economic warfare during the Cold War, and still uses sanctions as a tool of foreign power, but few if any other nations do the same. The intent of cyber espionage is to gain market or technological advantage. Coercive actions against government agencies or companies are intended to intimidate. Terrorists do not seek to inflict economic damage. The difficulty of wreaking real harm on large, interconnected economies is usually ignored.

Economic warfare in cyberspace is ascribed to China, but China's cyber doctrine has three elements: control of cyberspace to preserve party rule and political stability, espionage (both commercial and military), and preparation for disruptive acts to damage an opponent's weapons, military information systems, and command and control. "Strategic" uses, such as striking civilian infrastructure in the opponent's homeland, appear to be a lower priority and are an adjunct to nuclear strikes as part of China's strategic deterrence. Chinese officials seem more concerned about accelerating China's growth rather than some long-term effort to undermine the American economy.6 The 2015 agreement with the United States served Chinese interests by centralizing tasking authority in Beijing and ending People's Liberation Army (PLA) "freelancing" against commercial targets.

The Russians specialize in coercion, financial crime, and creating harmful cognitive effect—the ability to manipulate emotions and decisionmaking. Under their 2010 military doctrine on disruptive information operations (part of what they call "New Generation Warfare"). Russians want confusion, not physical damage. Iran and North Korea use cyber actions against American banks or entertainment companies like Sony or the Sands Casino, but their goal is political coercion, not destruction.

None of these countries talk about death by 1000 cuts or attacking critical infrastructure to produce a cyber Pearl Harbor or any of the other scenarios that dominate the media. The few disruptive attacks on critical infrastructure have focused almost exclusively on the energy sector. Major financial institutions face a high degree of risk but in most cases, the attackers' intent is to extract money. There have been cases of service disruption and data erasure, but these have been limited in scope. Denial-of-service attacks against banks impede services and may be costly to the targeted bank, but do not have a major effect on the national economy. In all of these actions, there is a line that countries have been unwilling to cross.

When our opponents decided to challenge American "hegemony," they developed strategies to circumvent the risks of retaliation or escalation by ensuring that their actions stayed below the use-of-force threshold—an imprecise threshold, roughly defined by international law, but usually considered to involve actions that produce destruction or casualties. Almost all cyber attacks fall below this threshold, including, crime, espionage, and politically coercive acts. This explains why the decades-long quest to rebuild Cold War deterrence in cyberspace has been fruitless.

It also explains why we have not seen the dreaded cyber Pearl Harbor or other predicted catastrophes. Opponents are keenly aware that launching catastrophe brings with it immense risk of receiving catastrophe in return. States are the only actors who can carry out catastrophic cyber attacks and they are very unlikely to do so in a strategic environment that seeks to gain advantage without engaging in armed conflict. Decisions on targets and attack make sense only when embedded in their larger strategic calculations regarding how best to fight with the United States.

There have been thousands of incidents of cybercrime and cyber espionage, but only a handful of true attacks, where the intent was not to extract information or money, but to disrupt and, in a few cases, destroy. From these incidents, we can extract a more accurate picture of risk. The salient incidents are the cyber operations against Iran's nuclear weapons facility (Stuxnet), Iran's actions against Aramco and leading American banks, North Korean interference with Sony and with South Korean banks and television stations, and Russian actions against Estonia, Ukrainian power facilities, Canal 5 (television network in France), and the 2016 U S. presidential elections. Cyber attacks are not random. All of these incidents have been part of larger geopolitical conflicts involving Iran, Korea, and the Ukraine, or Russia's contest with the United States and NATO.

There are commonalities in each attack. All were undertaken by state actors or proxy forces to achieve the attacking state's policy objectives. Only two caused tangible damage; the rest created coercive effect, intended to create confusion and psychological pressure through fear, uncertainty, and embarrassment. In no instance were there deaths or casualties. In two decades of cyber attacks, there has never been a single casualty. This alone should give pause to the doomsayers. Nor has there been widespread collateral damage.

### No Russian Cyber---AT: Ukraine

#### They’re not using cyberattacks in Ukraine

Jason Blessing 22, Ph.D., is a Jeane Kirkpatrick Visiting Research Fellow with the foreign and defense policy department at the American Enterprise Institute, “Where is Russia’s cyber blitzkrieg?,” The Hill, 3/9/22, <https://thehill.com/opinion/cybersecurity/597272-where-is-russias-cyber-blitzkrieg/>

Fighting in Ukraine continues but the much-anticipated Russian cyber blitzkrieg hasn’t occurred. Russian forces have failed to deploy devastating cyber attacks in the opening salvo, despite ample opportunity to cripple Ukrainian networks. Where is the dramatic, game-changing cyber war we were promised? Pundits are scrambling for explanations. Spoiler alert: Cyber isn’t a magic wand to wave and gain battlefield superiority. Cyber attacks are rarely decisive on their own, and they don’t exist in a vacuum. Strategic context is critical for unpacking the use of cyber operations, and Russia’s invasion strategy undeniably has shaped and restricted its menu of cyber options.

First, the Kremlin’s goal of regime change in Kyiv means that Russian cyber operations are subject to the “you break it, you buy it” rule. If your plan is to install a puppet government, the last thing you want to do is obliterate Ukraine’s communications networks and other critical infrastructure. Life would be miserable for any regime trying to manage a population with no electricity or water. Now add an extra layer of Ukrainian outrage against a Russian lackey whom they likely would violently oppose. As a result, the Russians have launched limited attacks to temporarily disrupt public services. This has included website vandalism, overloading government servers with traffic, and using malware to wipe data from banking networks.

Putin’s overconfidence in a swift and overwhelming victory is another reason for the lack of cyber-induced damage. In thinking that this would be a quick smash-and-grab, the Kremlin de facto shelved what could have been its most powerful cyber capabilities. High-impact cyber attacks require immense resources, planning time, and operational control so that they hit their mark and aren’t discovered before pulling the trigger. Meeting these conditions is extremely hard, and it’s not worth the effort if you expect a quick win. Disruption therefore takes a backseat to intelligence collection. While tracking targets on Ukrainian networks is valuable, taking them offline is counterproductive. Putin’s months-long military buildup gave time to plan for high-end cyber warfare. That we haven’t seen it is a testament to false assumptions of quick victory and an underestimation of Ukrainian cyber defense.

Finally, the Russian military’s poor planning and execution in the early stages of invasion cast doubt on its ability to truly integrate cyber with conventional operations in combat. As I’ve written, this is a challenge for many militaries. It is particularly true for Russia, where the military and intelligence cyber-ecosystem is crowded with units that constantly compete and lack coordination. But incorporating cyber effects into kinetic operations is even harder for a military whose soldiers don’t know where they are or why they’re deployed. Their reliance on civilian radios and mobile phones for communication doesn’t inspire much confidence either.

The Russians clearly excel in cyber espionage: By hacking one company (SolarWinds) and corrupting a single software product, Russian cyber operators gained access to several Fortune 500 companies and U.S. government agencies. However, given the lack of impact in the past and current logistical struggles, we should temper our expectations about Russian cyber prowess in wartime.

The Kremlin hasn’t gotten the military knockout blow it wanted, and missed its window of opportunity. Cyber operations would not have been decisive. But they could have enabled a first-mover advantage by taking out Ukraine’s digital eyes and ears, including the ability to receive and integrate intelligence shared by NATO. This is not to say that cyber has no role to play moving forward; quite the opposite. The longer the war lasts, the greater likelihood that Russian forces will test out new tools on Ukrainian networks. Such activity can manifest as increased intelligence collection or the use of cyber capabilities at the tactical level to produce limited, localized effects. Both could contribute to the lethality of Russia’s conventional strikes. For example, tactical cyber attacks could facilitate a ground unit’s ability to secure or destroy a target by briefly disrupting specific networks within the given area of operation.

### No Russian Cyber---Nuclear Deterrence---1NC

#### ‘Deterrence’ is about NC3 hacking---that’s nonsense

Dr. Andrew Futter 16, Associate Professor of International Politics and Director of Research for Politics and International Relations at the University of Leicester, “War Games Redux? Cyberthreats, US–Russian Strategic Stability, and New Challenges for Nuclear Security and Arms Control”, European Security, Volume 25, Issue 2, p. 171-172

It is of course highly unlikely that either the USA or Russia has plans – or perhaps more importantly, the desire – to fully undermine the other’s nuclear command and control systems as a precursor to some type of disarming first strike, but the perception that nuclear forces and associated systems could be vulnerable or compromised is persuasive. Or as Hayes (2015) puts it, “The risks of cyber disablement entering into our nuclear forces are real”. While the growing possibility of “cyber disablement” should not be overstated (notions of a “cyber-Pearl Harbor” (Panetta 2012) or “cyber 9–11” (Charles 2013) have done little to help understand the nature of the challenge), cyberthreats are nevertheless an increasingly important component of the contemporary US–Russia strategic context. This is particularly the case when they are combined with other emerging military-technical developments and programmes. The net result, especially given the current downturn in US–Russian strategic relations, and the way cyber is exacerbating the impact of other problematic strategic dynamics, is that is seems highly unlikely that either the USA or Russia will make the requisite moves to de-alert nuclear forces that the new cyber challenges appear to necessitate, or for that matter to (re)embrace the “deep nuclear cuts” agenda any time soon.

Assessing the options for arms control and enhancing mutual security

Given the new challenges presented by cyber to both US and Russian nuclear forces and to US–Russia strategic stability, it is important to consider what might be done to help mitigate and guard against these threats, and thereby help minimise the risks of unintentional launches, miscalculation, and accidents, and perhaps create the conditions for greater stability, de-alerting, and further nuclear cuts. While there is unlikely to be a panacea or “magic bullet” that will reduce the risk of cyberattacks on US and Russian nuclear forces to zero – be they designed to launch nuclear weapons or compromise the systems that support them – there are a number of options that might be considered and pursued in order to address these different types of threats and vulnerabilities. None, of these however, will be easy.

The most obvious and immediate priority for both the USA and Russia is working (potentially together) to harden and better protect nuclear systems against possible cyberattack, intrusion, or cyber-induced accidents. In fact, in October 2013 it was announced that Russian nuclear command and control networks would be protected against cyber incursion and attacks by “special units” of the Strategic Missile Forces (Russia Today 2014). Other measures will include better network defences and firewalls, more sophisticated cryptographic codes, upgraded and better protected communications systems (including cables), extra redundancy, and better training and screening for the practitioners that operate these systems (see Ullman 2015). However, and while comprehensive reviews are underway to assess the vulnerabilities of current US and Russian nuclear systems to cyberattacks, it may well be that US and Russian C2 infrastructure becomes more vulnerable to cyber as it is modernised and old analogue systems are replaced with increasingly hi-tech digital platforms. As a result, and while nuclear weapons and command and control infrastructure are likely to be the best protected of all computer systems, and “air gapped”14 from the wider Internet – this does not mean they are invulnerable or will continue to be secure in the future, particularly as systems are modernised or become more complex (Fritz 2009). Or as Peggy Morse, ICBM systems director at Boeing, put it, “while its old it’s very secure” (quoted in Reed 2012).

#### Alt causes---Klare says China, Iran, and North Korea will do it AND target the U.S., not NATO

#### Deterrence is strong and resilient---the only threats are alt causes

C. Todd Lopez 20, Reporter at DOD News, “U.S. Seeks to Maintain Credible Nuclear Deterrent”, DOD News, 3/3/2020, https://www.defense.gov/Explore/News/Article/Article/2101067/us-seeks-to-maintain-credible-nuclear-deterrent/

The United States maintains a robust nuclear arsenal that consists of ground-based, air-launched and sea-launched weapons. Together, it's commonly called the "nuclear triad," and it remains the centerpiece of the U.S. nuclear deterrent. The triad is fast approaching the end of its service life and must quickly be replaced before it's lost.

Victorino G. Mercado, currently performing the duties of the assistant secretary of defense for strategy, plans and capabilities testified today before the House Armed Services Committee, subcommittee on strategic forces. He told lawmakers that efforts to replace the triad are not part of an arms race.

"The U.S. seeks only what it needs to maintain a credible nuclear deterrent," he said. "In contrast to Russia, who maintains about 2,000 non-strategic nuclear weapons and are pursuing and fielding other novel nuclear capabilities, we have no desire or intent to engage in an arms race nor match weapon-for-weapon the capabilities being fielded by Russia."

The DOD's fiscal year 2021 budget request for nuclear forces, Mercado said, is $28.9 billion, or 4.1% of the total DOD request. The funding request to modernize the existing triad is about 1.7% of the budget request, he added. "The nation’s nuclear modernization program is affordable," he said.

Mercado said that after decades of deferred recapitalization of the nuclear triad, the U.S. must move ahead with modernizing its nuclear forces. Additionally, as defined in the Nuclear Posture Review, the U.S. must also pursue additional flexibility with systems like the sea-launched cruise missile, he said, "to ensure that there are no gains to be made through the use of any nuclear weapon, strategic or otherwise."

### No Grid Impact---1NC

#### Cyber attacks won’t take down the grid

Victoria Craig 16, Analyst at Fox Business, Citing the Senior Manager of Industrial Control Systems at Mandiant, “The U.S. Power Grid is 'Vulnerable,' But Don't Panic Just Yet”, http://www.foxbusiness.com/features/2016/02/02/u-s-power-grid-is-vulnerable-but-dont-panic-just-yet.html

The idea of the nation's power grids becoming the next battleground for cyber warriors could make hacking into consumers’ credit card accounts and personal information seem like child’s play. While U.S. power companies are likely targeted by foreign governments and others in increasingly sophisticated breaches, actually shutting off the lights and causing chaos is far more complicated than many pundits make it seem. Dan Scali, senior manager of industrial control systems at Mandiant, a cybersecurity consulting arm of FireEye ([FEYE](http://www.foxbusiness.com/quote.html?stockTicker=FEYE)), explained that while cyber criminals may gain access to power and utility data systems, it doesn’t necessarily mean the result will be a power outage and a total takedown of power grid control systems. In other words, the power grid is controlled by more than just a panel of digital buttons. “Losing the control system is bad from the perspective that it takes you out of your normal mode of operations of being able to control everything from one command center, but it doesn’t mean you’ve lost control or all the lights go out [in the city],” Scali explained. While many of the systems have been modernized to include digitized control panels, if a hacker were to infiltrate the system, a utility worker could still have the ability to manually control the machines by flipping a switch, pushing a button, or tripping a breaker. As the world saw with the recent attack in Ukraine, which caused a blackout for 80,000 customers of the nation’s western utility, the biggest problem may be ensuring the power grid’s control systems are not vulnerable to cyber break ins. The January attack in Ukraine was likely caused by a corrupted Microsoft Word attachment that allowed remote control over the computer, according to the U.S. Department of Homeland Security. Scali said there was no evidence from the incident in Ukraine that the hacker’s malware was able to physically shut down the power. “It wiped out machines, deleted all the files. Kill disk malware made it impossible to remotely control things. It caused chaos on the business network, and the area where control system operations sat. But the attacker, we believe, would have had to actually used the control system to cause load shedding, which caused the power to go out, or trip breakers to cause the actual problem. Malware itself didn’t turn the power out,” Scali said. He said what most likely happened in that incident was the hacker stole user credentials and logged into the system remotely. The bottom line: Yes, a similar event could happen in the U.S. And corporate America is concerned. A recent survey released in January on the state of information security, conducted by consulting firm Pricewaterhouse Coopers, showed cybersecurity as one of the biggest concerns among the top brass at U.S. power and utilities firms. Part of the problem, Brad Bauch, security and cyber sector leader at PwC said, is the interconnectedness of the industry’s tools. “Utilities want to be able to get information out of [their] systems to more efficiently operate them, and also share that information with customers so they have more real-time information into their usage,” he explained. While allowing access to their own consumption data allows the companies to give their customers more of what they want, it also opens up a host of access points for hackers, making the systems more vulnerable than they otherwise would be. But to say that the power grid is susceptible to cyber hackers is a bit of an oversimplification.

### No Grid Impact---No Cyber Threat---2NC

#### Russia won’t target the grid AND attacks would fail

Paul Wagenseil 19, Senior Editor of Security and Privacy at Tom’s Guide, Citing Selena Larson, Intelligence Analyst at Dragos Cybersecurity Firm, “Hackers Can't Cause Crippling Blackouts, Expert Says”, Tom’s Guide, 3/11/2019, https://www.tomsguide.com/us/blackout-hack-threat-rsa2019,news-29594.html

Don't believe the hype. Hackers cannot easily take down the North American electrical grid to cause massive blackouts, despite numerous news stories, magazine articles and books claiming that they can, a cybersecurity expert told the last week's RSA Conference.

"There are lots of misunderstandings about threats to the electric grid," said Selena Larson, an intelligence analyst at Maryland cybersecurity firm Dragos and a former CNN reporter. "The reality is that a destructive incident at one site would require highly tailored [malware] tools and operations, and would not effectively scale."

That's because U.S. power plants use different makes and models of hardware and software, are often at least partly isolated from the internet and from each other, and have already undergone a fair degree of hardening against cyberattacks. There's very little chance that a single hacker or group of hackers could knock out the power across a large swath of North America at once.

Scary headlines

Those inconvenient facts haven't prevented journalists and writers from penning what Larson deemed needlessly alarming stories. One July 2018 opinion piece in The New York Times entitled "To Hackers, We're Bambi in the Woods" began with a nightmare scenario of an America thrown back to the Stone Age by a cyberattack that kills the power, stops the trains, empties bank accounts and opens literal floodgates.

Later that same month, The Wall Street Journal ran a story called "Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say," lending credence to the nightmare scenario. But it was incorrectly reported — it was based on old information that had been revisited in a DHS presentation.

Larson didn't mention "Lights Out: A Cyberattack, A Nation Unprepared, Surviving the Aftermath," a best-selling 2015 book by former ABC News anchor Ted Koppel.

"A well-designed attack on just one of the nation's three electric power grids could cripple much of our infrastructure — and in the age of cyberwarfare, a laptop has become the only necessary weapon," reads the jacket blurb following another apocalyptic scenario of a months-long blackout leading to societal collapse.

State-sponsored attacks

The truth is that Russian hackers do try to get into American power plants, but so far they've only seemed to be performing reconnaissance, Larson said. Destructive malware has infected the office networks of some power companies, but the companies weren't specifically targeted, and the malware didn't cross over into plant operations.

"A ransomware infection at the financial-services division of an electric utility doesn't automatically translate to a blackout," Larson said.

While most state-sponsored hacker groups targeting power plants and other industrial-control systems only gather information, two other have gone further, Larson said. Those were the Electrum group, which used malware dubbed CrashOverride to take down a Ukrainian power plant in 2016, and the Trisis group, which infected the safety systems at a Saudi petrochemical plant in 2017.

Both attacks have been attributed to Russian state-sponsored hackers, and the Saudi-plant attack led another presenter at RSA 2019 to conclude that cyberattacks would soon kill people, either deliberately or accidentally.

But as Dragos founder and CEO Robert M. Lee stated in a 2017 blog posting describing the CrashOverride malware, "the public must understand that the outages could be in hours or days, not weeks or months."

Lee said that Dragos had "high confidence" that the CrashOverride hackers were the same who had in fact targeted U.S. and European infrastructure companies in 2014. And CrashOverride contained modules to "delete files and processes off of the running systems" to sabotage computer systems.

Larson said, however, that the CrashOverride creators had spent months or years planning the attack, and that the malware was specifically designed for that power plant. The attacks couldn't easily scale across the world, or even across Ukraine.

Outlook

There are true cyberattack threats out there, Larson added. For example, the Russian NotPetya ransomware worm in June 2017 cost the Maersk shipping line an estimated $200 million, and FedEx an estimated $300 million. The North Korean WannaCry attack the previous month crippled hospital computer systems in Europe and North America.

But in terms of the North American power grid, small animals such as squirrels, cats and raccoons are a much larger threat than hackers, and have caused hundreds of localized blackouts, Larson said. That mundane detail doesn't sell books.

The public should be reassured, she added, that the North American power grid (there are in fact three grids) has always been engineered to limit both the duration and the geographic reach of blackouts, and that there's no single power switch that can turn it all off.

"The truth is that the North American electric grid is resilient and segmented," Larson said.

