# Ban OCO - Case Neg



### 1NC---Russia Deterrence DA

#### Russian reliance on cyberwarfare escalates now---NATO is next

Cattler ’22 [David and Daniel Black; April 6; Assistant Secretary General for Intelligence and Security at NATO; Principal Analyst in the Cyber Threat Analysis Branch at NATO; Foreign Affairs, “The Myth of the Missing Cyberwar: Russia’s Hacking Succeeded in Ukraine—And Poses a Threat Elsewhere, Too,” https://www.foreignaffairs.com/articles/ukraine/2022-04-06/myth-missing-cyberwar/ceng

After Russia invaded Ukraine, many observers initially expected cyberattacks to steal the limelight as a major instrument in Russia’s arsenal. But after a month of fighting, a host of prominent scholars and analysts of cyberconflict have reached the opposite conclusion. Russia’s activities in cyberspace, they claim, have been paltry or even nonexistent. They have dismissed the role of cyber-operations, variously proposing that digital preparations for the invasion in Ukraine never occurred, were haphazard or lacked any real impact, or were mere continuations of Russia’s long-term cyber-activity against Ukraine that fell below the threshold of outright war. This is a dangerous misdiagnosis. All available evidence indicates that Russia has employed a coordinated cyber-campaign intended to provide its forces with an early advantage during its war in Ukraine. The apparent disconnect between these observed incidents, on the one hand, and the public analysis that Russian cyber-operations have been minimal, on the other, is jarring. Preconceived notions of the role of cyberattacks on the battlefield have made it hard for analysts to see cyber-operations in Ukraine for what they are and for the role they play within Russia’s military campaign. Leaning on these preconceptions will only lead to future policy and intelligence failures. Cyberspace is still a nascent domain of operations, and events in Ukraine will have outsized implications not just for any appreciation of Russian cyberpower but for an understanding of the nature of cyberconflict itself. OPENING SALVO The belief that cyber-operations have played no role in Ukraine does not stem from a lack of real-world impact. To the contrary, the magnitude of Moscow’s pre-kinetic destructive cyber-operations was unprecedented. On the day the invasion began, Russian cyber-units successfully deployed more destructive malware—including against conventional military targets such as civilian communications infrastructure and military command and control centers—than the rest of the world’s cyberpowers combined typically use in a given year. The cumulative effects of these attacks were striking. In the hours prior to invasion, Russia hit a range of important targets in Ukraine, rendering the computer systems of multiple government, military, and critical infrastructure sectors inoperable. Forensic analysis by Microsoft, the cybersecurity company Symantec, and the Slovak firm ESET has found that these attacks affected numerous government agencies, military institutions, civil emergency services, and a range of other critical infrastructure sectors such as defense industrial base manufacturers, information technology services, and energy companies directly relevant to Ukraine’s military capacity. Cyber-enabled sabotage also knocked offline the satellite Internet provider KA-SAT, which Ukraine’s military, intelligence, and police units depend on. Victor Zhora, the deputy chief of Ukraine’s State Service of Special Communication and Information Protection, has characterized the satellite outage as “a really huge loss in communications in the very beginning of war.” U.S. defensive cyberspace operations prevented further Russian attacks from disrupting the railway networks that were being used to transport military supplies and help millions of Ukrainian citizens evacuate. Russia continues to draw from its wartime arsenal of cybertools, deploying additional destructive malware on a weekly basis. Cities under siege from Russian shelling, including Kharkiv and Kyiv, have experienced cyber-enabled disruptions to Internet services. Ukraine’s national cyber-authorities continue to expose intrusion attempts by Russian and Belarussian cyber-units. All of this has occurred against the backdrop of a series of website defacements, denial-of-service attacks, and other destabilizing cyber-operations intended to produce chaos and further exhaust Ukraine’s cyberdefenses. If observers see this cyber-offensive as a series of isolated events, its scale and strategic significance get lost in the conventional violence unfolding in Ukraine. But a full accounting of the cyber-operations reveals the proactive and persistent use of cyberattacks to support Russian military objectives. The misperception that Russia has been restrained or ineffective in the prosecution of its cyberwar on Ukraine likely stems from the fact that Russia’s cyber-operations have not had the standalone, debilitating effects that assessments before the war imagined they would have. But those assessments pose an unrealistic test of strategic value. No single domain of operations has an independent, decisive effect on the course of war. Nevertheless, the lack of overwhelming “shock and awe” in cyberspace has led to the flawed presumption that Russia’s cyber-units are incapable, and even worse, that cyber-operations have offered Russia no strategic value in its invasion of Ukraine. THUNDER RUN Analysts should assess the use of cyberpower in its proper context. Evaluating Russia’s cyber-operations in Ukraine is impossible without accounting for the multiple tactical and strategic errors that have bedeviled other aspects of Moscow’s military campaign. Russian planners expected a swift victory in Ukraine, but their strategy failed for multiple reasons: inadequate coordination and preparation, the underestimation of the strength and resilience of Ukraine’s military, and various intelligence lapses. Russia’s missteps and struggles have almost certainly hurt its ability to fully employ its cyber-program in support