**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 op**eration**s**. **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 **op**eration**s** 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** cyber**attack** 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 op**eration**s**. **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 **op**eration**s** 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** **o**ffensive **c**yber **o**peration**s**1 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 op**eration**s** 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 **o**ffensive **c**yber into Alliance **o**peration**s** 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 **o**ffensive **c**yber **o**peration**s**. **Until then, whatever NATO does offensively**, it will **rely** heavily on the **U**nited **S**tates 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 **cyber**space 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 **op**eration**s** 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, **cyber**space **op**eration**s** 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 **coop**eration 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 **build**ing **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 **op**eration**s** 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 **o**ffensive **c**yber **o**peration**s** 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 **o**ffensive **c**yber **o**peration**s**.

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 **d**enial **o**f **s**ervice 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 **c**ommand **and** **c**ontrol.

**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 **N**orth **A**tlantic **C**ouncil 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. **Coop**eration 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 S**tates 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 war**fare 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 **s**pheres **o**f **i**nfluence 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 **s**pheres-**o**f-**i**nfluence **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 lead**ing the **resistance** to a **s**pheres-**o**f-**i**nfluence **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 **tech**nological **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 **op**eration**s** 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** state**s** hold **constant** joint operational strategic centers of **training** and operations; on and about among others, ballistic missile defense, **i**ntelligence, **s**urveillance, **r**econnaissance, **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 **tech**nology 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 **op**eration**s**, and constant accurate flow of **info**rmation.

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 **coop**eration 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 **op**eration**s** 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 tech**nologies **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 **d**efence **i**ndustrial **b**ase 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 **U**nited **S**tates has entered an era of long-term **competition** with **revisionist powers**. A key aspect of this competition will revolve around a contest for **tech**nological **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 **U**nited **S**tates, 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 **U**nited **S**tates in virtually **every region of the world.**

In pursuit of its goal of reshaping the world order, China aims to supplant the **U**nited **S**tates as the world’s **leading tech**nological **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–tech**nical **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 **U**nited **S**tates 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 tech**nologies— **advanced computing**, **big data** analytics, **a**rtificial **i**ntelligence, **autonomy**, **directed energy**, **hypersonics**, and **biotech**nology. **Multiple simultaneous tech**nological **revolutions** are likely to significantly impact the **character of war**. The competitor that **best harnesses** these **tech**nologies 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. **Tech**nology-**led** **cross-domain** **war**fare 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 Tech**nology that is now underway. **A**rtificial **i**ntelligence, **quantum** computing and **machine-learning**, **nano-tech**nologies, **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 **tech**nology 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** state**s** **to counter** with more agile ways **any emerging crises**. This will **efficiently manage** processes and purposes for **op**eration**s** against **any methods of e**lectronic **war**fare. **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 **info**rmation **“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 op**eration**s”** (Sendmeyer, 2010)—meaning **not only defensive**-clause operations but also in **counter-offensive** **op**eration**s** (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 **op**eration**s** 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 tech**nology 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 tech**nology, 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. **Tech**nology plays a **key role** in a global reach. Yet **so does NATO**, through the **framework** of a **limitless tech**nology applied in **military op**eration**s**. 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 op**eration**s** 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 tech**nology. **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 tech**nical **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 **cyber**space 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 **coop**eration 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 **tech**nology 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 **info**rmation **sharing**, participation in **training** and **exercises** as well as the provision of reciprocal assistance in the form of **intel**ligence 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 op**eration**s** 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. **Coop**eration with **industry** has been formalised in the NATO Industry Cyber Partnership (NICP), which was founded and endorsed by the Alliance **based** up**on** 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 **enable**d the Baltic state**s** 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 **coop**eration. 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 **intel**ligence 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 **U**nited **S**tates 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 **tech**nological **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 **equip**ping **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 **tech**nological **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 **tech**nological **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** state**s**. 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 tech**nologies **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 v**enture **c**apital to provide **safe financing** to NATO’s fledgling start-ups, thereby minimising their susceptibility to **nefarious f**oreign **d**irect **i**nvestment. 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 **tech**nology **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 tech**nologies at **speed**. They could partner with successful start-ups, perhaps through a joint venture or an **Alliance-wide p**ublic-**p**rivate **p**artnership, 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 **tech**nologies 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 tech**nologies 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 **U**nited **S**tates 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 **tech**nology 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 **U**nited **S**tates 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-op**eration 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 **a**nti-**sat**ellite weapon**s**. 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 **reservation**s 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 **cyber**space, 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 tool**31. 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 **a**n **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 op**eration**s** 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 **U**nited **S**tates.

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, **retal**iatory offensive cyber **op**eration**s** 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 **covert**ly 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 op**eration**s** 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 calc**ulations 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 20**03** 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 **Russia**n state (if it has **forbidden** mercenary acts) or a degree of caution by criminals.
* There is **enough uncertainty** among potential attackers about the **U**nited **S**tates’ ability to **attribute** that they are **unwilling** to risk **massive retal**iation 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** cyber**attack** 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 **U**nited **S**tates, **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 **U**nited **S**tates. 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 **No**rth **Ko**rea 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 **retal**iation 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 **US**A or Russia has plans – or perhaps more importantly, the desire – to fully undermine the other’s nuclear **c**ommand and **c**ontrol 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 **c**ommand and **c**ontrol 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 **U**nited **S**tates 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 **W**all **S**treet **J**ournal 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 **incorrect**ly reported — it was **based on old info**rmation 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 **Russia**n hackers do try to get into American power plants, but so far they've only seemed to be **perform**ing **recon**naissance, 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 **op**eration**s**.

"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 **cyber**attack 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 **cyber**attack, 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 **East**ern Interconnect, the **West**ern 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. **New**er **gen**eration**s** 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 **W**orld **H**ealth **O**rganization 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 mili**tary tech**nologies 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 **Russia**n 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 **interp**retation 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 **interp**retation 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 **resolve**d 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 a**rg**ument for disarmament that holds that if the **U**nited **S**tates 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 **who**se 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 **coop**eration, 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 **U**nited **S**tates 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 **U**nited **S**tates’ 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 **U**nited **S**tates 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 **op**eration**s**. 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 **U**nited **S**tates, 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 **strong**er **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 **U**nited **K**ingdom 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 **nuc**lear. 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 “**m**utual **a**ssured **d**estruction” 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 **nuc**lear 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 **B**elt and **R**oad **I**nitiative 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 **s**tatus **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 **U**nited **S**tates 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 **U**nited **S**tates 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 coop**eration 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 **U**nited **S**tates and **China** spend **proportionally far less** on their **militaries** than the **U**nited **S**tates 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 **U**nited **S**tates 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 **U**nited **S**tates 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 **U**nited **S**tates 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 de**stabilizing** than the Cold War’s MAD was at the global level?

Indeed, the actual situation of **being deterred** that **Israel**, **Saudi** Arabia, **the U**nited **S**tates, 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 **D**epartment **o**f **D**efense (**security cooperation**) or the **D**epartment **o**f **S**tate (**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.