#### No blackouts

Selena Larson 18, Cyber Threat Intelligence Analyst at Dragos, Inc., “Threats to Electric Grid are Real; Widespread Blackouts are Not”, 8/6/2018, https://dragos.com/blog/industry-news/threats-to-electric-grid-are-real-widespread-blackouts-are-not/

The US electric grid is not about to go down. Though it’s understandable if someone believed that. Over the last few weeks, numerous media reports suggest state-backed hackers have infiltrated the US electric grid and are capable of manipulating the flow of electricity on a grand scale and cause chaos. Threats against industrial sectors including electric utilities, oil and gas, and manufacturing are growing, and it’s reasonable for people to be concerned. But to say hackers have invaded the US electric grid and are prepared to cause blackouts is false. The initial reporting stemmed from a public Department of Homeland Security (DHS) presentation in July on Russian hacking activity targeting US electric utilities. This presentation contained previously-reported information on a group known as Dragonfly by Symantec and which Dragos associates to activity labeled DYMALLOY and ALLANITE. These groups focus on information gathering from industrial control system (ICS) networks and have not demonstrated disruptive or damaging capabilities. While some news reports cite 2015 and 2016 blackouts in Ukraine as evidence of hackers’ disruptive capabilities, DYMALLOY nor ALLANITE were involved in those incidents and it is inaccurate to suggest the DHS’s public presentation and those destructive behaviors are linked. Adversaries have not placed “cyber implants” into the electric grid to cause blackouts; but they are infiltrating business networks – and in some cases, ICS networks – in an effort to steal information and intelligence to potentially gain access to operational systems. Overall, the activity is concerning and represents the prerequisites towards a potential future disruptive event – but evidence to date does not support the claim that such an attack is imminent. The US electric grid is resilient and segmented, and although it makes an interesting plot to an action movie, one or two strains of malware targeting operational networks would not cause widespread blackouts. A destructive incident at one site would require highly-tailored tools and operations and would not effectively scale. Essentially, localized impacts are possible, and asset owners and operators should work to defend their networks from intrusions such as those described by DHS. But scaling up from isolated events to widespread impacts is highly unlikely.

#### All the important stuff is offline

Lila Kee 16, General Manager for GlobalSign's North and South American Operations, “Why Haven't We Seen a Disastrous Electric Power Grid Attack Yet?”, https://www.globalsign.com/en/blog/large-scale-electric-power-grid-attack/

If you based everything off what major news outlets are saying, you’d think our Critical National Infrastructure, particularly the energy sector, is riddled with weaknesses and ripe for a catastrophic cyber-attack. But the reality is, we haven’t experienced one yet (thankfully). Putting aside larger political reasons (fear of retaliation, widespread economic effects, etc.), is it possible that we haven’t seen one because these vulnerabilities have been overstated or the likelihood has been exaggerated? Below are some of my personal thoughts on the matter. Note: To be clear, I do not mean to imply we are “in the clear” and don’t need to worry about cybersecurity for the energy grid. On the contrary, continual efforts on best practices development, standards creation, regulation and vertical-specific technologies is of the utmost importance, especially as energy systems are brought online. I’m merely trying to see through the FUD and showcase the efforts that have helped keep the grid safe so far. Major Systems Have Been Offline and New Smart Systems Will Be Secured from the Start Grid providers are being hacked every day (303 incidents were reported to the Industrial Control Systems Cyber Emergency Response Team [ICS-CERT] in 2015), but most of those hacks were unsuccessful due to major systems that could cause devastation being either off-line or accessible only by private networks (i.e. not run over the internet). Vulnerabilities to older systems are being addressed through retrofits, but again most of these systems are offline. The good news is the next generation of smart grid systems are being designed with security in mind from day one. One good example is the Open Field Message Bus (OpenFMB) framework that provides a specification for intelligent power systems field devices to leverage a nonproprietary and standards-based reference architecture, which consists of internet protocol (IP) networking and Internet of Things (IoT) messaging. OpenFMB is one of Smart Grid Interoperability Panel’s (SGIP) Energy IoT initiative projects, developed to accelerate IoT innovation within the energy industry. As seen in other industries such as automotive, manufacturing and smart cities, the value added services around energy grid IoT innovation are virtually limitless. However, just like other industries, security concerns are top of mind. That’s where the North American Energy Standards Board’s (NAESB) role really proves vital. OpenFMB has smartly teamed with NAESB to develop a complementary set of standards for utility providers to follow. Given NAESB’s track record of standards development and tight relationship with NERC and FERC, a set of standards to accompany OpenFMB’s specification is more likely to gather industry participation and accelerate adoption.

#### Experts agree---the grid’s totally secure from cyber

Nancy Crotti 16, Writer and Editor at the Internet of Things Institute, “Could a Cyberattack Take Down the Power Grid”, http://www.ioti.com/security/could-cyberattack-take-down-power-grid

Panelists in another recent panel discussion on the cyberthreat to the grid disagreed with the widespread catastrophic thinking about it. “A nationwide blackout from a cyberattack is implausible,” said Caitlin Durkovich, assistant secretary for infrastructure protection at the Department of Homeland Security. While vulnerabilities exist, the utility industry has been working with local, state and federal government bodies for several years on prevention, detection, and recovery plans for a power grid cyberattack, Durkovich told listeners to the [discussion](http://event.on24.com/eventRegistration/console/EventConsoleNG.jsp?uimode=nextgeneration&eventid=1118796&sessionid=1&username=&partnerref=conf&format=fhaudio&mobile=false&flashsupportedmobiledevice=false&helpcenter=false&key=3EBDBAC544E4CBD4B1045A5D4BD2E918&text_language_id=en&playerwidth=1200&playerheight=1000&overwritelobby=y&eventuserid=152022306&contenttype=A&mediametricsessionid=120581314&mediametricid=1646231&usercd=152022306&mode=launch) on the topic hosted by The Energy Times. Utility companies deal with penetration attempts every day, said Gerry Cauley, CEO of the North American Electricity Reliability Corporation (NERC), an organization of U.S. electrical grid operators. NERC’s third grid attack simulation in November 2015 included participants from electric utilities; regional and federal law enforcement, first response and intelligence agencies; [information sharing and analysis centers](http://www.nationalisacs.org/) and other utilities; and supply chain stakeholder organizations. NERC is planning its [fourth grid attack simulation](http://www.nerc.com/pa/CI/CIPOutreach/Pages/GridEX.aspx) for November 2017. In the event of an actual cyberattack on the grid, the National Cybersecurity and Communications Integration Center in Arlington, VA would be the government’s control center. NERC has a representative at the center every day, according to a [report](http://thehill.com/policy/cybersecurity/281494-why-a-power-grid-attack-is-a-nightmare-scenario) by The Hill. In the event of a cyberattack that disabled large areas of the power grid, the person from NERC would be the liaison between the Department of Homeland Security and the electric industry. Working together will be key, according to Cauley. “This is not anyone’s problem to address or be prepared for, but it is a unity of effort across different agencies at the federal government as well as a state role in terms of a crisis to be able to make sure that the public is safe,” he said. Industry and government are focusing on real-time automated anomaly detection of cyber threats, according to Edna Conway, chief security officer of the global value chain for Cisco Systems, Inc. “We’re seeing some of that in the age of the Internet of Things and Big Data calculations that allow an operational-level view (in) real time and awareness to things that may not yet mean a security breach but are anomalous and need further investigation.”

### No Grid Impact---Resiliency---2NC

#### The grid’s fine---resiliency and redundancy check

Rick Geiger 16, Executive Director Utilities and Smart Grid at Cisco, “Power Grid Security: Separating Reality from Hype”, http://blogs.cisco.com/energy/power-grid-security-separating-reality-from-hype

We’ve all seen the news reports on power grid vulnerabilities and the possibility of an impending terror attack. Recently, Ted Koppel’s book, “[Lights Out](http://www.amazon.com/Lights-Out-Cyberattack-Unprepared-Surviving/dp/055341996X),” caused a wave of press around the issue. Similar spikes in press occurred in the year after the PG&E [Metcalf substation sabotage](http://www.nbcbayarea.com/news/local/PGE-Makes-Security-Upgrades-at-Metcalf-Substation-297045201.html) and around the National Geographic special in October 2013, “[American Blackout.](http://channel.nationalgeographic.com/american-blackout/)” There are both good points and some amount of exaggeration in the reporting on grid vulnerabilities, so I’ll be debunking a couple of [power grid security](http://www.cisco.com/c/en/us/solutions/industries/energy/external-utilities-smart-grid/security.html) myths. The [Associated Press](http://bigstory.ap.org/article/c8d531ec05e0403a90e9d3ec0b8f83c2/ap-investigation-us-power-grid-vulnerable-foreign-hacks) credits anonymous top experts for revealing about a dozen times in the last decade, “…sophisticated foreign hackers have gained enough remote access to control the operations networks that keep the lights on…” Rather than anonymous “top experts” you can find the results of an authoritative investigation, with attribution, in the 2007 report, “[Top 10 vulnerabilities of control systems and their associated mitigations](http://www.nerc.com/comm/CIPC/Related%20Files%20DL/2007_Top_10_Final_Approved_by_CIPC.pdf),” from the North American Electric Reliability Corporation (NERC) Control Systems Security Working Group. Headlines about the cyberattack on the Ukraine power grid greeted us at the start of 2016. [Ars Technica](http://arstechnica.com/security/2016/01/first-known-hacker-caused-power-outage-signals-troubling-escalation/) reported, “Highly destructive malware creates ‘destructive events’ at 3 Ukrainian substations.” Utilities Telecom Council Security offered a slightly different perspective in the Risk and Compliance Digest from January 6, 2016: “Some news media have speculated that the attacks were launched by or for Russia, in retaliation for Ukrainian activists’ attacks on the power supply to Crimea. That linkage will likely be impossible to prove or disprove. At present there is not enough evidence to positively conclude that this was a cyberattack or who is responsible. Regardless, the outage is fact. The discovered malware includes updated versions of known tools such as KillDisk, which is not in itself malware, and BlackEnergy. However there is no smoking gun – no piece of malicious code that definitively caused the outage. Researchers have yet to rule out the possibility of insider collaboration in the attack, possibly working in tandem with the malware.” Instead of panicking, let’s fact check some claims. Myth #1: Our power system is aging and outdated. The [Associated Press](http://bigstory.ap.org/article/c8d531ec05e0403a90e9d3ec0b8f83c2/ap-investigation-us-power-grid-vulnerable-foreign-hacks) warns that “Many of the substations and equipment that move power across the U.S. are decrepit and were never built with network security in mind…” It certainly is the case that many of the capital assets that comprise the United States grid infrastructure are used beyond their intended useful life of 25 years or longer. The initial operations certificates for nuclear power plants were 40 years. Of course they were never built with network security in mind because 40 years ago networks, if they existed at all, were local and limited (DECNet, Token Ring, etc.) For reference: The Hoover Dam was constructed in 1935. The San Onofre Nuclear Generating Station (SONGS) Unit 1 started operation in 1968. Cisco was founded in December of 1984. Despite their age, utilities every year spend billions of dollars maintaining and upgrading electric power infrastructure systems to maintain the level of reliability we’ve come to expect. For a closer look, watch this video of helicopter maintenance on an energized 765K Volt Line. Myth #2: We are unprepared if the grid goes down. Ted Koppel’s book primarily focuses on the potential consequences of an extended power outage, echoing the National Geographic special from 2 years earlier. Ted states that, “The Department of Homeland Security has no plans beyond those designed to deal with the aftermath of natural disasters.” And that “We are unprepared…” Both Ted Koppel and National Geographic start with the assumption that the grid has been disabled for months to establish the assumed starting conditions against which the story of preparedness for months of no power is told. The North American utility industry would disagree with the impression created by these writings that nothing has been done. They have spent billions implementing ever more stringent versions of NERC-CIP and other grid reliability measures. In addition to NERC-CIP, they have taken the following actions: Developed the NIST Interagency Report 7628, Guidelines for Smart Grid Cybersecurity Conducted GridEx, GridEx II, and GridEx III to exercise crisis response and recovery Complied with Presidential Order 13636 from February 2013 on Critical Infrastructure Security Applied recommendations from SuperStorm Sandy reports for grid resilience and response actions. Followed the Critical Infrastructure Security provisions in the 2016 budget bill just passed by the House. Is it enough? Can we relax? As the famous quote goes, “Eternal vigilance is the price of liberty” and in this case, Eternal Vigilance is the price of security of our critical infrastructure. Despite what has been done to secure the grid, the industry remains too smug about the disconnected nature of many critical systems. In doing so, they overlook the fact that some of the most successful and devastating cyberattacks have been carried out against systems that were not connected to the internet, the most prominent example being Stuxnet and the damage to the Iranian centrifuge capability. Despite having rifle bullets shot into the high voltage transformers in the Metcalf substation, not a single PG&E customer lost power. That’s a result of protections and redundancy that are an integral part of the design of the grid. Experiences with wide area outages and cascade failures have led to constant improvements in control systems and design redundancy. Is it perfect? Certainly not. Can it be improved? Definitely. We continue to learn from each large outage or natural disaster. The analysis of the 2011 Southwest Blackout jointly issued by NERC & FERC is one example. Lessons learned from Superstorm Sandy are another. The Bottom Line While vulnerabilities in the grid remain, considerable investment, study, and effort are being expended to identify vulnerabilities and secure the grid from cyber and physical attacks. Events like Superstorm Sandy and the sabotage of the Metcalf substation have caused Federal, State, and Local governments and regulators to rethink critical power requirements and develop plans that are tested during crisis exercises.

#### It won’t cascade---impossible

Chris Marciano 16, Utilities Worker and Researcher, “Could Terrorists Shut Down The United State's Entire Power Grid?”, https://www.quora.com/Could-terrorists-shut-down-the-United-States-entire-power-grid

Unlikely. First off, there are three separate grids in the US: the Eastern Interconnect, the Western Interconnect, and Texas (called ERCOT). Yes, Texas is its own entity. Don't act surprised. You can take an electron and run it from Louisiana to Maine, but you can't go to Houston or San Francisco. Several changes were made due to the Northeast Blackout of 2003. The grid operates on a principle of redundancy to avoid cascading failures. When a power line fails, the electrons near-instantaneously go to other lines. If the addition of those electrons cause these lines to overload and fail, the failures will continue like a domino effect. The operators of the grid, using fancy software, manage the grid so that no single failure leads to a cascading failure. If one failure does occur, they will make necessary changes to prevent another single failure from causing a cascading failure; that could include a starting reserve generation in particular areas (even if that generating resource is more costly) or by turning off the power of select areas.

### No Grid Impact---No Extinction---2NC

#### Their evidence cites the EMP commission. They’re professional crackpots!

Patrick Disney 11, Graduate Student Focusing on Iran and Nuclear Nonproliferation at Yale University, Former Assistant Policy Director for the National Iranian American Council, “The Campaign to Terrify You About EMP”, The Atlantic, 7/15/2011, https://www.theatlantic.com/international/archive/2011/07/the-campaign-to-terrify-you-about-emp/241971/

As with many things in Washington, a cottage industry of lobbyists, specialists, and ex-government officials has come together to attest to the danger of an EMP attack. Ballistic missile defense seems to be the panacea for this group's concern, though a generous dose of preemption and war on terror are often prescribed as well. Congress even created a special EMP commission in 2001 to study the issue and make recommendations to government and industry. It seems the only ones who take the time to talk about EMP publicly, however, are those who believe it to be the paramount threat facing America. According to their warnings over the last decade, our vulnerability worsens every day, and that vulnerability invites an attack.

For example, EMPact America, the group that hosted the conference at Niagara Falls, has been on a lobbying blitz in recent weeks to pass the SHIELD Act. The bill, which is backed by the Congressional "EMP Caucus" (yes, such a thing exists) is intended to protect the electrical grid of the continental United States from the effects of an EMP attack. EMPact America even produces a weekly, hour-long radio show devoted entirely to the issue, with recent guests including former CIA Director James Woolsey and Congressman Trent Franks. What sort of response have these warnings gotten so far? In Washington's nuclear arms control circles, where I've spent the past few months working as part of my research on the Iranian nuclear program, they're not really taken seriously.

But how can one side of a debate claim something threatens the very fiber of U.S. civilization, without getting so much as a nod in return? Serious public figures have taken up the cause: Congressmen, generals, scientists and strategists, all without much policy movement to show for their efforts.

It may be that a terrorist, after going through the trouble of acquiring a nuclear warhead and a missile capable of delivering it to America's shores, would be a fool to employ the ultimate weapon in such a cockamamie fashion. The effects of an EMP are far from universal; according to one commissioned study, a best-case scenario would impact 70 percent of electronics, while a worst-case estimate could be as low as 5 percent. Far better from the terrorist's perspective to deliver the bomb as it was intended, rather than hang his hopes on a series of unpredictable events and second- or third-order consequences. After all, a nuclear bomb need not be made any more devastating to serve a terrorist's purposes.

A slightly more plausible scenario could involve a state actor who, facing a vastly superior U.S. military massed on its border, might consider launching an EMP attack against U.S. troops as a way of evening the playing field. Because the U.S. military is much more highly dependent on technology than others, a rogue state facing the threat of invasion could conceivably attempt such a tactic against invading forces in the hopes that it could damage their capabilities without incurring the totally devastating retaliation that a "regular" nuclear strike would surely provoke. Of course, a wide-ranging EMP would knock out his own electronics as much as it would anyone else's, so even this scenario is a bit far-fetched.

But not as far-fetched as it may seem. One country's military has already come close to employing this tactic on the battlefield: our own. In 1991, Newsweek reported that General Norman Schwarzkopf sought authorization to use a nuclear EMP to cripple Saddam Hussein's forces at the start of the Gulf War. President George H.W. Bush nixed the plan, probably because the U.S. isn't in the habit of launching nuclear strikes of even the non-lethal kind, but the idea was tempting enough that this warfighter took it to his bosses for approval.

The bulk of the political debate today over EMP focuses on how disastrous it would be if the entire country's power went off all at once, which arms control experts argue is, to put it mildly, unlikely. Even "ideas man" Gingrich boils things down to a biblical catastrophe waiting to happen, but the reality is much more complicated. Nuclear weapons, after all, are more than enough of a threat in their own right. Putting too much emphasis on something as unlikely as an EMP attack against the American heartland risks distracting much-needed attention and resources away from threats that are simply more plausible.

As the Republican presidential primary heats up, Gingrich or another conservative voice may try to use the EMP "threat" as a campaign issue. So far, it has not been much of a political winner. Of course, when it comes to the politics of national security, it's often the loudest voice, not the most informed, that prevails.

### No Grid Impact---No Extinction---AT: Meltdowns

#### Blackouts don’t cause meltdowns and no extinction

Nick Stockton 16, Science Reporter for WIRED magazine, "Nuclear Power Is Too Safe to Save the World From Climate Change," WIRED, 4/3/2016, https://www.wired.com/2016/04/nuclear-power-safe-save-world-climate-change/

That’s a good deal, but still. Show a crowd a pair of cooling towers, and at least some of them will see an atomic apocalypse featuring three-eyed fish, leafless forests, and hospital-gowned Soviet defectors with skin like glistening mayonnaise. Nuclear power may be clean, but people still question whether it is, or ever will be, safe enough.

Those fears may be moot. Safety concerns didn’t delay construction on Watts Bar Unit 2 for so many years. Economics did. For all that fear, nuclear power still has the safest track record of any power source.

The Danger

Nuclear energy sources are dangerous because they emit radiation—particles and energy shed from unstable molecules trying to calm down. “Those radioactive missiles can hit the human body and damage cells or DNA,” says David Lochbaum, director of the Union of Concerned Scientist’s nuclear safety project. Enough radiation will give you cancer, or possibly even pass genetic mutations on to your kids. Too much can kill you outright.

But plants like Watts Bar don’t release much radiation into the environment. Inside, radioactive material heats water, which turns into steam, which spins the enormous turbines that generate electricity. Plants regularly release some of that water and steam at rates prescribed by the US Nuclear Regulatory Commission, and if you live downriver or downwind of one, the radiation within will raise your chances of developing a tumor by just one tenth of one percent. You’re far more likely to grow a tumor because you sneak a cigarette now and again.

But you aren’t afraid of routine releases. You’re terrified of another Three Mile Island, Fukushima, or Chernobyl.

These disasters were the result of a meltdown, which occurs when something impedes a reactor’s ability to cool the fuel. The US, where nearly 20 percent of electricity comes from 99 nuclear plants, uses uranium. Older reactors—which is every reactor in the US, including Watts Bar Unit 2—use electric pumps to move water through the system. The Fukushima disaster showed what happens if you have pumps but no power to use them. Newer generations rely on gravity instead, draining cooling water from elevated storage tanks to send it through the reactor core.

Those updates mean serious nuclear accidents are becoming ever more rare. Since Three Mile Island in 1979, the Nuclear Regulatory Commission found that the rate of shut-down-the-reactor-level problems has dropped from 2.5 per plant per year to around 0.1 (One such happened on March 29 in Washington). Even Three Mile Island wasn’t the disaster it could have been, because of that plant’s layers of redundant protection.

In terms of full blown nuclear disaster, there is really only one data point: Chernobyl. Which was horrifying. But in terms of real risk? The World Health Organization estimates the disaster will claim 4,000 lives, a figure that includes everything from direct victims to people born with genetic mutations well after the meltdown in 1986. By comparison, particulate matter from coal power plants kills about 7,500 people in the US every year. Radiation is the shark attack of environmental danger: An awful way to go, but far less likely than, say, a car wreck.