of its conventional forces. But even with those limitations, Russian cyber-units successfully attacked a range of targets in accordance with Russia’s war plans. Russian cyberattacks on government and military command and control centers, logistics, emergency services, and other critical services such as border control stations were entirely consistent with a so-called thunder run strategy intended to stoke chaos, confusion, and uncertainty, and ultimately avoid a costly and protracted war in Ukraine. Indeed, Russian cyber-units have demonstrated their ability to succeed without a great deal of advance warning and direction, and despite the overarching difficulties hampering Russia’s military effort. The reason for this relative success lies in the unique nature of competition and conflict in cyberspace. Unlike troop buildups or other forms of military mobilization that are infrequent and highly visible, cyber-operations are the result of operational cycles that occur covertly and continuously through peacetime and wartime. The targeting of sensitive networks during peacetime lets attackers lay the groundwork for malware intended for wartime use. The methods attackers use to establish initial footholds for espionage activities are indistinguishable from those that precede cyberattacks. For cyber-units, war does not fundamentally change the way they prepare or start to fight. Russia’s cyberattacks prior to the invasion suggest methodical preparations, with the attackers likely gaining access to Ukrainian networks months ago. This stands in stark contrast to the evident lack of preparation across Moscow’s other military instruments, including on the ground, in the air, and in its frequently used influence operations through media and social media. Russian cyber-units did not need direct military orders to prepare for the invasion or to generate new capabilities for the war. The operational realities of cyberspace required them to be ready well in advance. Russian cyber-units will probably continue to be in a state of permanent readiness and capable of supporting tactical and strategic objectives on short notice, either in Ukraine or beyond, as the war persists. The emerging consensus that claims Russian cyber-operations were ineffective misses the bigger picture. Russia’s strategy failed to capitalize on the full capabilities and numerous operational successes of its cyber-units. For instance, Russian cyber-units have not yet shut down electricity or Internet connectivity on a massive scale in Ukraine. That does not mean Russia is incapable of such attacks, as some observers have suggested, but that it envisioned a swift victory and did not see the need for such widespread, indiscriminate disruptions. In all likelihood, Russian military units were reliant on Ukrainian civil infrastructure for their planned seizure of Kyiv and could not risk blowback to their own operations. Russia is almost certainly capable of cyberattacks of greater scale and consequence than events in Ukraine would have one believe. Moscow has significantly improved its ability to conduct comprehensive cyber-operations in recent years and has actively invested in its cyber-capabilities, developing new and harder-to-detect variants of its more advanced malware and operational infrastructure. NO RESTRAINT The war in Ukraine is not over. Russia has been forced to change its operational approach, and Western intelligence points to Moscow shifting toward a strategy of attrition. With the likelihood that the conflict will become a protracted war, Russia will probably not exercise restraint in its use of additional disruptive and destructive cyber-actions. Russian President Vladimir Putin is most likely to double down on early cyber-successes and seek to further disrupt and undermine government, military, and civilian infrastructure, as well as defense industrial base enterprises. Russia’s recent attempts to strike the same targets it hit on the day of the invasion with additional destructive malware indicate this new phase of the conflict is well underway. Although less visible than cyberattacks, cyber-enabled espionage—the theft of sensitive information, in this case from Ukrainian networks—is also likely to play a grisly role in the Russian offensive. Russia’s Federal Security Service has allegedly used personal information stolen from Ukrainian federal databases to draw up kill lists of people who could lead a Ukrainian resistance movement in the event of a Russian victory. And as the war carries on, Russia may be increasingly tempted to tap into the latent strategic potential of hacking collectives aligned with the Kremlin that specialize in ransomware and can unleash chaos at a moment’s notice. Western policymakers should also be prepared for cyber-operations to spread beyond the confines of Ukraine. Several Russian cyber-operations since the invasion have already had spillover effects into NATO countries, affecting critical sectors and civilian Internet connectivity across Europe. Russia knowingly accepted the risk that its cyberattacks would cause collateral damage and has a history of similar reckless behavior. The U.S. Office of the Director of National Intelligence’s Annual Threat Assessment released in March judged that “Russia is particularly focused on improving its ability to target critical infrastructure … in United States as well as in allied and partner countries.” Active Russian preparations for future cyber-operations indicate that this not an idle threat. Cyber-operations have been Russia’s biggest military success to date in the war in Ukraine. They will continue to provide Moscow a flexible tool capable of hitting a range of targets in Ukraine and beyond. Disregarding their unprecedented use will only leave policymakers and analysts unprepared for what’s next. A clear-eyed view of the role cyberwarfare has played so far in Ukraine and a better understanding of its place in modern warfare are imperatives for NATO’s collective security and for managing the risks of escalation looming in cyberspace.

#### They’ll target U.S. critical infrastructure---only by advancing cyber mechanisms can Russia be deterred

Aldanova ’22 [Dina; May 30; Master’s Candidate at Georgetown University’s Eurasian, Russian, and East European Studies Program; National Interest, “Will Russia Launch a New Cyber Attack on America?,” <https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/will-russia-launch-new-cyber-attack>/ceng

International cooperation to this degree is not an asset that Russia benefits from. With the support of NATO Cooperative Cyber Defense Center of Excellence’s research and development projects, expertise, and training, U.S. retaliation to a potential Russian cyber attack could be not only detrimental but even more profound as a multilateral response. Based on all this, the fear of retaliation could indeed prevent Putin from engaging in offensive cyber operations against the United States. Finally, Putin has lost the upper hand in launching an attack by surprise. For instance, Russia invaded Georgia during the Olympics Games in Beijing in 2008, and Ukraine during the Sochi Winter Olympics in 2014. When Putin waged war on Ukraine in 2022—incidentally, immediately following the Beijing Winter Olympic Games—the West anticipated it. Putin invaded Ukraine anyway. He is unlikely to act recklessly in this way again, considering the failures the Russian military has experienced since the invasion. Furthermore, knowing that the United States and European allies have shielded up, Putin has no incentive to strike. Nevertheless, would Putin wait for a more favorable moment? Or scale back a potential attack, for instance, by meddling in the U.S. midterm elections in November? It would be misleading, however, to underestimate Russian cyber capabilities or Putin’s mind games and lose vigilance. In 2020, despite denying its involvement, Russia evidently hacked U.S. software company SolarWinds. By installing malware into the company’s updated Orion software program, the attack affected thousands of customers, a hundred companies such as Microsoft and Intel, and some federal agencies like the Treasury Department, the Pentagon, and the Cybersecurity and Infrastructure Security Agency. Cyber experts acclaimed the code used as phenomenal. More astonishingly, if not for a performance assessment and proper investigation, the attack could have easily gone unnoticed. For over six months, Moscow tracked emails and other traffic of sensitive information. Could there already be a similar malware in U.S. networks? Now, on the brink of a new Cold War, the United States must keep its guard up on cybersecurity. Although there are significant factors that challenge the probability of an imminent Russian cyber-retaliation, the United States should not disregard the potential for malicious activity in the near future. It needs to keep a sober view and not act hastily. Setting priorities for the long run, the United States needs to continue advancing cyber mechanisms that detect sensitive activity like the Solar Winds hack, and invest more in training and education about cyber hygiene for government agencies, private companies, and the public. It should not neglect to regularly test offline backups, run software updates, report incidents, use multifactor authentication, block unusable domain IP addresses, and assess third-party risks. Although Putin’s intentions are far from clear, his decision to pursue a cyberattack on the United States’ critical infrastructure that would instantly shut down electricity or disrupt clean water supply, the offense might come unexpectedly, and soon. Cornered with sanctions and burdened by the bitterness of defeat, Putin might act furiously. The United States and Western allies need to be vigilant and maintain strong lines of communication about any malicious activity. With a strong multilateral front in the West, Russia will have fewer incentives to engage in cyber warfare.

#### Grid collapse causes extinction

Friedemann 16 (Alice, transportation expert, founder of EnergySkeptic.com and author of “When Trucks Stop Running, Energy and the Future of Transportation,” worked at American Presidential Lines for 22 years, where she developed computer systems to coordinate the transit of cargo between ships, rail, trucks, and consumers, citing Dr. Peter Vincent Pry. Pry is executive director of the Task Force on National and Homeland Security, a Congressional advisory board dedicated to achieving protection of the United States from electromagnetic pulse and other threats. Dr. Pry is also the director of the United States Nuclear Strategy Forum, an advisory body to Congress on policies to counter weapons of mass destruction. Dr. Pry has served on the staffs of the Congressional Commission on the Strategic Posture of the United States, the Commission to Assess the Threat to the U.S. from an EMP Attack, the House Armed Services Committee, as an intelligence officer with the CIA, and as a verification analyst at the U.S. Arms Control and Disarmament Agency. 1-24-16, “Electromagnetic pulse threat to infrastructure (U.S. House hearings)” http://energyskeptic.com/2016/the-scariest-u-s-house-session-ever-electromagnetic-pulse-and-the-fall-of-civilization/)