#### Generators, non-electric turbine-driven pumps, and water flooding prevent meltdowns, even without electricity

Dr. Arthur Bradley 16, Ph.D., Author of the Handbook to Practical Disaster Preparedness for the Family, 3rd Edition, Prepper’s Instruction Manual: 50 Steps to Prepare for any Disaster, Disaster Preparedness for EMP Attacks and Solar Storms (Expanded Edition), and the Frontier Justice (The Survivalist Book 1)," https://thesurvivalmom.com/long-term-blackout-nuclear-meltdown/

Emergency systems Nuclear plants obviously require electricity to operate their cooling pumps, not to mention their control systems. That power is normally tapped off of the electricity that the reactor generates. If the plant is offline, the power is provided by the electrical grid. But what happens when the grid itself goes down? The short answer is that large on-site diesel generators automatically activate to provide electricity. And if those should fail, portable diesel generators, which are also on-site, can be connected. Recent standardization has also ensured that generators can be swapped between plants without the need to retrofit connectors. There are also a couple of additional emergency systems that can be used specifically to cool the reactor. These include the turbine-driven-auxiliary-feedwater pump, which uses steam generated by the reactor to power a cooling turbine. The pump requires an operator, but it runs completely without electricity. This system, however, is meant only for emergency cooling of the reactor during those critical first few days when the fuel rod assemblies are being brought down in temperature, not for long-term cooling. And finally, in the worst case, most plants have a method of bringing in river or ocean water to flood the reactor. This typically damages the cooling system, but again, it helps to cool and cover the reactor core should all else fail. Unlike in other countries, permission from the federal government is not required to flood the reactor. Worst-case power-loss scenario With backup systems to the backup systems, it would seem that there’s nothing to worry about, right? Under all but the direst of circumstances, I think that assessment is correct. However, one could imagine a scenario in which the grid was lost and the diesel generators ran out of fuel. Speaking of fuel, how much is actually stored onsite? It depends on the plant, but at the Watts Bar Nuclear Plant, for example, there is enough fuel to run the emergency diesel generators for at least 42 days. I say at least because it would depend on exactly what was being powered. Once the reactor was cooled down, a much smaller system, known as the Residual Heat Removal System, would be all that was required to keep the fuel assemblies cool, both in the reactor and the spent fuel rods pool. The generators and onsite fuel supply could power that smaller cooling system for significantly longer than if they were powering the larger reactor cooling system. Even if we assumed a worst case of 42 days, it’s hard to imagine a scenario in which that would not be enough time to bring in additional fuel either by land, water, or air. Nonetheless, let’s push the question a little further. What would happen in the unlikely event that the diesel fuel was exhausted? Even with the reactor having been successfully cooled, the biggest risk would continue to be overheating of the fuel rod assemblies, both in the reactor and the spent fuel rods pool. Without circulation, the heat from the fuel rod assemblies could boil the surrounding water, resulting in steam. In turn, the water levels would drop, ultimately exposing the fuel rods to air. Once exposed to air, their temperatures would rise but not to the levels that would melt the zirconium cladding. Thankfully, that means that meltdown would not occur. The steam might well carry radioactive contaminants into the air, but there would be no release of hydrogen and, thus, no subsequent explosions. The situation would certainly be dangerous to surrounding communities, but it wouldn’t be the nuclear Armageddon that many people worry about.

#### No meltdowns impact, and evacuation solves

Tiffany Kaiser 11, writer for Daily Tech, citing Nuclear Regulatory Commission Report, 8/2/2011, DailyTech, "NRC: Far Fewer People Would Die in a U.S. Nuclear Meltdown Than Previously Thought," https://tinyurl.com/y4aujwkz

The nuclear crisis at Fukushima Daiichi in Japan has caused a nuclear frenzy where leaders around the world are questioning the safety of their plants. For instance, French President Nicolas Sarkozy called for global nuclear review after visiting Japan, and U.S. senators demanded that the Nuclear Regulatory Commission (NRC) repeat an expensive inspection of the country's nuclear power.

But now, the NRC is close to completing a large nuclear study that may ease a few worried minds.

The NRC has been working with Sandia National Laboratories (a Department of Energy lab) on a study that revises previous projections of how quickly and how much cesium 137, which is a radioactive material made when uranium is split, could release from a plant after a nuclear core meltdown. The NRC has been working on the study for six years, and it will not be completely finished until next spring. But the nuclear watchdog group, Union of Concerned Scientists, has obtained an early copy of the report through a Freedom of Information Act request.

The new study is based on how much and how quickly cesium 137 could escape an American nuclear plant if a total blackout were to occur. A total blackout means complete loss of power from the grid, and backup diesel generators and batteries have failed as well. This leads to a nuclear meltdown. NRC scientists said that a total blackout would be rare at an American plant, but it is better to be safe than sorry. In addition, the NRC wanted to update previous projections related to cesium 137.

The NRC focused on two different types of reactors in the U.S.: the Peach Bottom Atomic Power Station in Pennsylvania, which has boiling-water reactors like Fukushima Daiichi, and the Surry Power Station in Virginia, which has pressurized-water reactors. Over 100 different plants were studied. Through computer models and engineering analyses, the NRC has concluded that the meltdown of a typical American reactor would lead to "far fewer deaths" than previously thought.

According to the new study, only 1 to 2 percent of a reactor core's cesium 137 could escape during a total blackout. Previous NRC estimates concluded that 60 percent of the cesium inventory could escape.

In addition, the new study found that one person in every 4,348 within a 10-mile radius of a nuclear meltdown would develop a "latent cancer" from radiation exposure. In previous estimates, it was one person in every 167.

The NRC said that large releases of radioactive material would not be "immediate," meaning that people within a 10-mile radius would have plenty of time to evacuate the premises. It concluded that the chance of death from acute radiation exposure within a 10-mile radius would be near zero, but some would be exposed to high enough doses to experience fatal cancers decades later.

"Accidents progress more slowly, in some cases much more slowly, than previously assumed," said Charles G. Tinkler, a senior adviser for research on severe accidents and an author of the study. "Releases are smaller, and in some cases much smaller, of certain key radioactive materials."

### Norms Fail---1NC

#### Cyber signaling and norms are impossible

Dr. Ian Hurd 19, Professor of Political Science and the Director of the International Studies Program at Northwestern University, "“If I Had a Rocket Launcher”: Self-Defense and Forever War in International Law." Houston Law Review, https://houstonlawreview.org/article/7952-if-i-had-a-rocket-launcher-self-defense-and-forever-war-in-international-law

Its history can also be told through the changing uses of law in the political practice of justification. The legal formulations that were once thought to enclose war fully within self-evident and constraining legal categories have turned inside out and now operate to disperse military action throughout the world. As national interests and military technologies have changed, the rules have adapted, both in ratione temporis and ratione materiale. The instrumental utility of expansive self-defense claims for powerful governments is great, and the power of state practice to redefine international law is well-accepted—together these two facts ensure that the operative understanding of international rules will not deviate far from the desires of strong states. As the rule has moved, so has its political effects. Today it serves to legitimize and legalize the turn to “endless war” that has characterized American foreign policy since 2001.

With self-defense now anchored on national security interests, it has released its former connections to time and to armed attack. From this new foundation, it became useful to ambitious governments who are eager to attack their enemies abroad. In self-defense defined as national security, these states found a legal justification that matched neatly with their new technologies of drones and cyber. Together, these tools encouraged those with the capabilities to engage in undeclared and perhaps never-ending military operations against those whom they see as enemies of the state.

The history of self-defense helps to show the gap between the mythology of international law and its practical life. The myth says that international law provides a stable framework of rules that enable states to act toward their objectives while limiting their capacity to engage in acts that are damaging to the entire community. The reality is that rules become tools which powerful actors aim to use to

their advantage. As Rebecca Sanders asserts, “There is nothing inherently progressive about legal culture[]” or international law.[82] The political effects of law depend on who is using it against what and against whom.

### Norms Fail---2NC

#### Cyber norms fail---states will cite i-law when it justifies their already decided policy and ignore it when it conflicts, proven by Iraq and every other recent example---that’s Hurd

#### Global agreement is impossible because security trumps values AND Russia and China won’t listen

James Shires 18, Research Fellow with the Cyber Security Project at the Belfer Center for Science and International Affairs, Harvard Kennedy School, DPhil candidate in International Relations at the University of Oxford, MSc from Birkbeck College, University of London, and BA from the University of Cambridge, “Between Multistakeholderism and Sovereignty: Cyber Norms in Egypt and the Gulf States”, War on the Rocks, 10/12/2018, https://warontherocks.com/2018/10/between-multistakeholderism-and-sovereignty-cyber-norms-in-egypt-and-the-gulf-states/

Conclusion

Amid deep conflict over basic norms, Egypt and the GCC states have maneuvered between two poles while enjoying the tacit, if not explicit, support of both sides. This has three key implications. First, global cyber norms are much more complex — and much more entangled with traditional governance practices, diplomatic relationships, and strategic concerns — than Western officials may like to admit. However uncomfortable it may be, international policymaking on cyber norms must take into account not only the “likemindedness” of some states, but also the fact of their strategic interests and relationships with other states that are less or not at all likeminded. Without this recognition, any attempt to create global cyber norms is hampered from the start. More broadly, to understand the complexity of cyber norms we must look outside the framework of great power competition.

Second, the United States and European allies of Egypt and the Gulf states need to decide where their priorities lie: Does consistency on global cyber norms outweigh broader security considerations? If a stable, coherent set of cyber norms is the primary aim, greater attention should be given to persuading friendly states to stay within the boundaries of these norms. However, if security alliances trump cyber norms, Western democracies should recognize that the rhetorical effect of denouncing Russian or Chinese action will be limited. For the United States, effective foreign policy regarding cyber security in the Middle East requires both the identification of a clear national interest, connected to broader strategic goals concerning the kind of cyber space the United States seeks to promote, and a good understanding of the evolving landscape in which the U.S. government and U.S. companies are operating. Right now, both are lacking.

Third, although the contradictions outlined here suggest that human rights and national security are important starting points for research, we should not confine cyber security research on these states to these well-trodden paths. In the Middle East, cyber security is changing regional alliances, altering the economic calculations of businesses, and reforging fundamental relationships between individuals and their governments. There are significant differences in cyber security approaches between these states, especially in Kuwait and Qatar. And there are many new initiatives and organizations, like Saudi Arabia’s National Cyber Security Authority (al-hai’a al-watniyya lil-‘amn al-sibrani), Egypt’s High Council for Cybersecurity, the UAE’s National Electronic Security Agency, and Oman’s Arab Region Cybersecurity Centre. As our understanding of cyber security evolves and its connection to other areas of foreign policy deepens, a broader approach to cyber security research in this region is urgently needed to adequately understand these new dynamics and inform future policy choices.

#### The Talinn Manual proves---no one outside of NATO signed on

Dr. Mette Eilstrup-Sangiovanni 18, Reader in International Relations and a Fellow of Sidney Sussex College at Cambridge University, PhD in Political Science from the European University Institute, “Why the World Needs an International Cyberwar Convention”, Philosophy & Technology, Volume 31, Number 3

The Necessity of an International Cyberwar Convention

This section presents the case for negotiating an international convention to govern cyber conflict between states. Despite growing threats from actors using ICT for aggressive and illicit purposes, few treaties address international cyber security issues. Presently, the main international agreements governing cyber conduct are the 2001 Convention on Cybercrime (and its Additional Protocol, 2006) and the Shanghai Cooperation Organization’s International Information Security Agreement (2009) (Vihul & Schmitt 2016, 39–40). Both agreements are severely limited, however, in terms of both their scope and membership.Footnote17 Calls for negotiating a comprehensive international treaty to govern cyber conflict—a so-called E-neva Convention—have so far met with disapproval, especially from Western states (ibid.)Footnote18 To date, the most elaborate discussions of cyber governance have thus focused on bringing existing international law to bear on cyber conflict. The *Tallinn Manual on the International Law Applicable to Cyber Warfare* (2013) is the most widely cited outcome of such discussions. This manual formulates a set of rules for how existing international law—chiefly *jus ad bellum*, international humanitarian law (IHL) and laws of state responsibility—apply in a cyber context (Talinn Manual 2013; Schmitt and Vihul 2014a, b, 2016; Lucas 2016). But while the Tallinn Manual (hereafter “the Manual”) provides a useful starting point for focusing attention on the need for stronger international cyber-governance, its practical value as an instrument to restrain cyber conflict is modest for (at least) three reasons. First, as Lucas points out (2017, 40), the Manual has generally failed to gain support outside the narrow group of NATO member-states that sponsored it. Second, the Manual does not propose or promulgate new international rules for the cyber domain but merely offers an interpretation of how existing laws may apply. So far, this interpretation has largely failed to persuade states to restrain their activities in the cyber domain (Lucas 2017, 17). What is more, the interpretation of many *jus ad bellum* and *jus in bello* treaty provisions as applied to cyber conflict remain unsettled (Schmitt and Vihul 2016, 43). Anticipating, as some of the leading legal scholars behind the Manual do, that “interpretative dilemmas concerning treaty law will be resolved through the recurrent practice of states in their application” (Ibid., 43–44) seems optimistic, especially when considering that the interpretation offered in the Manual has so far failed to influence state practice or opinio juris. Third, even if states were to agree on the general applicability of jus ad bellum and IHL in the cyber domain (which presently they do not), such agreement would hardly suffice. Each one of the international treaties and conventions currently governing the production, stockpiling, sale, transfer, and use of specific classes of armaments is testament to the states’ recognition that the general international prohibition on the use of force and IHL are by themselves insufficient to prevent or restrain international armed conflict.

#### U.S. restraint doesn’t cause global follow-on

James Lewis 12, Director of the Technology and Public Policy Program at the Center for Strategic and International Studies, “Benefits Are Great, and the Risks Exist Anyway,” New York Times, 6/4/2012, <http://www.nytimes.com/roomfordebate/2012/06/04/do-cyberattacks-on-iran-make-us-vulnerable-12/benefits-are-great-and-the-risks-exist-anyway>

Nor do cyberattacks against Iran increase the risk of damaging cyberattacks against the United States. It is true that we are defenseless; efforts to make us safer are hamstrung by self-interest, ideology and the gridlock of American politics. But we are no more vulnerable today than we were the day before the news. If someone decides to attack us, they may cite Iran as precedent, but it will only be to justify a decision they had already made.

We could ask whether the United States creates more problems for itself when it makes public a new weapon while potential opponents keep it secret. Four other countries can launch sophisticated and damaging cyber attacks -- including China and Russia -- and plan to use them in warfare. Another 30 nations are acquiring cyber weapons, including Iran and North Korea.

There is a very old argument for disarmament that holds that if the United States were to renounce some weapons -- usually nuclear weapons -- the world would be a better place. This utopianism has a revered place in American political thinking, but when humans invent weapons they rarely give them up, especially useful weapons whose components are easy to acquire. Cyberattack is now part of warfare, no different from any other weapon. The publicity around Stuxnet may complicate U.S. efforts to get international rules for the use of cyberattack, but the White House decided that tampering with Iran’s nuclear program was more important than possible risk to slow-moving negotiations.

#### Adversaries only care about balance of power

Dr. Keith Payne 15, PhD, Professor and Head of the Graduate Department of Defense and Strategic Studies at Missouri State University, “US Nuclear Weapons and Deterrence”, Air & Space Power Journal, July-August 2015, https://www.airuniversity.af.mil/Portals/10/ASPJ/journals/Volume-29\_Issue-4/V-Payne.pdf

Realists in this regard are from Missouri, the “show me” state, and ask utopians to explain how, why, and when a powerful new cooperative international norm with corresponding international institutions will become a reality. Realists point to the unhappy history of the unmet claims and dashed hopes of the 1928 Kellogg-Briand Pact (intended to prevent offensive war by global legal agreement), the League of Nations, and the United Nations. To be sure, the future does not have to be bound by the past, but before moving further toward nuclear disarmament, realists want to see some clear evidence of the emerging transformation of the global order—not just the claim that it can occur if all key leaders are so willing, faithful, and visionary and can “embrace a politics of impossibility.”12 As the old English proverb says, “If wishes were horses, then beggars would ride.” But has not everything changed in the twenty-first century? Has not the end of the Cold War ushered in a new global commitment to cooperation, the rule of law globally, and benign conflict resolution? The unarguable answer is no. Russian military actions against Georgia in 2008 and Ukraine since 2014 (the latter in direct violation of the 1994 Budapest Memorandum signed by Russia, Great Britain, and the United States) are sufficient empirical evidence to demonstrate that Thucydides’ stark description of reality is alive and well. China’s expansionist claims and military pressure against its neighbors in the East and South China Seas teach the same lesson. Why is this reality significant in the consideration of nuclear weapons? Because in the absence of reliably overturning the powerful norm of raison d’État and Thucydides’ explanation of international relations, states with the capability and felt need will continue to demand nuclear capabilities for their own protection and, in some cases, to provide cover for their expansionist plans. To wit, if Ukraine had retained nuclear weapons, would it now fear for its survival at the hands of Russian aggression? Former Ukrainian defense minister Valeriy Heletey and members of the Ukrainian parliament have made this point explicitly, lamenting Ukraine’s transfer of its nuclear forces to Russia in return for now-broken security promises of the Budapest Memorandum.13 This lesson cannot have been lost on other leaders considering the value of nuclear weapons. Nor is it a coincidence that US allies in Central Europe and Asia are becoming ever more explicit about their need for US nuclear assurances under the US extended nuclear deterrent (i.e., the nuclear umbrella). They see no new emerging, powerful global collective security regime or cooperative norms that will preserve their security; thus, they understandably seek the assurance of power, including nuclear power. The Polish Foreign Ministry observed in a recent press release that “the current situation reaffirms the importance of NATO’s nuclear deterrence policy.”14 This reality stands in stark contrast to utopian claims that powerful new global norms and international institutions will reorder the international system, overturn Thucydides, and allow individual states to dispense with nuclear weapons or the nuclear protection of a powerful ally. As the Socialist French president Francois Hollande has said, “The international context does not allow for any weakness. . . . The era of nuclear deterrence is therefore not over. . . . In a dangerous world—and it is dangerous—France does not want to let down its guard. . . . The possibility of future state conflicts concerning us directly or indirectly cannot be excluded.”15 There could be no clearer expression of Thucydides’ description of international relations and its contemporary implications for nuclear weapons. Opponents of the administration’s plan to modernize the US triad now double down on the utopian narrative by insisting that the United States instead lead the way in establishing the new global norm by showing that Washington no longer relies on nuclear weapons and does not seek new ones. Washington cannot expect others to forgo nuclear weapons if it retains them, they say, and thus it must lead in creation of the new norm against nuclear weapons by providing an example to the world. For instance, “by unilaterally reducing its arsenal to a total of 1,000 warheads, the United States would encourage Russia to similarly reduce its nuclear forces without waiting for arms control negotiations.”16 A good US example supposedly can help “induce parallel” behavior in others.17 If, however, the United States attributes continuing value to nuclear weapons by maintaining its arsenal, “other countries will be more inclined to seek” them.18 Nuclear realists respond, however, that the United States already has reduced its nuclear forces deeply over the last 25 years. America cut its tactical nuclear weapons from a few thousand in 1991 to a “few hundred” today.19 Moreover, US-deployed strategic nuclear weapons have been cut from an estimated 9,000 in 1992 to roughly 1,600 accountable warheads today, with still more reductions planned under the New START Treaty.20 The United States has even decided to be highly revealing of its nuclear capabilities to encourage others to do so, with no apparent effect on Russia, China, or North Korea.21 America has adhered fully to the reductions and restrictions of the 1987 Intermediate-Range Nuclear Forces Treaty—the “centerpiece of arms control”—but the Russians now are in open violation. As former undersec- retary of state Robert Joseph stated recently, decades of deep US reductions “appear to have had no moderating effect on Russian, Chinese or North Korean nuclear programs. Neither have U.S. reductions led to any effective strengthening of international nonproliferation efforts.”22 Utopians want the United States to lead the world toward nuclear disarmament by its good example, but no one is following. The basic reason, realists point out, is that foreign leaders make decisions about nuclear weaponry based largely on their countries’ strategic needs, raison d’État, not in deference to America’s penchant for nuclear disarmament or some sense of global fairness. A close review of India by S. Paul Kapur, for example, concluded that “Indian leaders do not seek to emulate US nuclear behavior; they formulate policy based primarily on their assessment of the security threats facing India.”23 The same self-interested calculation is true for other nuclear and aspiring nuclear states. Nations that are a security concern to the United States seek nuclear weapons to intimidate their neighbors (including US allies), to counter US conventional forces, and to gain a free hand to press their regional military ambitions. They see nuclear weapons as their trump cards and do not follow the US lead in nuclear disarmament. A bipartisan expert working group at the Center for Strategic and International Studies concluded accordingly that “U.S. nuclear reductions have no impact on the calculus of Iran and North Korea.”24

### No China Cyber---1NC

#### No major China cyber threat

Jon R. Lindsay 15, Ph.D. in Political Science from the Massachusetts Institute of Technology and M.S. in Computer Science and B.S. in Symbolic Systems from Stanford University, Assistant Research Scientist at the University of California, San Diego, “Exaggerating the Chinese Cyber Threat”, Belfer Center Policy Brief, May 2015, <https://www.belfercenter.org/sites/default/files/files/publication/linsday-china-cyber-pb-final.pdf> [language modified]

The rhetorical spiral of mistrust in the Sino-American relationship threatens to undermine the mutual benefits of the information revolution. Fears about the [loss] ~~paralysis~~ of the United States’ digital infrastructure or the hemorrhage of its competitive advantage are exaggerated. Chinese cyber operators face underappreciated organizational challenges, including information overload and bureaucratic compartmentalization, which hinder the weaponization of cyberspace or absorption of stolen intellectual property. More important, both the United States and China have strong incentives to moderate the intensity of their cyber exploitation to preserve profitable interconnections and avoid costly punishment. The policy backlash against U.S. firms and liberal internet governance by China and others is ultimately more worrisome for U.S. competitiveness than espionage; ironically, it is also counterproductive for Chinese growth.

### No China Cyber---2NC

#### No major China cyber threat:

#### No capabilities---they’re organizationally screwed with bureaucratic silos and info overload---can’t conduct big attacks

#### No motive---both sides will moderate to avoid economic blowback and destructive military retal---that’s Lindsay

#### They’re total n00bs who pose zero actual threat

Jon R. Lindsay 15, Ph.D. in Political Science from the Massachusetts Institute of Technology and M.S. in Computer Science and B.S. in Symbolic Systems from Stanford University, Assistant Research Scientist at the University of California, San Diego, “Exaggerating the Chinese Cyber Threat”, Belfer Center Policy Brief, May 2015, <https://www.belfercenter.org/sites/default/files/files/publication/linsday-china-cyber-pb-final.pdf>

Despite high levels of Chinese political harassment and espionage, there is little evidence of skill or subtlety in China’s military cyber operations. Although Chinese strategists describe cyberspace as a highly asymmetric and decisive domain of warfare, China’s military cyber capacity does not live up to its doctrinal aspirations. A disruptive attack on physical infrastructure requires careful testing, painstaking planning, and sophisticated intelligence. Even experienced U.S. cyber operators struggle with these challenges. By contrast, the Chinese military is rigidly hierarchical and has no wartime experience with complex information systems. Further, China’s pursuit of military “informatization” (i.e., emulation of the U.S. network-centric style of operations) increases its dependence on vulnerable networks and exposure to foreign cyberattack.

To be sure, China engages in aggressive cyber campaigns, especially against nongovernmental organizations and firms less equipped to defend themselves than government entities. These activities, however, do not constitute major military threats against the United States, and they do nothing to defend China from the considerable intelligence and military advantages of the United States.

#### China’s closed system prevents necessary improvements

Jack Detsch 15, Editorial Assistant at The Diplomat, Al-Monitor's Pentagon Correspondent, “Are We Exaggerating China’s Cyber Threat?”, The Diplomat, 5/20/2015, https://thediplomat.com/2015/05/are-we-exaggerating-chinas-cyber-threat/

So how much should we worry about China’s cyber capabilities?

Not much, according to Professor Jon R. Lindsay’s new policy brief, published by Harvard University’s Belfer Center. Public record on U.S. and Chinese cyber capabilities remains scant, but Lindsay suggests that the U.S. is gaining an “increasing advantage,” evidenced by a new DARPA program launched in 2012, and the use of the Stuxnet worm to damage computer systems at an Iranian nuclear enrichment facility in 2010. In America’s private cyber industry, the name of the game has shifted from defense to offense.

But China’s interest in developing cyber capabilities is political, not military, Lindsay argues, prompting incursions into foreign digitized space to suppress dissent, in the case of GitHub, or to steal secrets from adversaries. Even so, “lax law enforcement, and poor cyber defenses leave the country vulnerable to both cybercriminals and foreign spies,” Lindsay notes, suggesting that China struggles to use the information it comes away with for political gain. China’s successful campaigns target NGOs and private sector companies, and “do nothing to defend China from the considerable intelligence and military advantages of the United States.”

That doesn’t mean that the PLA isn’t busy playing catch-up. In a recent issue of The Science of Military Strategy, put out by the military’s chief research institution, analysts concede that the PLA indeed possesses network attack forces inside of intelligence and civilian wings of government, including the Ministry of State Security and the Ministry of Public Security. It suggests that the military will deal with critical infrastructure targets, like electrical grids and gas pipelines, while smaller, nimbler hacking units like Axiom, which has been suspected in intrusions against Fortune 500 companies and pro-democracy groups, will focus on industrial targets.

But making that leap will be challenging, and would force China to walk back its global positions on cybersecurity. Beijing hopes to become a leader on that front and has been heavily promoting its concept of “internet sovereignty” as the basis for international standards of behavior in cyber space. China wants to defend “internet sovereignty” at all costs. Any future cyber attack would probably be justified on those grounds.

That’s also a self-limiting belief. While it has allowed home-grown giants like Weibo, Alibaba, and Baidu to flourish, China’s exclusion of American companies and know-how put it at a serious disadvantage in building robust cyber capabilities. China’s own approach to these issues could prevent Beijing from reaching its cyber potential.

#### No US-China cyberwar and no escalation --- the US is too dominant. And, China will cheat.

Elizabeth **Thomas 16**, the Australian National University, 8-28-2016, "US-China Relations in Cyberspace: The Benefits and Limits of a Realist Analysis," E-International Relations, http://www.e-ir.info/2016/08/28/us-china-relations-in-cyberspace-the-benefits-and-limits-of-a-realist-analysis/

Cybersecurity issues have increasingly been singled out as an irritant in the United States(US)-China bilateral relationship. US-China relations in cyberspace exemplify tensions in the broader bilateral relationship, canvassing military competition, trade barriers, intelligence activity, and pathways to long-term economic and political strength.[1] However, cybersecurity is still a nascent foreign policy issue. Much of the existing literature on cybersecurity in international relations addresses the issue through the lens of policy rather than theory. This paper is a contribution to bridging the gap between policy and theory. It examines the extent to which offensive realist theory helps us understand how the US and China are managing their relations on cybersecurity. I argue that the US is a hegemon in cyberspace, and China a revisionist power. Based on that assessment, I consider the likelihood of cyberwar, the issue of economic espionage, their respective approaches to Internet governance, and conclude that offensive realism provides a useful framework for considering security-related issues. However, it cannot explain the full range of bilateral cyber-related activity, including examples of cooperation and norm-building in cyberspace. I briefly touch on liberal theories’ ability to explain other elements of the relationship and conclude that given the breadth of cyber-related issues, an issue-specific or analytically eclectic approach may be the most fruitful. The framework for analysis: offensive neorealism Offensive realism refers to a sub-school of neorealist international relations theory, which developed from Kenneth Waltz’s work on structural realism.[2] The classical realism of thinkers like Hans Morgenthau had focused on human nature.[3] Waltz shifted realism’s focus to the international system, positing that the anarchic structure of the international system forces states to pursue power to ensure their survival. Power – measured by the relative distribution of economic and military capabilities across the system – is a state’s only guarantee of security. Subsequently, sub-schools of defensive and offensive realism have developed based on Waltz’s work.[4] This paper focuses on the applicability of John J. Mearsheimer’s offensive realism to US-China cybersecurity relations.[5] I have chosen offensive realism as the basis for my analysis because the relationship is popularly characterized as conflictual. Offensive neorealism posits that great powers seek to ensure their security by maximising their share of world power. Being the dominant power – a hegemon – is the best means to ensure survival. States therefore are “primed for offense”.[6] Mearsheimer makes five key assumptions about the international system, which together cause states to formulate aggressive policies.[7] These are: (1) anarchy is the ordering principle of the international system; (2) great powers possess some military capability; (3) states can never be certain about other states’ intentions; (4) survival is the primary goal of great powers; and (5) that great powers are rational actors.[8] I will treat these assumptions as given for the purposes of my analysis. Combined, these factors result in three patterns of behaviour: fear, self-help, and power maximisation.[9] Unable to trust other states, and aware that they operate in a self-help system, states view becoming the most powerful states in the system as the best way to ensure survival.[10] States look to maximise their power and alter the balance of power using a variety of tools – even if doing so makes other states suspicious or hostile.[11] Capability is what matters, given the intentions of other states are uncertain. States will lie, cheat and use force if it can help them gain an advantage.[12] All great powers will have revisionist tendencies until they achieve hegemony, resulting in constant security competition.[13] Finally, in Mearsheimer’s view, multipolar systems are more likely to result in conflict than bipolar systems, and multipolar systems with an emerging hegemon are the most dangerous (“unbalanced multipolarity”).[14] What is the current balance of power in cyberspace? In order to understand whether there is a security competition in cyberspace, it is necessary to assess the current balance of power. Because I am considering cybersecurity in isolation from the wider bilateral relationship this analysis necessarily will be artificial, focusing only on relative cyberpower (broadly defined). Mearsheimer defines a hegemon as a “state that is so powerful that it dominates all the other states in the system.”[15] A state that is substantially more powerful than other powers in the system is not a hegemon – a hegemon is the only great power.[16] Mearsheimer concludes that it is virtually impossible for a state to become a global power because of the difficulties in projecting power across the world’s oceans.[17] However, the US arguably has hegemonic power in cyberspace, where geographic boundaries do not affect power projection. The US, thanks to its role in the Internet’s creation and development, retains a huge amount of influence over its operations and governance. Ten of the Internet’s 13 root servers are on US soil, and China, like many other states, is still reliant on technology from American firms like Microsoft.[18] Secondly, the US is generally believed to have the most significant cyber offensive capabilities in the world. While cyber capability is shrouded in secret, the US is likely to have a good chance at dominating other great powers in cyberspace. The question is then whether there are any other great powers in cyberspace. China has arguably risen as a cyber power, though its (known) activities to date are computer-network exploitation for intelligence rather than attacks causing disruption.[19] China sees cyber power as a cost effective, long range way to counter a superior adversary in conflict.[20] China has also become increasingly influential in global policy debates on Internet governance issues, as will be discussed below. However, the US has considerably more experience in managing complex network operations and the Peoples’ Liberation Army faces sizeable challenges implementing cyber tactics.[21] Cyberspace also is not a simple bipolar world. Russia, for instance, is widely considered to be one of the most capable actors in cyberspace and is believed to have deployed offensive cyber capability in support of its wider objectives (most recently shutting down a power grid in the Ukraine). Cyber capabilities also are proliferating widely, in part because of low barriers to entry.[22] Cyberspace therefore can loosely be characterized as a multipolar system. In an unbalanced multipolar system, we should expect to see an ongoing security competition, based on calculations of relative state power. The US will seek to check China’s activity to maintain its hegemony. China, as an aspiring hegemon and revisionist power, will use force to alter the status quo if the benefits outweigh the costs.[23] The polarity of the system will make states fearful and security competition is likely to be particularly acute in the cyber context. The secrecy shrouding states’ cyber capabilities makes it difficult to measure relative capability, which will increase suspicion. A spiral of mistrust – should we expect the outbreak of cyberwar? Relations between the US and China indeed have been marked by fear and mistrust. Growing concerns about competitive advantage have exacerbated that mistrust, along with ongoing intelligence activities and political rhetoric. China is suspicious that the US is using its dominance in cyberspace to undermine other states, which suggests a sense of vulnerability, and US has a deep sense of unease about a rising China.[24] Offensive realism suggests that how much states fear each other determines the severity of their security competition as well as the likelihood that they will fight a war.[25] As signaled above, states cannot accurately assess their relative cyberpower because offensive cyber capabilities tend to be highly classified. Fear has therefore driven both states to invest in offensive and defensive capabilities.[26] There is also an incentive for both to misrepresent their strength, so the true balance of power is unclear.[27] This may lead to a misperception of dominance, particularly when the effectiveness of ‘cyberweapons’ is poorly understood.[28] However, a cyber conflict between the US and China is highly unlikely. Examples of attacks with destructive or physical consequences are still very rare (although the number may be increasing). Since the late 1980s, there have been 61 attacks conducted by states against during peacetime, and 24 during wartime.[29] Examples include Russian attacks on Georgia in 2008 and the infamous Stuxnet attack on Iranian nuclear infrastructure (usually attributed to the US and Israel).[30] No state has ever declared a ‘cyberwar’.[31] This is partly because to develop sophisticated attacks like Stuxnet is very difficult, requiring high levels of technical expertise.[32] Attribution is also notoriously difficult in cyberspace. It is extremely tough to trace attacks and states may also use proxy or non-state actors, further confusing the issue.[33] Until recently, the failure to develop an effective deterrence policy has been related to the difficulty in attributing cyberattacks. Nevertheless, the US has “reserve[d] the right to use all necessary means – diplomatic, informational, military, and economic – as appropriate and consistent with applicable international law” to respond to hostile acts in cyberspace.[34] China has not used ‘force’ against the US in cyberspace but it is clear that cyberattacks would feature in any broader military clash. Difficulties arise in considering what constitutes a proportionate response to low-level attacks like hacking or cybercrime. It is very unlikely that any incident of that nature could justify a traditional military response.[35] To date, countermeasures have fallen well below the use of military force. The US has instead relied on diplomatic and law enforcement tools: attribution, indictments, and the threat of sanctions.[36] Cyber-enabled espionage – a constant, low level conflict? Intense security competition between the US and China is much more evident when considering the issue of cyber-enabled espionage. As a trading state, China has benefited from Internet connectivity, but it is still a net importer of advanced technology.[37] To maintain high growth levels in an innovation-driven world, economic espionage is a useful shortcut, and economic power is fungible.[38] The US has consistently alleged that China is conducting economic espionage on a massive scale to support Chinese firms. Good evidence exists to support this allegation. For instance, one study found that “96 percent of recorded, state-affiliated attacks targeting businesses’ trade secrets and other intellectual property in 2012 could be traced by to Chinese hackers.”[39] While each loss might be small, the net effect has been described as “the most significant transfer of wealth in history.”[40] In response, China has consistently accused the US of hypocrisy, supported by evidence in the Snowden disclosures of the extent to which the US had penetrated a range of Chinese companies and networks.[41] Chinese officials point out that China is the largest victim of cyber attacks in the world, many emanating from the US.[42] In China’s view, the US has no “moral standing” to make accusations against China or define norms of appropriate behaviour online.[43] Despite this, the US has attempted to draw a distinction between espionage for national security purposes and economic espionage for the benefit of a states’ firms (such as China’s state-owned enterprises). While China has historically refused to acknowledge this distinction, US policy has been calibrated both to develop this norm and to raise the costs of Chinese activity. Until recently, actions in cyberspace had been largely penalty-free. Over the last two years, the US has executed the first steps in a new strategy to change the cost-benefit-risk calculus for its cyber adversaries.[44] In May 2014, the Department of Justice indicted of five members of the Chinese Peoples’ Liberation Army (PLA) for hacking and commercial espionage against major US companies.[45] Following the high-profile hack of Sony pictures in December 2014, the US attributed the attack to North Korean actors – the first time that the US had publicly attributed an attack on a US company to a foreign government.[46] Then, in April 2015, President Obama signed an executive order allowing the US to impose severe financial restrictions on individuals or entities who engage in or benefit from cyber-enabled economic espionage.[47] In advance of President Xi Jinping’s first state visit to the US in 2015, there were serious indications that the Obama administration might impose sanctions against China in a second major volley on economic espionage.[48] Shortly before the visit, Obama described theft of intellectual property and trade secrets as an “act of aggression” and a “core national security threat”.[49] Despite previously refusing to accept the US distinction between ‘acceptable’ espionage for national security and ‘unacceptable’ economic espionage, President Xi reached a landmark agreement with President Obama in September 2015. The two leaders agreed that “neither country’s government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.”[50][51] The agreement was an unexpected reversal of the Chinese position. Offensive realism suggests that China may have signed the agreement for two reasons. Threatened with sanctions, China made a rational choice – the costs of cyber activity against the US were rising and it was in China’s interest to agree. More pessimistically, China may also have signed with no intention of adhering to the agreement. Offensive realism suggests that concerns about cheating will hinder cooperation, as states fear that the other side will cheat, putting them at a disadvantage. [52] Subsequent evidence suggests that China is not complying with the agreement. The Director of National Intelligence noted in February 2016 that “China continues to have success in cyber espionage against the U.S. government, our allies, and U.S. companies.”[53] Continuing Chinese activity suggests that the US has not succeeded in raising the real costs of economic espionage. The costs of an indictment and the threat of sanctions are slight in comparison to the benefits China is reaping from its economic espionage practices.[54] Cheating on a cyber agreement may also be simpler because deception is a core part of network intrusions.[55] As long as the benefits to China outweigh the risks, there is no reason to stop. For the US, it appears that more significant punishments may be too costly or escalatory to pursue.[56] Some of this reluctance likely derives from concerns about damaging relations with a state with a major economic market.[57]

### No China War---1NC

#### No US-China war.

Cui Lei 20, PhD and MA in International Politics, associate research fellow with the China Institute of International Studies, "Despite heated talk, risk of a US-China hot war is small", South China Morning Post, 7-24-2020, https://www.scmp.com/comment/opinion/article/3094121/why-risk-us-china-hot-war-small-despite-heated-talk

Many observers are pessimistic about deteriorating US-China relations and believe the two countries are heading towards a cold war. Even worse, some argue that the situation might be more dangerous than the US-Soviet Union Cold War, and that a hot war might break out between the two. This argument is unconvincing.

First of all, deterrents to a flare-up are much stronger in US-China relations than in US-Soviet relations. Although economic and people-to-people ties between China and the US are declining, they are still close compared to US-Soviet ties. It is hard to decouple two closely intertwined economies and societies.

Take two examples. China is expected to become the world's largest consumer market, a temptation hard to resist for exporters, including those from the US. And in education, more than 300,000 Chinese students study in the US, bringing in huge revenues for the US education industry.

Many universities go to great lengths to woo international students. Recently Harvard and the Massachusetts Institute of Technology even sued the government over its new visa restrictions, now aborted, on international students.

Second, even if there is decoupling, the pain would not be too great and can be kept out of the national security sphere if properly handled. In fact, for national security reasons, a modest degree of isolation will make both sides more secure and comfortable. For instance, if China’s information technology equipment cannot capture Western markets, the US will be more relaxed. If China cannot get advanced technologies from the US and its technological progress slows down, the US will be less anxious.

In the same vein, China feels assured knowing that if the Trump administration does impose a travel ban on Communist Party members, it would be abandoning one of the tools available to the US to promote “peaceful evolution” in China.

Economic decoupling is undeniably more painful for China than for the US. But unlike Japan during WWII, which was hit hard by the US oil embargo because of its lack of natural resources, China has no such problems. Given its large domestic market, losing the US as a major customer is not a disaster for China, and can be compensated through more dynamic economic activities at home. China can also make up for being freezed out of technological exchanges by turning to indigenous innovation.

As for the US, it can import goods from other developing countries, albeit less cheaply. The relative loss is acceptable when weighed against the heightened perception of economic independence and security.

Third, the ideological confrontation between China and the US is less intense than that during the Cold War. Unlike the obsession with ideology in those days, the line between capitalism and socialism is blurred today. The market economy has become universally recognised as the best way to promote economic growth and, politically, many countries have embraced democracy. Even North Korea calls itself the Democratic People’s Republic of Korea.

Although ideological hawks in the US still long for the day when the beacon of freedom will light up the world, after many years of fighting bloody wars overseas, most American people are not interested in promoting democracy abroad. Meanwhile, China just wants to preserve its political system and has no interest in exporting it to other countries, as the Soviet Union did.

Thus, ideological antagonism in China-US relations can easily be eased by calculations of realistic interests, which create conditions for compromise and cooperation.

Fourth, both China and the US have many options other than war to achieve their policy goals. While they have no allies to serve as a buffer, given the nature of the potential conflict in the South China Sea or Taiwan Strait, both countries are adept at operating in grey zones and fighting psychological, public opinion or diplomatic warfare below the threshold of war. The forced closure of the Chinese consulate in Houston by the US government is just the latest act of brinkmanship.

In addition, given China’s huge economic and financial interests in the US, the latter can wield the stick of sanctions when use of force is highly risky or not worth it. When both sides have many tools and options, why would they rush to war to achieve their goals?

Last but not least, the imbalance of power will act as a deterrent. Some say the US and Soviet Union did not fight a hot war because they were evenly matched. It was not the case, actually. At the beginning of the Cold War, the Soviet Union was at a relative military disadvantage.

Moreover, a country needs the will to fight before going to war, even if it is stronger militarily than its adversary. Having fought years of meaningless wars, the US is weary of war.

China, too, abhors war. Having a clear understanding of US strength, especially when its own economy is slowing down and it is facing various domestic challenges, China would not wish to recklessly start a war with the US.

In summary, the possibility of a hot war between China and the US is very small. The greatest danger for China is not a cold or hot confrontation with the US, but policymakers’ interpretation of the momentary hostility towards Beijing of a portion of the American population and the larger world. An erroneous interpretation could end China’s march to further opening up, and see it turn instead towards self-isolation.

### No China War---2NC

#### No US-China war

Charles C. Krulak & Alex Friedman 21, former President of Birmingham-Southern College, former Commandant of the US Marine Corps, M.S. from George Washington University; former Chief Financial Officer of the Bill & Melinda Gates Foundation, J.D. from Columbia University, “The US and China Are Not Destined for War,” Project Syndicate, 08-17-2021, https://www.project-syndicate.org/commentary/us-china-not-destined-for-war-by-charles-c-krulak-and-alex-friedman-1-2021-08

True, throughout history, when a rising power has challenged a ruling one, war has often been the result. But there are notable exceptions. A war between the US and China today is no more inevitable than was war between the rising US and the declining United Kingdom a century ago. And in today’s context, there are four compelling reasons to believe that war between the US and China can be avoided.