Modern civilization cannot exist for a protracted period without electricity. Within days of a blackout across the U.S., a blackout that could encompass the entire planet, emergency generators would run out of fuel, telecommunications would cease as would transportation due to gridlock, and eventually no fuel. Cities would have no running water and soon, within a few days, exhaust their food supplies. Police, Fire, Emergency Services and hospitals cannot long operate in a blackout. Government and Industry also need electricity in order to operate. The EMP Commission warns that a natural or nuclear EMP event, given current unpreparedness, would likely result in societal collapse. Terrorists, criminals, and even lone individuals can build a non-nuclear EMP weapon without great trouble or expense, working from Unclassified designs publicly available on the internet, and using parts available at any electronics store. In 2000, the Terrorism Panel of the House Armed Services Committee sponsored an experiment, recruiting a small team of amateur electronics enthusiasts to attempt constructing a radiofrequency weapon, relying only on unclassified design information and parts purchased from Radio Shack. The team, in 1 year, built two radiofrequency weapons of radically different designs. One was designed to fit inside the shipping crate for a Xerox machine, so it could be delivered to the Pentagon mail room where (in those more unguarded days before 9/11) it could slowly fry the Pentagon’s computers. The other radiofrequency weapon was designed to fit inside a small Volkswagon bus, so it could be driven down Wall Street and disrupt computers— and perhaps the National economy. Both designs were demonstrated and tested successfully during a special Congressional hearing for this purpose at the U.S. Army’s Aberdeen Proving Ground. Radiofrequency weapons are not merely a hypothetical threat. Terrorists, criminals, and disgruntled individuals have used home-made radiofrequency weapons. The U.S. military and foreign militaries have a wide variety of such weaponry. Moreover, non-nuclear EMP devices that could be used as radiofrequency weapons are publicly marketed for sale to anyone, usually advertised as ‘‘EMP simulators.’’ For example, one such simulator is advertised for public sale as an ‘‘EMP Suitcase.’’ This EMP simulator is designed to look like a suitcase, can be carried and operated by one person, and is purpose-built with a high energy radiofrequency output to destroy electronics. However, it has only a short radius of effect. Nonetheless, a terrorist or deranged individual who knows what he is doing, who has studied the electric grid for a major metropolitan area, could—armed with the ‘‘EMP Suitcase’’— black out a major city. A CLEAR AND PRESENT DANGER. An EMP weapon can be used by state actors who wish to level the battlefield by neutralizing the great technological advantage enjoyed by U.S. military forces. EMP is also the ideal means, the only means, whereby rogue states or terrorists could use a single nuclear weapon to destroy the United States and prevail in the War on Terrorism or some other conflict with a single blow. The EMP Commission also warned that states or terrorists could exploit U.S. vulnerability to EMP attack for coercion or blackmail: ‘‘Therefore, terrorists or state actors that possess relatively unsophisticated missiles armed with nuclear weapons may well calculate that, instead of destroying a city or military base, they may obtain the greatest political-military utility from one or a few such weapons by using them—or threatening their use—in an EMP attack.’’ The EMP Commission found that states such as Russia, China, North Korea, and Iran have incorporated EMP attack into their military doctrines, and openly describe making EMP attacks against the United States. Indeed, the EMP Commission was established by Congress partly in response to a Russian nuclear EMP threat made to an official Congressional Delegation on May 2, 1999, in the midst of the Balkans crisis. Vladimir Lukin, head of the Russian delegation and a former Ambassador to the United States, warned: ‘‘Hypothetically, if Russia really wanted to hurt the United States in retaliation for NATO’s bombing of Yugoslavia, Russia could fire an SLBM and detonate a single nuclear warhead at high altitude over the United States. The resulting EMP would massively disrupt U.S. communications and computer systems, shutting down everything.’’ China’s military doctrine also openly describes EMP attack as the ultimate asymmetric weapon, as it strikes at the very technology that is the basis of U.S. power. Where EMP is concerned, ‘‘The United States is more vulnerable to attacks than any other country in the world’’: ‘‘Some people might think that things similar to the ‘Pearl Harbor Incident’ are unlikely to take place during the information age. Yet it could be regarded as the ‘Pearl Harbor Incident’ of the 21st Century if a surprise attack is conducted against the enemy’s crucial information systems of command, control, and communications by such means as… electromagnetic pulse weapons… Even a superpower like the United States, which possesses nuclear missiles and powerful armed forces, cannot guarantee its immunity…In their own words, a highly computerized open society like the United States is extremely vulnerable to electronic attacks from all sides. This is because the U.S. economy, from banks to telephone systems and from power plants to iron and steel works, relies entirely on computer networks… When a country grows increasingly powerful economically and technologically…it will become increasingly dependent on modern information systems… The United States is more vulnerable to attacks than any other country in the world.’’ Iran—the world’s leading sponsor of international terrorism—in military writings openly describes EMP as a terrorist weapon, and as the ultimate weapon for prevailing over the West: ‘‘If the world’s industrial countries fail to devise effective ways to defend themselves against dangerous electronic assaults, then they will disintegrate within a few years… American soldiers would not be able to find food to eat nor would they be able to fire a single shot.’’ The threats are not merely words. The EMP Commission assesses that Russia has, as it openly declares in military writings, probably developed what Russia describes as a ‘‘Super-EMP’’ nuclear weapon—specifically designed to generate extraordinarily high EMP fields in order to paralyze even the best protected U.S. strategic and military forces. China probably also has Super-EMP weapons. North Korea too may possess or be developing a Super-EMP nuclear weapon, as alleged by credible Russian sources to the EMP Commission, and by open-source reporting from South Korean military intelligence. But any nuclear weapon, even a low-yield first generation device, could suffice to make a catastrophic EMP attack on the United States. Iran, although it is assessed as not yet having the bomb, is actively testing missile delivery systems and has practiced launches of its best missile, the Shahab–III, fuzing for high- altitude detonations, in exercises that look suspiciously like training for making EMP attacks. As noted earlier, Iran has also practiced launching from a ship a Scud, the world’s most common missile—possessed by over 60 nations, terrorist groups, and private collectors. A Scud might be the ideal choice for a ship-launched EMP attack against the United States intended to be executed anonymously, to escape any last-gasp U.S. retaliation. Unlike a nuclear weapon detonated in a city, a high-altitude EMP attack leaves no bomb debris for forensic analysis, no perpetrator ‘‘fingerprints.’’ Under present levels of preparedness, communications would be severely limited, restricted mainly to those few military communications networks that are hardened against EMP. Today’s microelectronics are the foundation of our modern civilization, but are over 1 million times more vulnerable to EMP than the far more primitive and robust electronics of the 1960s, that proved vulnerable during nuclear EMP tests of that era. Tests conducted by the EMP Commission confirmed empirically the theory that, as modern microelectronics become ever smaller and more efficient, and operate ever faster on lower voltages, they also become ever more vulnerable, and can be destroyed or disrupted by much lower EMP field strengths. Microelectronics and electronic systems are everywhere, and run virtually everything in the modern world. All of the civilian critical infrastructures that sustain the economy of the United States, and the lives of 310 million Americans, depend, directly or indirectly, upon electricity and electronic systems. Of special concern is the vulnerability to EMP of the Extra-High-Voltage (EHV) transformers, that are indispensable to the operation of the electric grid. EHV transformers drive electric current over long distances, from the point of generation to consumers (from the Niagara Falls hydroelectric facility to New York City, for example). The electric grid cannot operate without EHV transformers—which could be destroyed by an EMP event. The United States no longer manufactures EHV transformers. They must be manufactured and imported from overseas, from Germany or South Korea, the only two nations in the world that manufacture such transformers for export. Each EHV transformer must be custom-made for its unique role in the grid. A single EHV transformer typically requires 18 months to manufacture. The loss of large numbers of EHV transformers to an EMP event would plunge the United States into a protracted blackout lasting years, with perhaps no hope of eventual recovery, as the society and population probably could not survive for even 1 year without electricity. Another key vulnerability to EMP are Supervisory Control And Data Acquisition systems (SCADAs). SCADAs essentially are small computers, numbering in the millions and ubiquitous everywhere in the critical infrastructures, that perform jobs previously performed by hundreds of thousands of human technicians during the 1960s and before, in the era prior to the microelectronics revolution. SCADAs do things like regulating the flow of electricity into a transformer, controlling the flow of gas through a pipeline, or running traffic control lights. SCADAs enable a few dozen people to run the critical infrastructures for an entire city, whereas previously hundreds or even thousands of technicians were necessary. Unfortunately, SCADAs are especially vulnerable to EMP. EHV transformers and SCADAs are the most important vulnerabilities to EMP, but are by no means the only vulnerabilities. Each of the critical infrastructures has their own unique vulnerabilities to EMP: The National electric grid, with its transformers and generators and electronic controls and thousands of miles of power lines, is a vast electronic machine—more vulnerable to EMP than any other critical infrastructure. Yet the electric grid is the most important of all critical infrastructures, and is in fact the keystone supporting modern civilization, as it powers all the other critical infrastructures. As of now it is our technological Achilles Heel. The EMP Commission found that, if the electric grid collapses, so too will collapse all the other critical infrastructures. But, if the electric grid can be protected and recovered, so too all the other critical infrastructures can also be restored. Transportation is a critical infrastructure because modern civilization cannot exist without the goods and services moved by road, rail, ship, and air. Cars, trucks, locomotives, ships, and aircraft all have electronic components, motors, and controls that are potentially vulnerable to EMP. Gas stations, fuel pipelines, and refineries that make petroleum products depend upon electronic components and cannot operate without electricity. Given our current state of unpreparedness, in the aftermath of a natural or nuclear EMP event, transportation systems would be paralyzed. Traffic control systems that avert traffic jams and collisions for road, rail, and air depend upon electronic systems, that the EMP Commission discovered are especially vulnerable to EMP. Communications is a critical infrastructure because modern economies and the cohesion and operation of modern societies depend to a degree unprecedented in history on the rapid movement of information—accomplished today mostly by electronic means. Telephones, cell phones, personal computers, television, and radio are all directly vulnerable to EMP, and cannot operate without electricity. Satellites that operate at Low-Earth-Orbit (LEO) for communications, weather, scientific, and military purposes are vulnerable to EMP and to collateral effects from an EMP attack. Within weeks of an EMP event, the LEO satellites, which comprise most satellites, would probably be inoperable. Banking and finance are the critical infrastructure that sustain modern economies. Whether it is the stock market, the financial records of a multinational corporation, or the ATM card of an individual—financial transactions and record keeping all depend now at the macro- and micro-level upon computers and electronic automated systems. Many of these are directly vulnerable to EMP, and none can operate without electricity. The EMP Commission found that an EMP event could transform the modern electronic economy into a feudal economy based on barter. Food has always been vital to every person and every civilization. The critical infrastructure for producing, delivering, and storing food depends upon a complex web of technology, including machines for planting and harvesting and packaging, refrigerated vehicles for long-haul transportation, and temperature-controlled warehouses. Modern technology enables over 98 percent of the U.S. National population to be fed by less than 2 percent of the population. Huge regional warehouses that resupply supermarkets constitute the National food reserves, enough food to feed the Nation for 30–60 days at normal consumption rates, the warehoused food preserved by refrigeration and temperature control systems that typically have enough emergency electrical power (diesel or gas generators) to last only about an average of 3 days. Experience with storm-induced blackouts proves that when these big regional food warehouses lose electrical power, most of the food supply will rapidly spoil. Farmers, less than 2 percent of the population as noted above, cannot feed 310 million Americans if deprived of the means that currently makes possible this technological miracle. Water too has always been a basic necessity to every person and civilization, even more crucial than food. The critical infrastructure for purifying and delivering potable water, and for disposing of and treating waste water, is a vast networked machine powered by electricity that uses electrical pumps, screens, filters, paddles, and sprayers to purify and deliver drinkable water, and to remove and treat waste water. Much of the machinery in the water infrastructure is directly vulnerable to EMP. The system cannot operate without vast amounts of electricity supplied by the power grid. A natural or nuclear EMP event would immediately deprive most of the U.S. National population of running water. Many natural sources of water—lakes, streams, and rivers—would be dangerously polluted by toxic wastes from sewage, industry, and hospitals that would backflow from or bypass wastewater treatment plants, that could no longer intake and treat pollutants without electric power. Many natural water sources that would normally be safe to drink, after an EMP event, would be polluted with human wastes including feces, industrial wastes including arsenic and heavy metals, and hospital wastes including pathogens. Emergency services such as police, fire, and hospitals are the critical infrastructure that upholds the most basic functions of government and society—preserving law and order, protecting property and life. Experience from protracted storm-induced blackouts has shown, for example in the aftermath of Hurricanes Andrew and Katrina, that when the lights go out and communications systems fail and there is no gas for squad cars, fire trucks, and ambulances, the worst elements of society and the worst human instincts rapidly takeover. The EMP Commission found that, given our current state of unpreparedness, a natural or nuclear EMP event could create anarchic conditions that would profoundly challenge the existence of social order.