First and foremost, any military conflict between the two would quickly turn nuclear. The US thus finds itself in the same situation that it was in vis-à-vis the Soviet Union. Taiwan could easily become this century’s tripwire, just as the “Fulda Gap” in Germany was during the Cold War. But the same dynamic of “mutual assured destruction” that limited US-Soviet conflict applies to the US and China. And the international community would do everything in its power to ensure that a potential nuclear conflict did not materialize, given that the consequences would be fundamentally transnational and – unlike climate change – immediate.

A US-China conflict would almost certainly take the form of a proxy war, rather than a major-power confrontation. Each superpower might take a different side in a domestic conflict in a country such as Pakistan, Venezuela, Iran, or North Korea, and deploy some combination of economic, cyber, and diplomatic instruments. We have seen this type of conflict many times before: from Vietnam to Bosnia, the US faced surrogates rather than its principal foe.

Second, it is important to remember that, historically, China plays a long game. Although Chinese military power has grown dramatically, it still lags behind the US on almost every measure that matters. And while China is investing heavily in asymmetric equalizers (long-range anti-ship and hypersonic missiles, military applications of cyber, and more), it will not match the US in conventional means such as aircraft and large ships for decades, if ever.

A head-to-head conflict with the US would thus be too dangerous for China to countenance at its current stage of development. If such a conflict did occur, China would have few options but to let the nuclear genie out of the bottle. In thinking about baseline scenarios, therefore, we should give less weight to any scenario in which the Chinese consciously precipitate a military confrontation with America. The US military, however, tends to plan for worst-case scenarios and is currently focused on a potential direct conflict with China – a fixation with overtones of the US-Soviet dynamic.

This raises the risk of being blindsided by other threats. Time and again since the Korean War, asymmetric threats have proven the most problematic to national security. Building a force that can handle the worst-case scenario does not guarantee success across the spectrum of warfare.

The third reason to think that a Sino-American conflict can be avoided is that China is already chalking up victories in the global soft-power war. Notwithstanding accusations that COVID-19 escaped from a virology lab in Wuhan, China has emerged from the pandemic looking much better than the US. And with its Belt and Road Initiative to finance infrastructure development around the world, it has aggressively stepped into the void left by US retrenchment during Donald Trump’s four-year presidency. China’s leaders may very well look at the current status quo and conclude that they are on the right strategic path.

Finally, China and the US are deeply intertwined economically. Despite Trump’s trade war, Sino-American bilateral trade in 2020 was around $650 billion, and China was America’s largest trade partner. The two countries’ supply-chain linkages are vast, and China holds more than $1 trillion in US Treasuries, most of which it cannot easily unload, lest it reduce their value and incur massive losses.

To be sure, logic can be undermined by a single act and its unintended consequences. Something as simple as a miscommunication can escalate a proxy war into an interstate conflagration. And as the situations in Afghanistan and Iraq show, America’s track record in war-torn countries is not encouraging. China, meanwhile, has dramatically stepped up its foreign interventions. Between its expansionist mentality, its growing foreign-aid program, and rising nationalism at home, China could all too easily launch a foreign intervention that might threaten US interests.

Cyber mischief, in particular, could undercut conventional military command-and-control systems, forcing leaders into bad decisions if more traditional options are no longer on the table. And Sino-American economic ties may come to matter less than they used to, especially as China moves from an export-led growth model to one based on domestic consumption, and as two-way investment flows decline amid escalating bilateral tensions.

A “mistake” on the part of either country is always possible. That is why diplomacy is essential. Each country needs to determine its vital national interests vis-à-vis the other, and both need to consider the same question from the other’s perspective. For example, it may be hard to accept (and unpopular to say), but civil rights within China might not be a vital US national interest. By the same token, China should understand that the US does indeed have vital interests in Taiwan.

The US and China are destined to clash in many ways. But a direct, interstate war need not be one of them.

#### No US/China War

* Diplomacy, institutional ties, and economic flows have expanded
* Tensions and criticism occur against a cooperative backdrop
* Far lower military spending than cold war
* Nukes kept at low alert
* Water barriers limit escalation and build in negotiation time because of low force numbers and unclear barriers – can’t conquer anything
* Other countries act as buffers
* Ideologically against conflict

Dr. Joshua Shifrinson 19, Assistant Professor of International Relations at Boston University. The ‘new Cold War’ with China is Way Overblown. Here’s Why. 2/8/2019. https://www.washingtonpost.com/news/monkey-cage/wp/2019/02/08/there-isnt-a-new-cold-war-with-china-for-these-4-reasons/?noredirect=on&utm\_term=.f8ca8195c4e4]

Is a new Cold War looming — or already present — between the United States and China? Many analysts argue that a combination of geopolitics, ideology and competing visions of “global order” are driving the two countries toward emulating the Soviet-U.S. rivalry that dominated world politics from 1947 through 1990.

But such concerns are overblown. Here are four big reasons why.

1. The historical backdrops of the two relationships are very different

When the Cold War began, the U.S.-Soviet relationship was fragile and tenuous. Bilateral diplomatic relations were barely a decade old, U.S. intervention in the Russian Revolution was a recent memory, and the Soviet Union had called for the overthrow of capitalist governments into the 1940s. Despite their Grand Alliance against Nazi Germany, the two countries shared few meaningful diplomatic, economic or institutional links.

In 2019, the situation between the United States and China is very different. Since the 1970s, diplomatic interactions, institutional ties and economic flows have all exploded. Although each side has criticized the other for domestic interference (such as U.S. demands for journalist access to Tibet and China’s espionage against U.S. corporations), these issues did not prevent cooperation on a host of other issues. Yes, there were tensions over the past decade, but these occurred against a generally cooperative backdrop.

2. Geography and powers’ nuclear postures suggest East Asia is more stable than Cold War-era Europe

The Cold War was shaped by an intense arms race, nuclear posturing and crises, especially in continental Europe. Given Europe’s political geography, the United States feared a “bolt from the blue” attack would allow the Soviet Union to conquer the continent. Accordingly, the United States prepared to defend Europe with conventional forces, and to deter Soviet aggrandizement using nuclear weapons.

Unsurprisingly, the Soviet Union also feared that the United States might attack and wanted to deter U.S. adventurism. Concerns that the other superpower might use force and that crises could quickly escalate colored Cold War politics.

Today, the United States and China spend proportionally far less on their militaries than the United States and the Soviet Union did. Though an arms race may be emerging, U.S. and Chinese nuclear postures are not nearly as large or threatening: Arsenals remain far below the size and scope witnessed in the Cold War, and are kept at a lower state of alert.

As for geography, East Asia is not primed for tensions akin to those in Cold War Europe. China can threaten to coerce its neighbors, but the water barriers separating China from most of Asia’s strategically important states make outright conquest significantly harder. Of course, as scholars such as Caitlin Talmadge and Avery Goldstein note, crises may still erupt, and each side may face pressures to escalate. Unlike the Cold War, however, U.S.-Chinese confrontations occur at sea with relatively limited forces and without clear territorial boundaries. This suggests there are countervailing factors that may give the two sides room to negotiate — and limit the speed with which a crisis unfolds.

3. The Cold War had just two major powers

The Cold War took place in a bipolar system, with the United States and Soviet Union uniquely powerful, compared with other nations. This dynamic often pushed the United States and the U.S.S.R. toward confrontation and contributed to more or less fixed alliances; moreover, it encouraged efforts to suppress prospective great powers, such as Germany.

In 2019, it’s not at all clear we are back to bipolarity. Analysts remain divided over whether the U.S. unipolar era is waning (or is already over) — and, if so, whether we are heading for a new period of bipolarity, modern-day multipolarity or something else. Regardless, most analysts accept that other countries will play a central role in East Asian security affairs.

Russia, for example, still benefits from legacy military investments, India is developing economically and militarily, and Japan is beginning to build highly capable military forces to complement its still-significant economic might. Even if these nations aren’t as powerful as the United States or China, their presence makes for more fluid diplomatic arrangements and more diffuse security concerns than during the U.S.-Soviet competition. The resulting security dynamics are therefore likely to look very different.

4. Ideology plays less of a role in U.S.-Chinese relations

Many people see the Cold War as an ideological contest between U.S.-backed liberalism and Soviet-backed communism. But that’s not the whole story.

The early 20th century saw liberalism, communism and fascism vie for ideological preeminence. With fascism defeated alongside Nazi Germany, the postwar stage was set for a struggle between communism and liberalism to reinforce the U.S.-Soviet contest. That each ideology claimed universal scope ensured that the ideologies served as rallying cries for Third World conflicts, which were subsequently associated with the U.S.-Soviet struggle.

The respective “ideologies” of the United States and China do not favor this type of contest today. Indeed, analysts calling for a hard-line stance against China have faced difficulties even identifying a coherent Chinese ideological alternative. And while some researchers claim that a nascent ideological contest pitting an “autocratic” China against the “liberal” United States is emerging, this narrative ignores the political contests that shape Chinese politics (and have parallels in U.S. politics). Autocracies and democracies often cooperate. And on one important ideological issue — how they organize their economic lives — China and the United States have both embraced economic growth via trade, the private sector and semi-free markets.

### No Middle East War---1NC

#### Middle East war is more unlikely than ever

Mara Karlin 19, International Studies Professor at John Hopkins University, Nonresident Senior Fellow at the Brookings Institution, and U.S. Deputy Assistant Secretary of Defense for Strategy and Force Development 2015-2016, & Tamara Cofman Wittes, a Senior Fellow in Foreign Policy at the Brookings Institution and U.S. Deputy Assistant Secretary of State for Near Eastern Affairs from 2009-2012, America’s Middle East Purgatory: The Case for Doing Less, Foreign Affairs, January/February 2019, 98(1)

LESS RELEVANT REGION In response to the Iraq war, the United States has aimed to reduce its role in the Middle East. Three factors have made that course both more alluring and more possible. First, interstate conflicts that directly threatened U.S. interests in the past have largely been replaced by substate security threats. Second, other rising regions, especially Asia, have taken on more importance to U.S. global strategy. And third, the diversification of global energy markets has weakened oil as a driver of U.S. policy. During the Cold War, traditional state-based threats pushed the United States to play a major role in the Middle East. That role involved not only ensuring the stable supply of energy to Western markets but also working to prevent the spread of communist influence and tamping down the Arab-Israeli conflict so as to help stabilize friendly states. These efforts were largely successful. Beginning in the 1970s, the United States nudged Egypt out of the pro-Soviet camp, oversaw the first Arab-Israeli peace treaty, and solidified its hegemony in the region. Despite challenges from Iran after its 1979 revolution and from Saddam Hussein’s Iraq throughout the 1990s, U.S. dominance was never seriously in question. The United States contained the Arab-Israeli conflict, countered Saddam’s bid to gain territory through force in the 1990–91 Gulf War, and built a seemingly permanent military presence in the Gulf that deterred Iran and muffled disputes among the Gulf Arab states. Thanks to all these efforts, the chances of deliberate interstate war in the Middle East are perhaps lower now than at any time in the past 50 years.

### No Middle East War---2NC

#### No Middle East war---deterrence.

Helena Cobban 19, MA, Senior Fellow at the Center for International Policy, 10-13-2019, "Mutual Deterrence: Good for the Middle East, Bad for the Nuclear Weapons Industry?", LobeLog, https://lobelog.com/mutual-deterrence-good-for-the-middle-east-bad-for-the-nuclear-weapons-industry/

Over the past three-plus months it has become increasingly clear that, despite the bombast that Pres. Donald Trump has hurled against the Islamic Republic of Iran (along with a full deck of extremely harmful sanctions and some cyber attacks), neither he nor his closest regional allies in the anti-Iran coalition have been willing to escalate to any military attack against Iran that could escalate to all-out war.

Might the Middle East now be seeing the emergence of a situation of mutual deterrence that could bring it some much-needed stability — and that could also put the long-vaunted “value” of nuclear weapons into deep question?

Let’s do a quick recap. On June 20, Iranian forces shot down a large U.S. Reaper Hawk drone that had almost certainly ventured into Iranian airspace. The military reaction from the United States, Saudi Arabia, Israel, and the United Arab Emirates? As I noted here a few weeks later: goose egg. Then on September 14, either Iranian allies or Iran itself launched a large-scale, stunningly intricate attack against Saudi Arabia’s oil complex at Abqaiq. More goose egg.

Along the way, in late August, Israel killed two fighters affiliated with Iran’s Lebanese ally, Hizbullah, in Syria and sent explosive drones against two Hizbullah-related targets inside Lebanon. The Hizbullah chief warned publicly that the organization would retaliate against Israel. Israel’s response? Its military leaders organized a very public withdrawal of their forces from a strip along the country’s northern border with Lebanon. Then, after Hizbullah indeed launched a quick missile strike against an Israeli military vehicle fleeing deeper into Israel, the Israelis’ only response was to shoot a few pieces of ordnance, seemingly at random, into uninhabited parts of southern Lebanon.

In an analysis of the incident and its background that I published September 5, I noted that, “the situation of reciprocal (if highly asymmetrical) deterrence that has existed between Israel and Hizbullah since … 2006 remains in place.”

Now, in the aftermath of the Abqaiq attacks, it is clearer than ever that a situation of mutual (if asymmetrical) deterrence exists not just between Israel and Hizbullah over the Lebanon-Israel border, but also more broadly in the region between Israel and Hizbullah’s backers in Iran.

In Israel, nuclear scientist Uzi Even recently assessed the capabilities the Iranians or their allies revealed during the Abqaiq attack:

The Iranian technology is reliable and advanced, and the Iranians are capable of producing and operating simultaneously a large number of drones and cruise missiles.

He argued that,

Either the Saudi defense system failed or communication between the Iranian missiles was hidden and hard to discover. Either way, the attack was successful and effective… The Iranians, or their proxies, showed that they can hit specific targets with great precision and from a distance of hundreds of kilometers. We have to accept the fact that we are now vulnerable to such a strike. Yes, we can also carry out such strikes and perhaps inflict great damage on them, but so what? Does rational deterrence always work in the Middle East?

He also argued that,

above all… operation of [Israel’s] Dimona nuclear reactor should be halted. It has now been shown to be vulnerable, and the harm it could cause would likely exceed its benefits.

For the staunchly pro-war and pro-Israel New York Times columnist Thomas Friedman, the main takeaway from Even’s analysis was that:

Israel has been signaling two things to Hezbollah and Iran. One is that in response to any missile attacks, Israel will carpet bomb neighborhoods in Lebanon where Hezbollah’s families live and where it manufactures the missiles, and turn them into rubble, as it did on a small scale in 2006. And it will make the Lebanese economy collateral damage.

And the other is that Israel will attack Tehran directly, either with precision long-range missiles from Israel or submarine-launched missiles from the Persian Gulf, with this message: “Every time Tel Aviv is hit by your proxies, we will hit Tehran. You will not sit out this war. And you will not out-crazy us.”

Notably, neither of these “signals” seemed to be ones that Friedman disagreed with, or had any problem with. But his analysis of the crucial war that Hizbullah and Israel fought in 2006 also seemed badly askew: the bombing that Israel carried out that year of the “neighborhoods in Lebanon where Hizbullah’s families live” — and indeed, of numerous key elements of the country’s vital national infrastructure — was extremely far from “small-scale.” It was truly monumental. Yet Hizbullah not only survived it, it survived it with its standing in Lebanon’s political system significantly enhanced and with the Israeli ground units that had attempted a broad invasion of the country racing back as fast as they could to Israel with their tails between their legs.

Hizbullah’s performance in 2006 reaffirmed to all objective observers that a situation of reciprocal (if asymmetrical) deterrence existed between it and Israel — and it achieved that by having only relatively “dumb” weapons at its command. Friedman was right to warn that with the much smarter surveillance and guidance systems now presumably at its command, Hizbullah’s ability to project targeted threats against vital Israeli infrastructure is almost certainly much, much higher.

Friedman’s conclusion was that the demonstrations that Iran and its allies (whether in Lebanon, Yemen, or elsewhere) have given in the past few months of the high level of their targeting and command-and-control capabilities have made the Middle East a considerably more dangerous place:

[T]he Middle East may look calm right now, but that’s an illusion. Everyone is recalculating: The Iranians are emboldened, the Arabs are frightened and Israel and Iran are one miscalculation away from a war of precision missiles that neither can afford.

I question this conclusion, which seems unthinkingly Israelocentric. After all, for 40 years of the US-Soviet Cold War, the situation of reciprocal deterrence and “Mutually Assured Destruction” (MAD) between the world’s two largest, nuclear-armed superpowers gave a measure of strategic calm to a world still reeling from the two globe-girdling wars of the first half of the 20th century. (True, there were lots of nations in the Global South that suffered in that era.)

But why would we think that in the Middle East of the second quintile of the 21st century, a situation of Mutual Intraregional Deterrence (MID) would be any more destabilizing than the Cold War’s MAD was at the global level?

Indeed, the actual situation of being deterred that Israel, Saudi Arabia, the United States, and the UAE have all evinced in recent months — at the hands of the non-nuclear-weapons state Iran and its allies in the region — is the most intriguing aspect of the current situation. Bearing in mind that two of those powers, Israel and the United States are both well-endowed nuclear powers, what does this tell us about the utility of nuclear weapons in today’s world? A subject for another day…

#### No Middle East war and no great power involvement

Ekaterina Stepanova 16, researcher at the Institute of World Economy and International Relations, Summer 2016, “Russia in the Middle East: Back to a “Grand Strategy” – or Enforcing Multilateralism?,” http://www.cairn-int.info/article-E\_PE\_162\_0023--russia-in-the-middle-east.htm

In contrast to the 20th century and the early years of the 21st century, the regional crisis in the 2010s developed at a time when, overall, the role and leverage of major powers external to the Middle East, as either active meddlers or security guarantors in the region, or both, actually declined rather than increased. The United States serves as the most evident case in point: the “post-interventionist” US administration has clearly become “tired of the Middle East”, struggling and often failing to keep pace with the dynamically changing situation and unable to alter or decisively affect the course of events. The same even more strongly applies to the European powers. In terms of activity and impact, regional actors (Iran, Saudi Arabia, Qatar, UAE and Turkey) increasingly appeared to outplay external powers and influence.

For external powers, however, that did not remove a number of risks and threats connected to, or emanating from, the Middle East. The increase and diversification of global energy supply and the latest crisis in energy prices made the region less central to the global economy than it had been in the past. At the same time, the fundamental socio-political, statehood and security crisis in the Middle East brought with it new security concerns and implications. They mostly stemmed from reinforced perceptions about the long-term nature of regional instability, the continuing potential for further destabilization, and the related consequences and implications beyond the region, ranging from terrorist connections to migration flows. These challenges affect external powers unevenly. For instance, the role of the Iraq-Syria area as the main focal point for global terrorism activity and magnet for transnational flows of violent extremists in the mid-2010s poses a threat to everyone (but mostly to the countries of the region itself, as well as to those in Europe and Eurasia). In contrast, the avalanche of refugee and migrant flows from the Middle East primarily targets Europe (rather than North America, Eurasia, or other regions).

Until recently, the main type of response by key (Western) external powers to turbulent developments in the Middle East, while not amounting to a hands-off approach, boils down to limited containment. Examples range from limited air strikes against “Islamic State” positions in Iraq and Syria, carried out by the US-led coalition since 2014, to the 2013 deal on Syria’s chemical disarmament co-brokered by the United States and Russia. Not surprisingly, this limited-containment approach has had equally limited results for Syria, Iraq and the region – as well as for the West itself (as shown, e.g., by the persistent migrant flows and accelerating terrorist attacks in Europe). Despite the growing centrality of the Middle East to global politics and security, and its more direct impact on and ties to the West, this damage limitation course taken by key external actors has not been very different from, e.g., the approach taken by the United States and its Western allies (and also by Russia and China) to the Afghanistan problem in recent years.

### No Turkey Aggression---1NC

#### Interdependence and fears of backlash check Turkey aggression

Paul Taylor 20, contributing editor at POLITICO, writes the “Europe At Large” column, senior fellow at the think-tank Friends of Europe, “How rogue can Turkey go?,” POLITICO, 1/1/20, https://www.politico.eu/article/turkey-rogue-state-recep-tayyip-erdogan/

There is no mechanism for expelling an errant NATO member. The alliance in the past turned a blind eye to military regimes in Greece and Turkey. But diplomats say pragmatic ways would be found to work around Ankara if it cannot be persuaded to mothball the Russian air defense system.

On the political front, the EU could in theory pull the plug on Turkey’s accession negotiations, which are going nowhere given Erdoğan’s assault on judicial independence, media freedom and civil rights since he survived a failed 2016 military coup. But to do so would risk triggering another refugee influx into Europe and do severe damage to an economic relationship important for both sides. Germany would strongly oppose any such move.

A more potent check on Turkish disruption, at least in the short term, could be Erdoğan’s own ambitions.

The Turkish leader needs to maintain a regular flow of foreign investment to steady the economy and reassure the urban middle class that his first decade of prosperity helped to swell.

His political dream is to crown two decades of AKP rule by refounding the Turkish Republic as the new Atatürk on the 100th anniversary of its creation in 2023.

That gives Western officials reason to hope that Erdoğan will hold off escalating his confrontations to the point of crisis. For now, anyway.

### No Turkey Aggression---No Entrapment

#### Zero chance of entrapment---NATO would simply refuse aid

Michael Moran 16, Visiting Media Fellow and author of The Reckoning: Debt, Democracy and the Future of American Power, “Turkey’s Article 5 Argument Finds No Takers,” Carnegie Corporation of New York, 2-24-2016, https://www.carnegie.org/news/articles/turkeys-article-5-argument-finds-no-takers/

The ferocity of the fighting between Syria’s government forces and various proxies vying for control of territory and resources has Turkey on edge and has already led to several deadly clashes involving the only NATO member state bordering the civil war.

With Turkey, Russia, Iran, Iraq, and Gulf states pursuing their own, often conflicting aims in Syria, all against the backdrop of a U.S.-led air and commando campaign against the Islamic State (IS), there is renewed concern at NATO’s headquarters in Brussels that Turkey could see the next flare-up as grounds for citing Article 5: in effect, demanding that its NATO allies deploy forces and come to its collective defense.

Turkey has already invoked the lesser-known Article 4—a demand for an emergency consultation of the alliance—following the downing of a Turkish warplane under disputed circumstances last spring. Incidents like this and the threat that Bashar Assad’s forces might launch Scud missiles into Turkey led NATO members—the United States, Germany, and Spain—to deploy Patriot anti-aircraft missiles along the border in early 2013, though the German and American batteries have since been withdrawn. Spain’s—a less capable version of the Patriot—is geared towards anti-aircraft, as opposed to anti-ballistic missile defense, and therefore deemed more appropriate

But could a new incident—a missile strike, an IS incursion, or Syrian artillery bombardment across the border—bring the full might of NATO into the war? Many are skeptical, and for good reason.

The history of invocations of NATO’s Article 5 is short and somewhat underwhelming. In the 68 years of the North Atlantic alliance’s history, plenty of low-intensity conflicts involving NATO nations have raged, from rebellion in France’s Algerian departments, to the U.S. war in Vietnam, through the Balkan wars of the 1990s. Yet only once has Article 5’s “all-for-one, one-for-all” facility been invoked: that was September 12, 2001, the day after the al-Qaida attacks on the United States.

Even then, its effect was primarily symbolic. While the United States expressed its deep appreciation at the time, NATO involvement in Afghanistan would be minimal for years to come, though British, French, and a handful of other elite forces arrived as early as November that year. In practice, though, it was not until late 2003, when NATO assumed command of the International Security Assistance Force (ISAF), that alliance troops arrived in force, and even then often under restrictive rules of engagement that limited their effectiveness.

Indeed, ISAF, the force NATO led from August 2003 to December 2013, was a UN-sanctioned operation that included not only forces from NATO’s 28 militaries but troops and specialists from 48 states, including such disparate contributors as Mongolia, Tonga, and Singapore. At its height in 2010–11, ISAF numbered more than 42,000 troops, augmenting 100,000 U.S. troops.

Turkey would sorely like a commitment of that scale. Yet the subtle diplomatic realities of the North Atlantic alliance—as well as the very unsubtle nature of its own activity inside Syria—make this highly unlikely.

For one thing, Turkey’s own military has acted aggressively in targeting Syria’s Kurdish rebels, the People’s Protection Units, or YPG, which Ankara views as little more than a proxy for the outlawed separatist guerrillas of the Turkish Kurds, the Kurdistan Workers’ Party, or PKK. Last week, the Turks opened up on the Kurdish-held air base at Aleppo, in spite of the fact that the city is surrounded by forces loyal to Assad, the presumed enemy in Syria. The act enraged almost everyone. Russia demanded at an emergency Security Council meeting a censure of Turkey’s violation of Syrian sovereignty, and President Obama, who regards the Kurdish as the most reliable ground force in the fight against the IS, urged Turkish President Recep Tayyip Erdogan in an 80-minute phone call on February 19 to avoid provocative actions.

While NATO has taken no official position on the question of Article 5—not surprising, since no formal request has been made—through back channels the alliance has been telegraphing a resounding “no” to Turkey for weeks. Last week, Luxembourg’s Foreign Minister Jean Asselborn told Germany’s DerSpiegel that “NATO cannot allow itself to be pulled into a military escalation with Russia as a result of the recent tensions between Russia and Turkey.”

Whatever the fate of the current U.S.-push to secure a cease fire, a large NATO ground force, of the kind that deployed to Bosnia, Kosovo, and Afghanistan, is not on the table.

#### Especially if war was provoked by Turkey---allies would prevent Turkey from even invoking Article 5 by clarifying through backchannels that illegal aggression does not require military support

Thomas O. Falk 19, studied law in London before obtaining his M.A. in International Relations at the University of Birmingham, has been working as part of an international team that provides the European Commission and NATO with political news and developments, “Turkey and NATO's (Non) Conundrum of Article 5,” InsideOver, 10-20-2019, https://www.insideover.com/war/turkey-and-natos-non-conundrum-of-article-5.html

Turkey’s invasion of northern Syria has been met with criticism amongst European leaders. Some of which have openly floated the idea that Erdogan could seek the support of NATO if the conflict widened. It which would make a large proportion of European states accessories of Erdogan’s move under NATO’s Article 5 – only in theory, however.

Not unexpectedly, EU foreign ministers were unable to agree on a collective arms embargo against Turkey due to the invasion of Syria at their meeting in Luxembourg. The necessary unanimity was not achieved, several countries, especially Hungary, opposed the motion.

Instead, the EU states solely committed to “strong national positions with regard to their arms exports to Turkey”. Based on EU criteria that the stability of the region should not be endangered. What it amounts to is yet another display of a European Union divided on a message and utterly powerless on the actual matter.

Whether or not an arms embargo could have had an actual impact or had been political posturing in the first place, can certainly be debated. What cannot be debated any longer is that Turkey continues to advance its troops in Syria. Furthermore, while the ceasefire announced today has only delayed the issue, it is hard to believe that Erdogan will suddenly concede his grand strategy quest for a neo-Ottoman Empire.

As for the Europeans, Turkey’s actions so far carry more than just humanitarian connotation. A potential attack on Turkey by the Syrian army of allied actors in the conflict could lead to Turkey invoking NATO’s Article 5 – collective self-defence. Under Article 5, an attack against a NATO member is considered an attack against all, and so far, has only been utilised once in the Treaty’s history.

Nevertheless, invoking Article 5 does not automatically warrant unconditional support from the member states. Turkey would have to invoke Article 4 first. Under Article 4, any member state can convene a meeting with the other members to “consult”. Here, Turkey would have to make a case for why it feels that either its independence or security is in jeopardy.

Even in this scenario, however, chances of Erdogan’s proceeding to the next level (i.e. Article 5) seem inconceivable, and there are valid reasons for it.

First, the vast majority of NATO countries have already called on Ankara to retreat immediately after the invasion began. Besides, several NATO states timely pointed out the possible dangers of destabilisation of the entire region. Germany, the Netherlands and France have temporarily stopped selling arms to Turkey in protest, with Merkel and French President Emmanuel Macron condemning the Turkish invasion as an attack. Also, NATO Secretary-General Jens Stoltenberg stated last week he expects Turkey to act with restraint.

Second, for Article 5 to be invoked, attack and defence action need to be distinguished cleanly. All NATO states must, therefore, regard the military actions of Turkey in Syria as lawful under international law – which is reasonably unlikely also, particularly after the remarks that have been made and the rules laid out for self-defence under the Charta of the United Nations, Chapter VII, Article 51.

Considering these factors, the necessary unanimity for collective self-defence appears to be highly unlikely in almost any scenario. In fact, due to the international community’s resentment towards Turkey, a freeze of Turkey’s NATO membership seems more conceivable than other NATO members taking Turkey’s side on the battlefield.

## T---Security Cooperation

### OFF---1NC

#### T SECURITY COOPERATION:

#### “Security cooperation” requires DOD action---the plan is not the DOD.

Alexandra **Kerr 18**, Visiting Research Fellow at the National Defense University in the Center for Complex Operations, “Defense Institution Building in the U.S. Context,” Connections, Vol. 17, No. 3, [Italics in original]

Finally, in the U.S. government, “security cooperation” and “security assistance”—which are the chief lines of effort in the U.S. toolkit to help partners bolster their security and work with the United States to support common security objectives—are overlapping but not necessarily interchangeable. The distinction between “security cooperation” and “security assistance” activities has to do with the agency administering the program: in simplest terms, it is either an activity of the Department of Defense (security cooperation) or the Department of State (security assistance).

DOD and the Department of State (DOS) have shared responsibility for engaging with foreign partner militaries since the mid-twentieth century, with the bulk of congressional security assistance funding allocated to DOS. Any security assistance *administered* by DOD—whether funded under Title 10 (Armed Services) or Title 22 (Foreign Affairs) of the U.S. Code—is a “security cooperation” activity.21 After the terrorist attacks on September 11, 2001, the legal framework for the funding and administration of such activities evolved in response to emerging threats. Congress increasingly granted funding and authorities directly to DOD under Title 10 for security cooperation.22 Therefore, while DOS security assistance programs can include DIB components, the majority of DIB-specific programming is currently funded under and implemented by the Department of Defense and is thus considered security cooperation.

#### Voter for limits and ground---actor proliferation opens the floodgates on a bidirectional topic with three large areas and zero link uniqueness, but DOD action guarantees core agent counterplans and disads.

### O/V

**1. FUNCTION---** Only the DOD can do SC and other actors would make things more complicated and prevent the DOD from properly carrying out the SC activities. The plan violates this bc it doesn’t specifically include the DOD.

**2. TEXT-**-- Judge, choose our definition as it is better for fairness and education. Objectiveness creates hurdles for the neg in being able to respond properly and most effectively, which is not fair to us. In addition, vagueness is better for the topic in general because we are able to learn about more topics and it is overall better for education.

**SC---Requires DoD---2NC**

**Security Cooperation requires the DoD to be the source of funding**

**Fenell 11**, Captain, US Marine Corps, In Partial Fulfillment of the Requirements for the Degree MASTER OF ARTS in INTERNATIONAL STUDIES, at the UNIVERSITY OF SAN FRANCISCO (Nathan, “Security Cooperation Poorly Defined” December, <https://repository.usfca.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1020&context=thes>)//BB

Security cooperation is a compilation of financial, educational, and material resources, that at their foundation are supported by the United States, in particular the Department of Defense, and are used to support the peaceful development of democracies in foreign countries. The resources provided by the Department of Defense are available to foreign countries after the host nation requests the peaceful assistance of the U.S. military in response to systemic deficiencies in the bureaucratic management of a nation state or when a nation state recognizes that its military limitations prevent it from properly defending its geographic borders. The host nation’s request for support from the U.S. is typically an effort by the foreign country to develop its internal capacity to protect its people and limit internal or external threats. The security cooperation exercise Baltic Operation, held in Estonia, is an example of a foreign country using the resources 9 provided by the United States to improve its national defense capabilities in direct response to a perceived threat to its sovereign borders. In this scenario Estonia is attempting to develop its military capabilities and project an image of strength in an effort to maintain the freedom it earned, from Russia, at the conclusion of the Singing Revolution in 1992 and prevent a future Russian incursion across its borders. In contrast to this appropriate use and definition of security cooperation as a strategy to prevent conflict, the Obama Administration is using the term security cooperation as a way to define a national exit strategy from a two front war, a strategy that at its heart is based on the reconstruction of a damaged infrastructure. The false labeling of reconstruction operations as security cooperation is the foci of this thesis project.

**In addition, extend Kerr 18.**

Security cooperation and security assistance are distinct and are not interchangeable. They agree with this bc their own card says “SC and SA are not the same”

**It's strictly limited to DoD actions**

**Reynolds 19**, et al, Commandant, Defense Institute of Security Cooperation Studies (Ronald, “The Management of Security Cooperation,” <http://cebw.org/images/docs/Legislacao_Webinar/Greenbook_39_0.pdf)//BB>

Introduction to Security Cooperation

Introduction

The term security cooperation was first introduced in 1997 by the Defense Reform Initiative (DRI). At that time, the then named Defense Security Assistance Agency (DSAA) already had day to day management responsibilities of many security assistance programs authorized by the Foreign Assistance Act (FAA) and the Armed Export Control Act (AECA). The DRI proposed that DSAA also manage certain Department of Defense (DoD) funded international programs along with their personnel and associated resources. So that other U.S. government (USG) agencies, the private sector and foreign governments could better understand DSAA’s enlarged mission and diverse functions beyond security assistance (SA), DoD re-designated DSAA as the Defense Security Cooperation Agency (DSCA) effective 1 October 1998.

In recent years, DSCA has absorbed management responsibilities for many DoD international programs. In addition, DSCA leads the broader USG security cooperation enterprise. However, many security cooperation programs continue to be managed by other elements of the Office of the Secretary of Defense (OSD), the combatant commands (CCMDs) or the military departments (MILDEPs). What further complicated the management of security cooperation was that the in-country point of contact between the USG and the host nation generally is either the Defense Intelligence Agency (DIA) sponsored defense attaché office (DAO) or the DSCA sponsored security cooperation office (SCO). These two spigots for security cooperation with a country required a broad knowledge and skill baseline of the very different international programs that are initiated, funded, and managed throughout the DoD and its agencies and the MILDEPs. Most disconnects regarding SCO-DAO coordination of in-country security cooperation were generally resolved with the establishment of the Senior Defense Official-Defense Attaché (SDO/DATT) having oversight over both the SCO and DAO organizations. It was not until 9 June 2004 that DoD published a formal, yet still very broad, definition of security cooperation in Joint Pub 1-02:

All DoD interactions with foreign defense establishments to build defense relationships that promote specific U.S. security interests, develop allied and friendly military capabilities for self-defense and multinational operations, and provide U.S. forces with peacetime and contingency access to a host nation.

DODD 5132.03, DoD Policy and Responsibilities Relating to Security Cooperation, 29 December 2016, further defines security cooperation with assigned responsibilities:

All DoD interactions with foreign defense establishments to build defense relationships that promote specific U.S. security interests, develop allied and partner nation military and security capabilities for self-defense and multinational operations, and provide U.S. forces with peacetime and contingency access to allied and partner nations. This includes DoD administered security assistance programs.

**The most clear and specific definition conclusively requires the DoD**

**Reighard 6**, Lt Col in USAF (Robert, “SECURITY COOPERATION: INTEGRATING STRATEGIES TO SECURE NATIONAL GOALS,” USAWC STRATEGY RESEARCH PROJECT, https://apps.dtic.mil/sti/pdfs/ADA449543.pdf)//BB

Security cooperation has been a part of the U.S. Armed Forces for many years. In fact, historians reveal that the U.S. military has always engaged in security cooperation with other countries and their military forces. However, the term used to designate such activities is now “Security Cooperation,” a term that has evolved conceptually through various programs over the years. During the 1990s, the terms “engagement” and “shaping” were used without sufficient specificity; they were often used interchangeably, resulting in confusion that led to problems in both planning and execution. DOD thus adopted “Security Cooperation” in 2001. It included a broad range of military-to-military activities, but it also clarified roles and responsibilities. The term Security Cooperation thus describes a broad range of activities used by the Department of Defense in peacetime operations. These activities refer to all DOD interactions that are carried out with foreign defense establishments, such as combined exercises, combined training, combined education, military-to-military contacts, humanitarian assistance, and information operations.

**Budget classification proves it’s military-to-military**

**Van Eerden 20**, Captain (James, “Seeking Alpha in the Security Cooperation Enterprise A New Approach to Assessments and Evaluations,” Journal of Advanced Military Studies, 11.1)//BB

The Fiscal Year (FY) 2019 President’s Budget: Security Cooperation Consolidated Budget Display outlines seven categories of security cooperation activity, including military-to-military engagements, support to operations, and humanitarian and assistance activities, among others.6 The security cooperation framework traditionally includes security assistance (SA), security force assistance (SFA), and some aspects of foreign internal defense (FID).7 In the context of this article, the term security cooperation refers primarily to military-to-military engagements, where the U.S. military engages in training partner forces under the auspices of Title 10 and Title 22 authorities.

**Even the broadest definitions require the DoD**

**Williams 12**, Lt Col in Army National Guard (James, “The National Guard State Partnership Program: Element of Smart Power,” <https://apps.dtic.mil/sti/pdfs/ADA562110.pdf>)//BB

Similarly, the six Geographic Combatant Commanders (COCOMs) have underscored security cooperation and building partner capacity as essential to their respective Theater Strategy Plans and Country Campaign Plans in support of National Security objectives. In every COCOM posture statement the reader will find references 7 to the importance of the concepts of cooperation, engagement, and building partner capacity. “Security Cooperation” is defined broadly as interactions between the Department of Defense and foreign militaries that promote specific United States security interests; develop allied and friendly military capabilities; and provide the United States with both peacetime and contingency access to host nations.12 Typical security cooperation and engagement activities include military-to-military contact, coalition training, nation assistance and long term operations. These types of activities range from Navy ship port visits to combined training exercises, foreign military education, leader conferences, foreign military sales and counter-drug operations.

**Security Cooperation requires a military branch to be the implementing agency**

**Arnold 20**, colonel in USAF (Jason, “Add Value to Security Cooperation through Joint Unification,” FAO Journal of International Affairs, <https://faoajournal.substack.com/p/add-value-to-security-cooperation?s=r)//BB>

In the Security Cooperation Enterprise, the military departments loom large as the primary implementing agencies of Foreign Military Sales (FMS) cases, Building Partner Capacity (BPC) cases, and in training activities.[6] These SC programs provide our international partners with the capabilities they require both for their own security and to assist in regional security objectives that improve the overall global security situation. Most open SC cases have one of the military departments as an Implementing Agency (IA) and each service has built its own organizational structure, bureaucracy, and automated systems to support the effort.[7]

**SC---Prefer Our Interp---2NC**

**Given that basically any activity is included, the only functional limit on the topic must come at the agent-level**

**Mazarr 22**, senior political scientist at the RAND Corporation. Previously he worked at the U.S. National War College, where he was professor and associate dean of academics; as president of the Henry L. Stimson Center; senior fellow at the Center for Strategic and International Studies; senior defense aide on Capitol Hill; and as a special assistant to the Chairman of the Joint Chiefs of Staff (Michael, “Security Cooperation in a Strategic Competition,” RAND, <https://www.rand.org/pubs/research_reports/RRA650-1.html>)

To pursue this analysis, we first had to define the bounds of what we would assess. Official U.S. government definitions of security cooperation are very broad. One definition from the Defense Security Cooperation Agency states that security cooperation

comprises all activities undertaken by the Department of Defense (DoD) to encourage and enable international partners to work with the United States to achieve strategic objectives. It includes all DoD interactions with foreign defense and security establishments, including all DoD-administered Security Assistance (SA) programs, that build defense and security relationships; promote specific U.S. security interests, including all international armaments cooperation activities and SA activities; develop allied and friendly military capabilities for self-defense and multinational operations; and provide U.S. forces with peacetime and contingency access to host nations.3

Such definitions clearly include almost any security-related activity for any purpose. To scope the focus of the study, we reviewed official state documents and strategies and the literature on security cooperation to identify 11 types of activities:

1. military aid, which includes funding through the Foreign Military Financing (FMF) program, the Excess Defense Articles program, and other grants and loans

2. arms sales and transfers,4 such as U.S. arms sales through the Foreign Military Sales (FMS) and Direct Commercial Sales (DCS) programs

3. military capacity-building, such as U.S. activities under Section 1206 of the annual National Defense Authorization Act and Sections and 2282 and 333 of U.S. Code, Title 10 (the train and equip authority)

4. education and training, including international military education and training (IMET), professional military education (PME), and regional centers

5. personnel exchanges, such as U.S. activities under the Military Personnel Exchange Program and the State Partnership Program

6. military exercises, both bilateral and multilateral and those that involve foreign partners

7. access-related agreements, such as status of forces agreements (SOFAs) and agreements related to base access and information-sharing

8. armament-related agreements, such as those for co-development of systems and for research, development, test, and evaluation activities

9. sustainment of donor-nation equipment by the donor, the partner, or third parties

10. institutional capacity–building to strengthen the partner institutions that support security services

11. humanitarian assistance and disaster relief (HA/DR), which offers support for efforts to relieve suffering.

These categories offered a consistent template for gathering data across our various study components. A major challenge was that reliable and consistent data on each of the 11 categories were not available for all the competitors—not even for the United States. Especially at the unclassified level, there is simply no comprehensive roster of security cooperation activities by the United States, and neither China nor Russia publishes inclusive data sets of its programs. An additional challenge was that, in some cases, the different countries define the categories somewhat differently, so we could not develop data on entirely comparable sets of security cooperation activities.

**AFF GROUND-**-- extend our Fenell 11 card.

**NEG GROUND---** including other actors complicates things as was stated in the overview.

**GRAMMAR**--- While it is true that the USFG isn’t only the DOD, the plan can only BE carried out by the DOD so the actor is unnecessarily large and doesn’t solve anyway.

**REASONABILITY---** Good enough doesn’t work for the neg bc it explodes the topic, and we will only be able to respond with generic arguments. This means that the aff has an unfair advantage which is bad for debate overall.