### 2NC---Russia Deterrence DA

#### Russian cyberattacks cause NC3 entanglement

Whyte ’22 [Christopher; March 31; assistant professor of homeland security and emergency preparedness in the L. Douglas Wilder School of Government and Public Affairs at Virginia Commonwealth University; World Politics Review, “Cyber and Nuclear Threats Make for a Dangerous Mix in Ukraine,” <https://www.worldpoliticsreview.com/articles/30439/cyber-and-nuclear-make-for-a-dangerous-mix-in-the-ukraine-war>/ceng

To say that the world is closer to the brink of nuclear war today than at any time since the Cuban Missile Crisis of 1962 feels less controversial by the day. United Nations Secretary-General Antonio Guterres recently told media representatives that the “prospect of nuclear conflict, once unthinkable, is now back within the realm of possibility.” Certainly, Russian President Vladimir Putin has been signaling a willingness to at least consider the nuclear option. In late February, he raised the readiness level of Russia’s nuclear response force, stating that Western interference in the ongoing war in Ukraine will result in “consequences greater than any you have faced in history.” And despite calming messaging from the Biden administration, further Russian mobilizations—including the deployment of nuclear missile launchers to Siberia and nuclear submarines to the Barents Sea for supposed “drills”—have continued to stoke public fears over nuclear weapons’ use. Even Russia’s recent pledge not to use nuclear weapons in Ukraine has done little to calm fears about the potential use of tactical nuclear devices, with many claiming the statement is nothing more than an attempt to bolster Moscow’s negotiating position. Amid these rising nuclear tensions, there is one dimension of potential escalation that has not yet received much public attention: that of a cyber-enabled nuclear event. It’s time for policymakers to consider whether cyber operations affecting elements of nuclear command, control and communications, or NC3, systems could prompt nuclear escalation in the current crisis. Experts across the West have been scrambling to place Putin’s threats, both tacit and explicit, in strategic and political context in order to gauge the possibility of a nuclear escalation leading to nuclear war. Others still have more narrowly—and perhaps more realistically—focused their analysis on what strong nuclear threats mean for fraught international engagement with Russia, and on whether Putin is likely to authorize the use of any nuclear weapons at all. On the digital side of things, experts on cyber conflict have thus far narrowly focused their attention on the non-nuclear aspects of tactics being employed in the war. Scholars rightly predicted that the “cyber blitzkrieg” anticipated by many pundits was unlikely, pointing out that, contrary to popular portrayals, cyber instruments actually make for poor tools of coercion and battlefield augmentation. By contrast, the entry of so many nonstate and semi-state cyber forces into the conflict on both sides, including nearly 300,000 volunteers coordinated by the Ukrainian government and a pro-Russia equivalent calling itself “Killnet,” was less expected. Even given so much robust analysis of the ongoing war, the nuclear tie-in has remained curiously underexamined. This is particularly concerning given the manner in which scholars have in recent years suggested that the logic of cyber warfare could undermine the logic of nuclear deterrence under highly specific circumstances. Overall, experts are right to dismiss the threat of a so-called “cyberwar,” a fantastical scenario that contradicts what we know about the strategic and operational functions of cyber instruments. But could cyber operations affecting elements of NC3 prompt nuclear escalation in the current crisis? Perhaps. The conflicting logics of cyber and nuclear warfare, when considered in the context of the present crisis, suggest real reasons to be concerned about the possibility of a cyber-enabled nuclear escalation. Off the bat, it’s important to remember that several elements involved in that question could present themselves in a range of ways. Nuclear escalation itself could take a number of forms, from additional escalatory rhetoric or mobilization to the actual use of a nuclear weapon. Likewise, a cyber operation impacting NC3 systems—which essentially comprise the networks of intelligence sensors, communications systems, other early warning assets and arms control mechanisms that underlie a country’s nuclear deterrent forces—could be an actual attempt to interfere with a nation’s deterrent capability by means of disrupting or taking over an element of its command system. That could be perceived by the targeted party as a prelude to a preemptive strike. But it could also be something as simple as an exploratory probe not intended to subvert system functions. Significantly, these different attacks could be hard to differentiate from the defensive perspective and so misinterpretation is entirely possible. While countries like Russia and the United States have historically reacted with caution to nuclear provocations, uncertainties borne of the current crisis might diminish that inclination. Such uncertainties could also encourage Russian leaders to lend less weight to the cyber attribution problem—that is, the difficulty inherent in identifying the party responsible for a cyber-attack that, even under ordinary circumstances, complicates efforts to organize an appropriate response. Even more concerning than the uncertainties bound up in interpreting certain cyber actions is the oft-cited and well-documented vulnerabilities of most states’ NC3 systems. Scholars have noted that NC3 weaknesses are widespread and, at times, quite glaring. There’s little doubt that American or Russian second-strike capabilities could be made to function effectively in the event of a nuclear war. But both sides’ reliance on a blend of new and legacy technologies to coordinate a complex detection, analysis and strike apparatus for nuclear weapons virtually guarantees errors in how these systems function as a whole. For example, in the past, American forces have lost contact with launch systems for hours due to faulty circuitry. At other times, they have detected false launches because legacy machinery was mishandled by operators. These base conditions are cause for at least minimal concern. Both the probability of either side’s NC3 systems being vulnerable to some form of cyber compromise and the possibility that either side might mistakenly believe its NC3 is being targeted by hostile foreign cyber operations clearly create the potential for a cyber-enabled nuclear event where perceived cyber-preemption against NC3 leads directly to either coercive or real military escalation. Admittedly, the stakes of nuclear weapons’ use suggest that escalation is not an especially likely outcome most of the time, even given these known issues. But unique circumstances might change this calculus. In particular, the conflicting logics of cyber and nuclear warfare, when considered in the context of the present crisis, suggest real reasons to be concerned. Nuclear and cyber forces are polar opposites with regard to their operational features. The former relies on open signaling to “warn” adversaries about potential consequences in order to generate a deterrent effect. The latter typically banks on secrecy, exploiting the element of surprise to avoid giving an opponent the opportunity to upgrade their defenses. The combination of the two creates unusual commitment problems, where the coercive brinksmanship usually on display in nuclear contests might be absent as one side tries to use cyber instruments to neutralize the other’s NC3. Importantly, with cyber in the mix, the side that detects cyber activity targeting NC3 will likely also notice that the attempted breach was done in secret, creating new uncertainties over how they might respond to such an attack. In addition to the potential weaknesses of NC3 systems, the unique political dynamics currently on display in Moscow, where Putin seems to be both isolated and dependent on politicized intelligence that has effectively undermined his decision-making, complicates this game of nuclear chicken. Given the difficult intelligence assessments and operational decisions that any government trying to reconcile cyber and nuclear logics in real-time will be required to make, this is worrisome to say the least. And Russia’s many obvious logistical failures in launching its invasion are cause for further concern. After all, objectively assessing the risks of cyber-enabled nuclear interference requires having the ability to locate potential NC3 compromises and to mitigate any that are found. This means robust intra-service communication and deployment of expertise, neither of which has been on prominent display in Moscow when it comes to the invasion of Ukraine. The range of cyber forces arrayed against Putin’s government in the current crisis also represents a potential source of further uncertainty that could produce cyber-prompted nuclear escalation. In addition to Ukraine’s cyber forces, which are active against Russian targets of all stripes, Kyiv has benefited from massive Western support for its operations in cyberspace, including from hacktivist elements to hundreds of thousands of volunteers that are being coordinated by Ukrainian state auspices. Added to this is the fact that, in addition to military equipment, Kyiv has been receiving non-battlefield aid from NATO member states, particularly those that are most geographically proximate, including Poland, Slovenia and the Czech Republic. There is clearly a narrow situation here in which Russian leadership, under the current internal political conditions, may see possible Western intention in cyber events involving NC3 or related systems.

#### It blurs the line of mutually assured destruction cascading in preemptive strikes---it’s the *only* scenario for nuclear war

Jacquelyn Schneider, 03-07-2022, (Jacquelyn Schneider is a Hoover Fellow at the Hoover Institution at Stanford University), “The Biggest Cyber Risk in Ukraine?, Foreign Affairs, https://www.foreignaffairs.com/articles/ukraine/2022-03-07/biggest-cyber-risk-ukraine/ceng

Why the apparent restraint? It is almost impossible to know exactly why (or if) the Russians have indeed held back. Perhaps cyber-operations have been attempted and failed; perhaps Russian President Vladimir Putin has held his cyber-capabilities in reserve, saving them for later. Or maybe cyber-operations have taken place, but their effect—which is often virtual and not clearly attributed—will take longer to materialize. What is known is that the conflict is far from over, and the next question becomes whether cyber-operations could play a larger role as the war turns more violent. It is likely that the next stage of conflict will more than ever be defined by planes, tanks, artillery, and soldiers. It seems unlikely, given the amount of indiscriminate damage currently being inflicted by Russia, that cyber-operations will escalate the violence of the campaign within Ukraine. That said, could cyber-operations lead to horizontal escalation, drawing NATO into the fight, for example? Or, given that the United States and Russia are the world’s largest nuclear powers, could cyber-operations escalate to the worst possible outcome—nuclear war? Recent wargaming research suggests that cyber-exploits into nuclear command and control may be enticing for states looking to neutralize a nuclear escalation threat in the midst of a conventional war, and that actors may underestimate the danger of these exploits and vulnerabilities to nuclear stability. GETTING PULLED IN One way cyber-operations could lead to escalation is by pulling the United States or NATO into the conflict. Mark Warner, the Democratic senator from Virginia, warned in late February that potential Russian cyberattacks on critical infrastructure in Ukraine could have accidental spillover effects on NATO countries—for instance if a Russian cyberattack on Ukrainian energy infrastructure caused an outage in a NATO neighbor like Poland. This could inadvertently trip Article 5 of NATO’s founding treaty, which states that an armed attack against one member state will be considered an attack against them all. This would be uncharted waters for NATO, which only recently publicly stated that cyberattacks might invoke Article 5 and is still ambiguous about what types of cyberattack—which range from virtual outages to data manipulations to physical damage (in extremely rare circumstances)—might be serious enough for NATO to respond with conventional retaliation. The Biden administration has warned that the United States would respond to cyberattacks on U.S. critical infrastructure, such as the country’s electrical grid or water supply (although officials stopped short of saying how the United States would respond). So far, the United States has answered previous cyberattacks with either sanctions, law enforcement actions, or the confiscation of cryptoassets. None of these options seem likely to deter Putin at this point, and so the Biden administration may find itself in an unprecedented position of having few credible options to threaten Russia. It is certainly possible that Putin, facing a conventional war that he thinks he might lose, could attack critical infrastructure in the United States or other NATO countries in the hope that their citizens will push their governments to abandon Ukraine. The financial sector, in particular, would seem to be a logical target for Russian cyberattacks, given the damage that Western economic actions have already done to the Russian economy. It is difficult to create widespread and long-lasting effects with cyberattacks, however, and the financial sector is the best equipped and most advanced cyber-defender in the world. Plus, research I’ve conducted with Sarah Kreps, director of the Cornell Tech Policy Lab, finds that the American public views cyberattacks as qualitatively different from conventional means of warfare—more akin to economic sanctions than bombs. Thus, cyberattacks are unlikely to provoke the kind of retaliation or emotional response that would pull the United States or its NATO allies into a war with Russia. What’s more, the United States can probably withstand the short-term damage to critical infrastructure that a Russian cyberattack might create, and such attacks might actually increase resolve to support Ukraine. This means a deliberate choice by Russia to use cyberattacks against the United States or NATO to “escalate to dominate”—deliberately ratcheting up the pressure to force Washington to back off—would likely fail. A more troubling scenario involves accidental escalation from cyber-operations—that is, when critical infrastructure is