# LEFTOVERS

#### Cyber arms racing destabilizes deterrent relationships

Andreas Wenger & Myriam Dunn Cavelty 22, Wenger is professor of international and Swiss security policy at ETH Zurich and director of the Center for Security Studies (CSS), Switzerland; Cavelty is deputy head of research and teaching at the Center for Security Studies (CSS), ETH Zurich, Switzerland, “Conclusion,” Cyber Security Politics, 1st ed., Routledge, 01/18/2022, pp. 239–266 DOI.org (Crossref), doi:10.4324/9781003110224-18

Emerging technologies and the future of cyber security politics

Ever since cyber security issues have appeared on the agenda of national and international politics, Jon R. Lindsay (2022) argues in his chapter on the ambiguity of a cryptologic advantage, two analytically distinct perspectives have informed the debate about their relevance for cyber security politics. A first perspective builds on the premise that technology determines politics. Anticipating the transformative potential of emerging technologies, this view tends to extrapolate dramatic consequence for security politics. We have already reviewed early expert assumptions along the line that the nature of cyberspace is destabilizing and favors the offense. A second perspective starts from the opposite end of the relationship and assumes that politics determines technology. Such an analytical perspective translates into expectations that the sociopolitical context mitigates the supposed advantages of cyber offense and reinforces established power relationships (cf. Dunn Cavelty and Wenger 2019).

We argue throughout the volume that a perspective that combines the two views and unpacks the co-constitution and co-dependency of technology and politics provides a more productive analytical lens for studying the ambiguous implications of rapid technological change on cyber security politics and vice versa. Within this context, the chapters in this volume discuss three key insights on the interrelationship between emerging technologies and the future of cyber security politics. A first subsection concentrates on tech race dynamics as drivers of cyber threat perceptions. The focus here is on the interplay between global market and geopolitical dynamics under multidimensional uncertainty and how these dynamics feed into threat narratives. A second subsection highlights that the sociopolitical context conditions the strategic utility of emerging technologies. Here the focus is on how social and institutional factors shape the influence that emerging technologies have on the balance between the offense and the defense. A third subsection deals with the growing role of private actors in digital innovation in general and in securing cyberspace more specifically. The focus here is on how the multiplication of actors increases the socio-technical uncertainty and the sociopolitical ambiguity of the governance space around emerging technologies.

Tech race dynamics as drives of cyber threat perceptions

The dynamic and emergent trajectory of technology development is a key factor shaping the interplay between technology and politics. Multidimensional uncertainty – about the scope and tempo of the technological development and about market dynamics and social acceptance – is a key driver of the innovation process (see Figure 16.1). Technology firms are exposed to market pressures and driven by profit. They make their design and development decisions, including complex trade-offs between the performance and the safety and transparency of their products and services, in the shadow of a potential first-mover advantage and the promise of huge economies of scale. Conversely, governments influence the innovation process via the formulation and implementation of technology strategies that specify national levels of ambition. Such strategies aim at incentivizing the domestic uptake of new technologies and creating a regulatory environment that fits their societies’ institutional and normative contexts while positioning their countries in the best possible way in the emerging global innovation space (Bonfanti 2022).

As new technological possibilities – linked to the development of artificial intelligence, quantum computing, or space technologies – appear on the horizon, both governments and corporations focus on their potentially transformative capacities, and, more specifically, anticipate what role these technologies will play in shaping cyber security. Most technologies discussed in the chapters of this volume are dualuse technologies and as such might influence the global economic and military balance. As a consequence, great powers tend to treat such technologies as a potential strategic resource. Out of these technical, economic, and (geo)political dynamics an ambiguous political interaction dynamic evolves that fits the logic of the security dilemma (Jervis 1978): The means – in this case maneuvring to attain or sustain an advantage in critical technologies – by which a state tries to maximize its national interests and security threatens the interests and relative security of other states.

From a political perspective, it is problematic if the technology development process is dominated by only a few dominant economic (global tech firms) and political actors (great powers). A concentration of technical resources in the hands of a few actors might affect the global distribution of economic and military power and create or deepen asymmetric economic and political dependencies. A context of an intensifying technology competition creates incentives for states to influence the innovation process and the proliferation of new technology in their narrow national interest (Fischer and Wenger 2019). Conversely, technology race dynamics act as drivers of national threat perceptions and tend to feed doom scenarios. State actors see themselves increasingly caught in a global race for AI or quantum dominance (Lindsay 2022; Bonfanti 2022). From the perspective of science and technology studies, such threat narratives are co-constituted by the micro-politics of design decisions in competitive global markets and the macropolitics of great powers that act strategically in a competitive international system (Fischer and Wenger 2021).

The strategic utility of emerging technologies depends on the sociopolitical context

The insight that the balance between offense and defense in intelligence has always depended more on institutional factors and strategic context than on technological architecture represents the key message of Chapter 6 in this volume. Analyzing the tumultuous relationship between cryptologic technology and political advantage, Jon R. Lindsay (2022) highlights the fundamental political paradox between cryptography (code-making) and cryptanalysis (code-breaking): They must cooperate to compete and respect the constraints of a cooperatively produced cryptosystem. As a consequence, cryptology turns into an organizational contest and as such heavily depends on social factors. It does not come as a surprise against this background that one of the central insights of cryptologic history is that “gullible humans are the Achilles Heel of classical cryptology” (Lindsay 2022: 89). This again, Lindsay argues, makes it reasonable to expect that humans “will also be the undoing of quantum cryptology” (Lindsay 2022: 89).

A working quantum computer should be able to crack the current cryptographic protocols that are vital for cyber security. Anticipating a one-sided technological breakthrough easily translates into fear that a breakthrough in quantum computing might compromise the existing public key infrastructure. As China began to heavily invest into quantum technology, a threat narrative evolved in Western states that perceived the great powers to be locked into a global race to gain a quantum advantage. A quantum breakthrough would have major repercussion for security and defense, so the arguments went, since one’s own intelligence would be locked out while the first-movers’ communication would become impenetrable. Should this indeed happen, policymakers and strategists feared, global stability could be at risk.

Yet the implications of the interaction between technology and politics will likely be more ambiguous, Lindsay argues. First, such a perspective overlooks that the search for quantum safe protocols begins parallel to the development of a quantum computer that would be able to break the current cryptographic protocols. Second, quantum computing would not change the reliance of cryptology on social factors. Intelligence remains fundamentally a contest between human organizations. The current golden age of cyber espionage was not enabled by a mathematically and technically weak public key infrastructure. It can be traced back to an overly complex organizational setup of the infrastructure and poor cyber hygiene among computer users. Third, even if one side in a geopolitical contest would develop a cryptographic advantage, how this advantage would translate into a political outcome is not predetermined by technology. Rather it would be contingent on the overarching strategic context and the specifics of institutional decision-making. A cryptanalytic success, Lindsay notes, can make a bargain more likely or a surprise attack more attractive, and it may even provide a false sense of security.

In his chapter, Matteo E. Bonfanti (2022) in a similar vein discusses the implications of emerging AI technologies for the offense–defense balance in cyber security. These implications are difficult to predict, he argues, because the context is characterized by widespread uncertainty and ambiguity. Most AI tools can be used in support of both cyber defense as well as cyber offense. AI-based cyber capabilities will affect both the logical (software) dimension as well as the semantic (content) dimension of cyberspace. That AI will have major implications for cyber security is undisputed among experts. Yet who will be the winner – offense or defense, states security agencies or private threat intelligence firms, democracies or autocracies – remains to be seen. The eventual outcome of the integration of AI technologies into cyber security depends on the strategic and sociopolitical context and the risk-benefit calculations of many different public and private cyber security stakeholder.

#### Cyberdeterrence fails because of signaling uncertainty

Andreas Wenger & Myriam Dunn Cavelty 22, Wenger is professor of international and Swiss security policy at ETH Zurich and director of the Center for Security Studies (CSS), Switzerland; Cavelty is deputy head of research and teaching at the Center for Security Studies (CSS), ETH Zurich, Switzerland, “Conclusion,” Cyber Security Politics, 1st ed., Routledge, 01/18/2022, pp. 239–266 DOI.org (Crossref), doi:10.4324/9781003110224-18

Strategic stability under multidimensional uncertainty

The assumed revolutionary potential of cyberspace, Miguel A. Gomez and Christopher Whyte (2022) note in their chapter, was the product of the twin uncertainties about the scope and tempo of the technical innovation and the related social and political responses. As new technological possibilities emerged, politics began to catch up in a process of sociopolitical normalization. As a consequence, state behavior evolved over time. In the absence of a demonstrable strategic utility of cyber operations and a strategic context characterized by a puzzling co-existence of restraint at the high end of conflict and persistent low-level cyber conflict, key states started to increasingly move away from deterrence to cyber conflict management. In 2018, the United States issued a new cyber strategy signaling a shift to persistent engagement and defend forward. The logic of the new approach emphasized that the characteristics of the operational environment in cyberspace – a space of constant contact – demand a continuing engagement and degradation of adversarial cyber capabilities and operations wherever they were found (US Cyber Command 2018; US Department of Defense 2019).

This shift away from deterrence might be premature and underestimate the potential of (unintended) escalation, Gomez and Whyte argue. Moreover, it is still unclear why states invest substantial technical, financial, and organizational resources in using the domain offensively if cyber operations are indeed of limited strategic utility only. Within this context, the chapters in this volume focus on three interconnected aspects of upholding strategic stability under multidimensional uncertainty. A first subsection concentrates on the micro-dynamics of decision-making that might drive escalation under uncertainty and ambiguity. The focus here is on how prior beliefs and cognitive biases might influence the response decisions of elite stakeholders in varying national strategic cultures. A second subsection deals with the ambiguities of attribution as a precondition for a credible deterrence threat. The focus here is on how policymakers perceive cyberspace as a completely human-built domain and how this translates into political apprehension about the applicability of deterrence in cyberspace. A third subsection analyzes the growing role of intelligence in cyberspace. The focus here is on how the digitalization of intelligence changed its strategic and operational role and what (un)intentional consequences this had for cyber insecurity, on the one hand, and for great powers’ views on (un)acceptable behavior of intelligence services in cyberspace, on the other.

Escalation: The micro-dynamics of decisionmaking in varying sociopolitical contexts

Precisely because it is difficult to control the strategic effects of cyber (influence) operations, more research is needed on the micro-dynamics of decision-making that may drive unintended escalation. Contributing to the behavioral turn in cyber security research, Miguel A. Gomez and Christopher Whyte (2022) investigate the effects of uncertainty on judgment in the context of (crisis) decision-making under cyberattack. In such situations, the ambiguity of diffuse actors and malicious actions increases the uncertainty of decision-makers about both the intent behind and the consequences of cyber (influence) operations. The authors use war gaming as a pseudo-experimental method to determine if and how decision-makers use well-known heuristic mechanisms such as prior beliefs and analogical reasoning to discern intent and consequences behind cyber operations. The authors find distinct evidence in support of the notion that decision-makers, when faced with digital insecurity and the use of adversarial cyber operations, fall back on noncyber situations to make their task simpler.

The degree to which heuristic shortcuts interfere with objectivity and results in more or less severe responses depends on distinct national (strategic) cultures. Gomez and Whyte discuss evidence of cross-national cultural variations influencing the response decision among elite stakeholders. The socio-institutional correlates of civil–military relations in a given democracy stand out to have a unique impact on decision-making processes. Based on their observations from cross-national war games, they conclude that the interaction between the microfoundations of decision-making in a given cultural and institutional setting “might ultimately have some effect on the strategic calculations states make around signaling and adversary behavior” (Gomez and Whyte 2022: 125). The fact that unintended escalation due to prior beliefs, cognitive biases of decision-makers, and/ or bureaucratic politics cannot be excluded in strategic context characterized by uncertainty and ambiguity highlights the advantage of deterrence as a conflict management tool: As a theory of interdependent decision-making, it might prevent militarization and escalation (Schelling 1966).

#### Deterrence failure from ambiguous attribution

Andreas Wenger & Myriam Dunn Cavelty 22, Wenger is professor of international and Swiss security policy at ETH Zurich and director of the Center for Security Studies (CSS), Switzerland; Cavelty is deputy head of research and teaching at the Center for Security Studies (CSS), ETH Zurich, Switzerland, “Conclusion,” Cyber Security Politics, 1st ed., Routledge, 01/18/2022, pp. 239–266 DOI.org (Crossref), doi:10.4324/9781003110224-18

Deterrence: The ambiguity of attribution in the context of cyber conflict management

Over the years there has been considerable work invested at the science-policy interface in adapting deterrence to the ambiguous context of cyberspace. The scope of the practical applicability of the tenets of deterrence to cyberspace is considerably more limited than in more traditional conventional and nuclear deterrence settings (Soesanto and Smeets 2020). At the same time, deterrence attempts in cybersecurity and cyber defense span a wide spectrum of threats, including cybercrime, cyber espionage, and operational cyberattack.

From a conceptual point of view, the attention at the lower end of conflict shifted to criminological conceptions of deterrence and from punishment to denial mechanisms converging on target hardening through cyber resilience (Wenger and Wilner 2021). In such settings, though, deterrence approaches are typically integrated with other coercive and non-coercive tools into a broader conflict management strategy. Conversely, at the higher end of conflict the attention of strategists has shifted to the concept of cross domain deterrence (Lindsay and Gartzke 2019). The focus here is on adversaries that apply ambiguous “gray zone” strategies that integrate military and non-military coercive instruments while evading attribution. Cross domain deterrence tends to include both positive inducements and negative threats and brings the concept of deterrence “back to the broader coercive diplomacy literature from which it originally emerged” (Sweijs and Zilinick 2021: 152).

In his chapter on the limited reliance of Israel on cyber deterrence, Amir Lupovici (2022) explores how new digital technologies enter into doctrine and strategy. Acknowledging the methodological difficulties of studying cyber deterrence, he deliberately shifts the focus from studying what makes deterrence effective in a given strategic context to analyzing how the cyber domain is embedded in Israel’s strategic culture and identity. From such a viewpoint, Lupovici argues, it is puzzling that Israel has so far not developed a clear cyber deterrence strategy, given the prominent role deterrence has played in Israel’s strategy and the country’s “deterrer identity” (Lupovici 2016). Israeli policymakers, he concludes, seem to recognize the uncertainty and ambiguity involved in establishing a deterrence balance in cyberspace and consequently shy away from formulating a declaratory cyber deterrence strategy.

From an operational point of view, Lupovici (2022) argues, Israel’s repeated use of offensive cyber operations against the Iranian and Syrian nuclear programs have been interpreted by some experts as attempts to establish cumulative deterrence through the actual use of force, a concept which is deeply ingrained in Israeli strategic culture (Adamski 2021). Yet the effectiveness of such a strategy remains in dispute, Lupovici insists, and whatever deterrent threat might get through to the adversary is communicated in an indirect and implicit way only. From a conceptual perspective, the US strategy of persistent engagement and defend forward seems to share some of the tenets of the Israeli concept of cumulative deterrence (Tor 2015; Kello 2017). Yet the concept of cumulative deterrence was customarily rejected by most US strategists and policymakers, since in the context of nuclear deterrence the use of force was seen as a symptom of deterrence failure, signalizing a shift from a policy of influence to a policy of control (Adamsky 2021).

It is quite telling that two of the leaders in thinking about and in practicing deterrence in their different strategic contexts have come to accept the limits of deterrence in cyberspace. The way US and Israeli policymakers and strategist conceptualize the cyber domain – as an operating environment with a high degree of technical interconnectedness (increasing uncertainty) and constant political contestation (increasing ambiguity) – seems to be part of the explanation why they, respectively, moved away from cyber deterrence (United States) and never declared a clear deterrence strategy (Israel). Although cyberspace is conceptualized as the fifth domain of warfare, its structural characteristics differ from the other four domains. Cyberspace is completely human-built, shaped by technology companies, and operating in it will always be hard and only partially under control of any one actor (Seebeck 2019). Precisely because cyberspace is completely designed by humans, states can shape it according to their interest. Yet as in cryptology they must cooperate to compete and accept the constraint of a cooperatively produced network of networks.

The economic and political logic of cyberspace as something completely designed by humans might explain why states seem to perceive cyberspace as a domain of intelligence rather than warfare. As discussed above, the fact that setting up cyber exploitation is more expensive than countering released exploitation translates into an incentive to keep the target at risk. From a political point of view, transparent attribution as a precondition of a credible deterrence threat is difficult. Relating an intrusion set to a politically responsible party, Kuerbis et al. (2022) argue, remains challenging because it includes a judgment about the relation between victim and adversary. As such, it should be interpreted as “a product more of political science or intelligence studies than computer science” (Kuerbis et al. 2022: 222).

#### Card

Jarno Limnéll & Charly Salonius-Pasternak 16, Jarno Limnéll, Professor of Cybersecurity, Aalto University, Finland; Charly Salonius-Pasternak, Senior Research Fellow, The Finnish Institute of International Affairs, “Challenge for NATO – Cyber Article 5,” Briefing Paper published by the Center for Asymmetric Threat Studies, June 2016, <https://www.diva-portal.org/smash/get/diva2:1119569/FULLTEXT01.pdf>

NATO members have declared cyber as an operational domain, just like air, see and land. The decision reflects a notable adaptation in the Alliance’s 67-year history, and can be seen as part of a broader move to adapt the alliance to changing warfare and security needs. In doing this, NATO members have agreed to defend against attacks in cyberspace just as they do against attacks launched against targets on other warfare domains. NATO is adapting to its cumulative dependence on the digital domain and responding to the increasing sophistication of cyber capabilities developed by state and non-state actors. The cyber domain is acknowledged to be an integral part of today´s modern wars, conflicts and crises, and more specifically NATO´s current and future operative security environment.

Cyber is becoming an inseparable part NATO’s fundamental principle of collective defense. The need for ambitious decisions in the Warsaw Summit and beyond is driven forward by the accelerating threat and increasing questions over resilience of networks upon which daily life has come to depend. Incorporating cyber into other activities, clarifying the cyber policy with regard to Article 5 and readiness to conduct full-spectrum cyber operations with shared capabilities are not just a wish for NATO - they are a necessity in today´s dynamic, complex and uncertain world.

The declaration of cyber as a domain of warfare means that cyber-attacks can more easily be used to justify invoking the collective defence clause - article 5 - of the North Atlantic Treaty. The declaration also reminds NATO member-states that collective cyber credibility begins with countries´ own cyber defenses, which needs to be strengthened. Article 5 specifies “an armed attack” and NATO is officially ready to consider cyber-attacks as an armed attack.

A preliminary step in this direction was taken at the Wales Summit two years ago, when NATO declared that a “decision as to when a cyber-attack would lead to the invocation of Article 5 would be taken by the North Atlantic council on a case-by-case basis.” The declaration clarified that the invocation of Article 5 would be conditioned to each single cyber-attack. However, any kind of cyber-attack against a state is a type of aggression. The declaration opens the way for members to take action against the aggressor, including the use of armed force, to restore security.

One of the consequences of this new step is that the Alliance will have to develop a comprehensive cyber doctrine as a separate entity, as well as integrate it into overall planning and strategy documents. Though easy on the surface, it will require NATO to address a number of questions, while acknowledging that the most binary of domains (cyber) is ultimately also one of the more political ones – leading to the concept of cyberpolitics. With the creation of cyberspace, a new arena for the conduct of politics is taking shape, and we may well be witnessing a new form of politics in NATO. The ubiquity, fluidity, and anonymity of cyberspace have already challenged such concepts as deterrence, national security and diplomacy in the traditionally state-centric arena of international relations.

Whatever the shape of the doctrine, whether public or secret, when a cyber-attack occurs in the future and NATO is involved, the doctrine will have to provide reasonable guidelines when satisfactory answers are sought to the following questions:

Who did it? Attributing cyber-attacks to their sponsor remains a significant challenge, especially if attribution is to be public and one-hundred percent certain. The trend is also towards governments outsourcing cyber operations to non-state actors.

What were the consequences of the attack? The speed and covert nature of cyber-attacks makes it difficult to readily establish their magnitude and consequences; moreover, are secondary or tertiary effects to be included in the estimate of consequences?

What are the instruments to respond? And, what is a proportional response? Because cyber capabilities will continue to be primarily national, it is possible that some member states could respond symmetrically, while others must consider asymmetric responses. This is a question of the levers of national power at a state’s disposal and willingness to use them. The judgement on proportionality is a political judgement, as it will require a more flexible and historically context aware judgement than a IF-THEN statement in code.

There’s also a possibility that when a cyber-attack occurs a member-state may overreact. Political prudence is needed, even though a successful public cyber-attack that is attributed to specific actors would likely create significant political pressure to respond. Restraint should be encouraged, but based on the emerging “cyber warfare playbook” this may be quite challenging.

What then might lead to cyber-attack causing Article 5 to be invoked? No one knows, as it is situationally dependent. The old way of thinking is that a ‘severe cyber-attack’ has to involve physical destruction – people have to die and physical damage must be seen in the critical infrastructure. However, as we become ever more dependent on data and ‘non-kinetic assets’, could for example the manipulation of health records lead to Article 5 being invoked? Moreover, is there a difference between banking data and health-care data being manipulated, with one potentially leading to severe economic disruptions and the other in extremis to death.

Formulating clear doctrines is frequently preferred by militaries, while politicians and diplomats prefer flexibility in message and response. The Alliance has two paths it can chose in creating the doctrine regarding cyber. It can either chose a public approach, rather similar to its approach when creating its most recent strategic concept. In such a document it could generally describe what constitutes an attack that would qualify for the invocation of Article 5, and what would be an accepted retaliatory action. The other path is to maintain strategic ambiguity, recognizing that formulating clear redlines would invite potential adversaries to push up to the red line. In this case developing the doctrine is still important, but would then be for internal use only. This non-public approach may reduce the objective of improving the Alliance´s cyber deterrence. The pace of development in the field would argue against an overly specific set of guidelines or doctrine, lest it require too frequent and politically challenging updates.

The current ‘cyber warfare playbook’ is still a slim volume - but it is growing by the day. In order to remain a credible defence alliance, NATO must possess a credible cyber policy, including cyber deterrence. Credibility comes from a largely similar set of actions as NATO has engaged in regarding conventional military. Doing it in the cyber domain is, however, harder at the moment. For example, what is the equivalent of standing up in practice permanent battalions in member states? How do you exercise, publicly message determination to defend and counter aggression, in a serious but non-threatening way?

NATO has to find a clear way to deal with a ‘Cyber Article 5’ event. It may be necessary to reinterpret what Article 5 and an armed attack constitute in today´s world. The biggest challenges is to reach a shared understanding of the limits (physical and cyber) which could lead a member state to invoke Article 5 and delineate what proportionality in response means. The decisions are political by their nature and requires strong understanding on strategic cyber domain and its development by the political actors involved. Ultimately, success will depend on how the cyber is blended with traditional political and military power.

#### Cyber brink

Jack Detsch & Mary Yang 22, Detsch, Foreign Policy’s Pentagon and national security reporter; Yang, an intern at Foreign Policy, “Russia Prepares Destructive Cyberattacks,” Foreign Policy, 3/30/22, <https://foreignpolicy.com/2022/03/30/russia-cyber-attacks-us-ukraine-biden/>

Russia is preparing disruptive cyberattacks that could target U.S. energy and financial industries to cause further pain to the Biden administration, in retaliation for heavy sanctions against the Kremlin for its invasion of Ukraine, several people familiar with the matter told Foreign Policy.

The FBI warned five U.S. energy companies in mid-March that computers using Russian internet addresses had been scanning their networks, in a possible prelude to bigger cyberattacks. Top U.S. cybersecurity officials have warned that Russia is looking to conduct disruptive or destructive digital attacks, as opposed to conducting routine espionage.

The Russian handiwork could provide a means for poking the United States and other NATO countries for their support of Ukraine without provoking a wider conflict. Unlike the tit-for-tat ladder of escalation that U.S. military doctrine applies to a possible nuclear conflict with Russia or China, American officials over the last three administrations have struggled to draw clear rules of the road for cyberattacks. Jen Easterly, director of the Cybersecurity and Infrastructure Security Agency, said last week that every U.S. sector is likely vulnerable to digital strikes.

Russia, which seems to have little defense for American- and European-delivered anti-tank and anti-aircraft missiles on the Ukrainian battlefield, doesn’t have to hit the biggest American target to have an impact, experts said, but can bloody the nose of U.S. companies in digital attacks that fall below the threshold of demanding a response from President Joe Biden and his team.

“The goal is to inflict pain in a way that they can walk back from,” said Nick Biasini, the head of outreach at Cisco Talos, the cybersecurity company’s threat intelligence arm. “They’re going to be going after where they can inflict damage, where they can actually cause pain.”

Dave Lewis, a Cisco global advisory chief information security officer, took it one step further. “Back in the early days of the internet, the attackers would try to get their defacement up and that was their whole modus operandi,” he said. “Now it’s just a matter of whose IP [address] is coming up next. They’re going to cast a wide net and see what they can hit.”

Most companies have been preparing for a range of scenarios for years that Russia could roll out, including denial of service attacks to shut down networks by flooding them with traffic, defacement of government and corporate websites, or ransomware attacks that seize and lock down servers until their operators cough up cash, like the 2021 attack that knocked out the Colonial pipeline in the southeastern United States for nearly a week.

But experts believe that Russia doesn’t have to use digital attacks that harm physical infrastructure in the United States and elsewhere to cause problems. Biasini said that Russia had learned from the Colonial pipeline attack that it could cause chaos by simply hacking into the enterprise software that underlies energy companies, instead of taking more destructive and sophisticated cyberattacks that render equipment inoperable.

There are also public signals that Russian hackers could put U.S. energy companies in the crosshairs. The U.S. warnings come as pro-Kremlin propaganda channels and news outlets have ridiculed the Biden administration’s assertion that Russian President Vladimir Putin is responsible for higher global gas prices because of the wider invasion of Ukraine.

Both the United States and the United Kingdom have barred imports of Russian oil and natural gas, and major European states such as Germany—which already shelved the Nord Stream 2 pipeline project over the invasion—have promised to begin the arduous process of weaning themselves off of Russian energy, which accounts for more than 40 percent of European gas imports.

“It’s kind of paradoxical,” said Gavin Wilde, a nonresident fellow at Defense Priorities and an expert on Russia and information warfare who previously served as a director for Russia, Baltic, and Caucasus affairs on the U.S. National Security Council. “The more isolated Russia is on the global stage, the fewer constraints it may feel to act in cyberspace.”

Experts said that the higher energy prices go, the more difficult it could become for the United States to keep antsy European capitals in line with crushing sanctions on the Russians. “Now, I think, would be a good time from the Russian standpoint to do it, given that they’re sort of getting into a standstill on the ground in Ukraine,” said Dmitri Alperovitch, a cybersecurity expert at the Silverado Policy Accelerator. “They can refocus their attention on the West and try to divide the Europeans from the U.S. on these sanctions moves.”

But even though American energy and financial companies have been girding themselves for a range of possible Russian cyberscenarios, the Kremlin’s well-honed capability and determination to render U.S. networks inoperable could make it a formidable adversary, even for the best-defended firms. “If the Russians focus their efforts on a target and they want to compromise that target and destroy it, they’ll be able to do so,” Alperovitch said.

These aren’t garden-variety smash-and-grab cybercrime attacks that U.S. officials and experts are expecting from Russia this time. Russia tends to blur the line between criminal gangs and government-backed hackers, experts said, making it difficult to determine exactly what the Kremlin will order. “You’re dealing with an adversary that’s in a very difficult mindset and one that’s shifting all the time,” said Biasini, the Cisco expert. “So it’s something that may be on the table today [but] might be off the table tomorrow and vice versa.” In the past, Russia has also drawn on privateers and activists motivated by financial gains.

Domestically, the Russian government has been systematically tightening its grip on its own cybersphere, too—especially over the past few years—in pursuit of a grand strategy to cement into law the Kremlin’s total control over the internet. Since 2019, when Putin introduced a set of amendments granting the Kremlin the power to interfere with the dissemination of information online, Russians have been engaging with an increasingly engineered, censored internet. A flurry of laws passed since then have only put more pressure on tech companies to comply or face fines and other kinds of punishment.

For example, the Russian government throttled—intentionally slowed down—Twitter when the social media company refused to remove posts showing minors at protests during a surge in support for Alexei Navalny, the imprisoned Russian opposition leader, when he experienced a sharp deterioration in health in March 2021. The Kremlin had labeled sensitive content involving minors and sensitive issues, such as drug abuse and suicide, as prohibited, using it as leverage to cover up the scope of dissent, explained Grant Baker, a technology and democracy researcher at the U.S.-based nonprofit Freedom House.

During the monthlong war in Ukraine, Russian hackers have mostly tried to grab as many footholds as they can in Ukrainian networks to steal information, gain remote access, and use malicious so-called wiper software to destroy valuable files, Lewis and Biasini, the Cisco experts, told Foreign Policy. Biasini said Cisco and other U.S. companies are working with Ukraine to kill significant numbers of remote access Trojans that are used to gain remote control of computer systems.

But just as U.S. officials believe that Russian troops have run into stiffer-than-expected resistance from Ukrainian troops on the physical battlefield, Kyiv has also proved more resilient in cyberspace than the Kremlin anticipated, U.S. officials and experts said. Speaking during a Senate hearing on Tuesday, Gen. Tod Wolters, the head of U.S. European Command and NATO’s supreme allied commander, told lawmakers that Ukraine’s command of its military forces remained in place, while Russia is facing difficulties getting military orders to its units due to problems with its communications equipment, as well as disciplinary infractions in the ranks. Wolters added that he believed the United States and NATO had “dramatically” improved their offensive and defensive cybertactics and ability to control the information environment over the course of the Ukraine conflict.

“The internet’s a live-fire environment,” said Lewis, the Cisco cybersecurity expert. “They’re just one more adversary in an absolute rogue’s gallery that is out there.”

#### Cutting

Cassia Sari 22, correspondent intern at the OWP, Political Science and Journalism Student at UNC Chapel Hill, “Cyberattacks Can Invoke NATO Defence Clause,” The Organization for World Peace, 4/25/22, <https://theowp.org/cyberattacks-can-invoke-nato-defence-clause/>

The ability to communicate in real-time with friends, family, and random internet strangers thousands of miles away falls nothing short of spectacular. Every rose has its thorn, and every computer system can be a victim of a cyberattack. In a world ever-connected, “Everything is reliant in some form on digital capabilities,” said Michael Daniel, CEO of the Cyber Threat Alliance and a former cybersecurity official during the Obama administration. This means there are many “different avenues to create disruptions… for the West.”

Amidst the war in Ukraine, concerns over cyberattacks across the globe threaten the security of countries and alliances. A cyberattack on any NATO member state would trigger Article 5, the collective defense clause, which says that an act of war against any member will trigger a response from the full alliance. No lines have been marked as to where cyberaggression falls in the spectrum of “acts of war,” but a NATO official said last week that the allies might consider significant malicious cumulative cyber activities as an armed attack.

United States Senate Intelligence Committee Chairman Mark Warner posed a hypothetical case in which they and other NATO allies would have to retaliate against Russian cyber warfare. If a Russian cyberattack on Ukraine impacts Poland, a NATO member, and the attack triggers power outages that result in hospital patients dying or knocking out traffic lights that cause fatal road accidents involving U.S. troops, then NATO would have to intervene.

Most officials agree that the chances of a Russian cyberattack, either directly or indirectly against the U.S., are very low due to the exponentially escalating nature of doing so. The U.S. and Western Europe have already taken severe unprecedented financial measures against Russia by cutting the country off from roughly $600 billion in reserves held by the Central Bank of Russia, according to a Reuters article. NATO members also banned Russian state banks from using a bank messaging system to conduct international transactions. Despite all of the sanctions and financial misery the U.S. and Europe have imposed on Russia, Vladimir Putin has demonstrated cyber restraint.

The question is not whether Russia can “Carry out cyberattacks against Europe or the United States,” said Melissa Griffith, a senior science and technology innovation program associate at The Wilson Center. Rather it is what Russia would gain and risk “By carrying out cyberattacks against the United States and Europe.”

Warner thinks that is soon to change. “I think we will probably see that in the coming days and weeks as Putin tries to lash out against the crippling level of sanctions we’ve put on him,” Warner said.

He is not alone in his fears. Last week, the Cybersecurity and Infrastructure Security Agency (CISA) updated the “Shields Up” guidance to urge businesses and organizations to prioritize their cybersecurity.

“While there are no specific or credible cyber threats to the U.S. homeland at this time, Russia’s unprovoked attack on Ukraine, which has involved cyber-attacks on the Ukrainian government and critical infrastructure organizations, may impact organizations both within and beyond the region, particularly in the wake of sanctions imposed by the United States and our Allies,” the CISA guidance states. “Every organization — large and small — must be prepared to respond to disruptive cyber activity.”

Daniel, the CEO of the Cyber Threat Alliance, expects retaliation to come in the form of cyberspace. Daniel posited that many people “In the industry expect that some form of retaliation will come through cyberspace because it’s an area where the Russians have a lot of capability, and it’s one where the West has a lot of vulnerabilities.” What has been the greatest accomplishment of the 21st century is now the biggest weak spot in the West, as the U.S. and Western Europe are digitally dependent societies where life is unimaginable without the internet.

However, our social media accounts and school emails aren’t likely targets for Russian cyberattacks. Cyber experts expect the oil and gas industries are the most vulnerable because they are not mandated by law to invest in cybersecurity. Meanwhile, President Biden has urged critical infrastructure in the financial, energy, and health care sectors to strengthen their cyber defenses.

Western European countries are the likely targets of Russian cyberattacks. James Lewis, a senior vice president and program director at the Center for Strategic and International Studies, said the U.K, France, and the Baltic states must remain vigilant in their cyber defense. He predicts Russia will save its ammunition for France until the presidential election is held in mid-April in order to interfere with the process.

If France or any other NATO country falls victim to Russian cyberattacks, there is no guarantee yet on whether article five will really be invoked. “We will not speculate on how serious a cyberattack would have to be in order to trigger a collective response,” said the NATO official. “Any response could include diplomatic and economic sanctions, cyber measures, or even conventional forces, depending on the nature of the attack.” There are no clear guidelines on how NATO would respond if called to defend a member country from a cyberattack, said Warner.

No one knows if or when a cyberattack from Russia is on the timeline, but Lewis said that “Cyberattack is now part of everybody’s military planning.”

#### Cutting

Katrina Manson 22, reporter at Bloomberg Business covering cyber and emerging tech, “Nobody Knows Where the Red Line Is for Cyberwarfare,” Bloomberg, 5/2/22, <https://www.bloomberg.com/news/articles/2022-05-02/russia-cyberattacks-raise-questions-about-hacking-red-lines#xj4y7vzkg>

A common explanation for why the Soviet Union never used nuclear weapons during the Cold War was the expectation that any attack would likely prompt a devastating nuclear response. The fear of mutually assured destruction was enough to keep both the USSR and the U.S. from launching a nuclear attack, even as they spent decades building up huge stockpiles of weapons.

Cyberweapons are different. Cyberattacks by both governments and private hackers have exploded in recent years. Many of these are financially motivated, but others involve espionage or, in several high-profile cases, the sabotage of physical infrastructure. There’s broad agreement that at some point a cyberattack would be considered an act of war. Yet no one knows quite where the line is.

[TABLE OMITTED]

The situation is more dangerous than ever. Russia’s bloody invasion of Ukraine raises the specter of cyberattacks starting an escalatory spiral that results in an all-out war with the U.S. The Biden administration has already warned Russian President Vladimir Putin against targeting 16 sectors at the heart of U.S. economic and national security, including energy and finance. “We will respond with cyber,” Joe Biden told reporters last summer after meeting Putin face to face in Geneva. The president didn’t lay out exactly what that would entail but added, darkly, “he knows.”

On May 4-5, cyber experts from the Biden administration, the military, and academia are gathering at Vanderbilt University to discuss the new contours of modern conflict at an event organized by Brett Goldstein, a former senior Pentagon official and computer scientist who’s now special adviser to Vanderbilt’s chancellor. Goldstein says that in the next 5 to 10 years the U.S. should develop a strategy of cyber mutually assured destruction—or cyberMAD—as a form of deterrence. “It is essential that we take lessons from the success of nuclear MAD concepts,” he says, warning that U.S. vulnerabilities are only going to grow.

The Department of Defense is preparing a new cyber strategy this year that’s likely to include a more prominent role for deterrence. U.S. officials and policy experts have been debating whether it’s better to dissuade attacks with the promise of retaliation in cyberspace or elsewhere, or to try to prevent them by taking offensive cyber measures that cut off rivals’ ability to carry them out. The Biden administration’s strategy will be based on integrated deterrence—the concept that attacks can be prevented by threats of economic penalties or other responses that rely on various levers of U.S. power.

Lawmakers from both parties and experts from outside government are pushing for their own vision of deterrence. A two-year, congressionally mandated bipartisan effort that concluded last year, the Cyberspace Solarium Commission, favors a variation of the theme “layered cyber deterrence,” which combines a focus on hardening technical defenses against attacks with the promotion of international norms against, say, cyberattacks targeting civilian infrastructure.

Goldstein’s faith that the threat of catastrophic response could prevent state-sponsored cyberattacks makes him an outlier. Deciding when to respond would be fraught, because determining who has carried out any breach can be tricky. The best hackers often mask their identities. Russian hackers, for instance, have left bread crumbs suggesting they’re North Korean or Iranian, cybersecurity experts have said. Officials say they’ve become better in recent years at determining responsibility for attacks.

Unlike nuclear weapons, which haven’t been used since World War II, the tools of cyberwarfare are widely available and used regularly for attacks of varying seriousness. “Redlines are notoriously difficult to define in cyberspace,” Emily Goldman, a cyber strategist at U.S. Cyber Command, wrote in a 2022 paper for the journal The Cyber Defense Review. She argued that sanctions, criminal indictments, and other deterrent measures have proven ineffective: “More of the same will not produce different results.”

General Paul Nakasone, the leader of the U.S.’s 6,000-person military Cyber Command and one of the speakers at Goldstein’s event, has dismissed the nuclear parallels. “Cyber deterrence is not nuclear deterrence,” he told Congress in April. For the past several years he’s overseen an increase in the Pentagon’s continuous offensive cyber operations outside U.S. borders, under a strategy he’s described as “defending forward.”

The U.S. began changing its approach when Russian interference in the 2016 presidential election led U.S. leaders to overcome their reluctance for counteroffensive cyberattacks, according to Jonathan Reiber, who authored the government’s 2015 cyber strategy when he was the chief strategy officer for cyber policy at the Department of Defense. In 2018, Congress changed the legal definition of offensive cyber operations, classifying them as traditional military activity. That same year the Trump administration issued a classified policy memo that some U.S. lawmakers said essentially delegated authority to the Defense Department to conduct them without the White House signing off.

Nakasone told Congress that both the legal change and the policy memo have been “very helpful.” The Biden administration is reviewing the memo, and proponents of the “defend forward” strategy worry it could decide to restrict Cyber Command’s ability to act effectively.

One problem with using the threat of cyberattacks as a deterrent is that cyber superiority is inherently ephemeral, according to Nakasone. While a nuclear arsenal’s power is persistent, cyberweapons rely on exploiting vulnerabilities in code, which can be patched and disappear as quickly as they’re found. So, unlike nuclear weapons, Nakasone’s cyber arsenal and access routes must change all the time. The U.S.’s ability to find and exploit such vulnerabilities is significant, but its ability to carry out attacks on specific targets may ebb and flow.

Some academics argue that “defending forward” is a euphemism for the U.S. waging its own attacks. In a paper for the Atlantic Council in March, cyber coercion expert Jenny Jun argued that the strategy leaves “much room for misjudgment and misinterpretation” about how the U.S. will respond and that instead of being a deterrent, it could encourage adversaries to strike first rather than wait to be compromised themselves.

Amid such uncertainty over the nature of cyberwar, Erica Lonergan, a senior director on the Cyberspace Solarium Commission, says that debates over deterrence have become unhelpfully “binary.” The best way to prevent major cyberattacks may not be to threaten or execute cyber operations, she says, but to rely on other instruments of national power. In 2018 the Trump administration listed using nuclear weapons as a potentially appropriate response to a non-nuclear strategic attack, a category that could include a catastrophic cyberattack. The Biden administration reserves the right to choose how it responds, including with military force, and insists a cyberattack against any NATO ally could trigger a joint response from all 30 countries.

One challenge is that the lack of a clear definition of cyberwarfare has tempted countries to test the limits, carrying out smaller attacks under the assumption they won’t be enough to provoke a major response. Some experts warn that the U.S.’s ability to establish norms surrounding such attacks has been undermined by its own history of cyberattacks, digital spying programs that targeted civilians—including allied leaders—and the Stuxnet attack that targeted Iran’s nuclear facilities more than a decade ago, a campaign widely believed to have been carried out by the U.S. and Israel.

Michael Daniel, a former cybersecurity coordinator under the Obama administration, says the U.S. could do a lot more to deter the proliferation of cyberattacks that fall below the threshold of war in cyberspace. “The question is, can you use the government’s national power to reduce the volume of malicious activity in cyberspace and reduce its impact on the United States?” he says.

A small, and potentially temporary, comfort is that Russia’s war with Ukraine has so far resulted in less cyberwarfare than many experts expected. One theory as to why, put forth by Lennart Maschmeyer, a cybersecurity researcher at ETH Zurich, is that they aren’t as effective as many people believe. He’s studied the impact of Russian cyberattacks against Ukraine since 2014. “They have really achieved almost no measurable strategic impact,” he says. Another explanation could be that Russia didn’t plan any, because it anticipated swift military victory. That could change as the war grinds on, and recent research from Microsoft indicates Russia has been using “destructive and relentless” cyberattacks against Ukrainian services and institutions.

It’s also possible deterrence is working and Russia has been fearful of carrying out cyberattacks outside of Ukraine because that could trigger NATO’s Article 5, the collective defense clause, and draw other nations into the conflict. For Goldstein, this hesitance points to a strategic opportunity. “We may be seeing the early bones of what deterrence could look like,” he says.