unintentionally damaged by a cyberattack or when a cyberattack is misattributed to Russia (or the United States). This is especially dangerous for civilian infrastructure that also serves military or security purposes—for example, harming a refugee train by using a cyberattack targeting railroads also used to move troops and supplies to the front. Plus, a jumble of actors has jumped into this space, from criminal syndicates to cyber-militias to hacker collectives such as Anonymous. That increases the chances that one of these players will target civilian infrastructure, and misattribution to either Russia or the United States could needlessly trigger retaliation. WHEN CYBER GOES NUCLEAR By far the most dangerous form of escalation is the possibility that a cyber-operation increases the likelihood of nuclear war. How likely is such a scenario? No one may know if Russia has a cyberweapon that can target nuclear weapons (or, for that matter, whether the United States does), but there are theories and some data about how the cyber-realm might affect nuclear stability. American policymakers have generally recognized that attempting to interfere with nuclear command, control, and communications could lead to dangerous incentives for states to launch nuclear weapons preemptively. Threats to nuclear command and control, for example, could leave states so fearful about their second-strike capability (the ability to launch a nuclear weapon in retaliation against an attacker) that in the midst of a conflict they would feel compelled to use nuclear weapons preemptively. Some scholars have warned that attacks against nuclear command-and-control systems could make it impossible to control nuclear war and keep it limited, leading to inadvertent nuclear Armageddon. Despite these fears about the dangers of attacking nuclear command and control, there was never an agreement between the United States and the Soviet Union (and subsequently Russia) to not attack each other’s nuclear command, control, and communications. Would Russia, or even the United States and its allies, launch a cyberattack against an enemy’s nuclear command-and-control system if they could? And how might that capability affect nuclear instability? Beginning in 2017, my team at the Naval War College and the Hoover Institution ran a wargame that explored this very question. It took place over three years and included 580 players from across the world—predominantly nuclear, cyber, and military experts ranging from former heads of state to military officers to industry leaders. In our simulations, we found that teams who were told they possessed cyber-exploits against nuclear command-and-control systems overwhelmingly used them. Because cyber-operations can be denied and are covert and virtual, players appeared to believe that they did not pose too great a risk of escalation. The tools seemed too valuable not to use, especially because they have a quick expiration date, with vulnerabilities quickly patched once discovered.

### 1NC---OCOs Good

#### Deterrence in cyberspace is possible and sufficient to avoid conflict, but NATO having offensive capabilities is necessary to prevent Russian malfeasance

Maldre 16 – Patrik Maldre, Adjunct Fellow at the Center for European Policy Analysis, “Moving Toward NATO Deterrence for the Cyber Domain,” May 2016, https://cepa.ecms.pl/files/?id\_plik=2446

Cyber deterrence clearly warrants more discussion among NATO members than ever, given the threats they now face—particularly from the East. Yet the Cyber Defence Committee doesn’t really cover it, nor will a full-fledged cyber deterrence concept be announced at the upcoming NATO summit in Warsaw. The main debate in Brussels and in national capitals centers on whether cyberspace should even be considered a domain of warfare, as many member states have already decide; the fuzzy concept of active cyber defense is only tentatively mentioned. However, senior NATO leaders have espoused deterrence as a potential future direction for the alliance. Importantly, several member states, including the United States, Britain and Estonia, are also publicly exploring such a strategy.20 The moment is not yet right for an alliance-wide declaration on this topic, but with concerted effort at all levels, NATO can and should continue to move toward deterrence for the cyber domain. Deterrence aims to discourage an adversary from taking offensive action. Traditionally, its two pillars have been deterrence-by-denial and deterrence-by-punishment. The first refers to measures that reduce or eliminate the benefits of a certain aggressive move, while the second seeks to impose additional costs for performing it. NATO’s traditional mandate of defending its own systems fits comfortably into the deterrence-by-denial part of this framework. Deterrence-by-punishment, however, is far more controversial because of the problem of attribution—which refers to the difficulty of identifying the perpetrators of operations. Finally, both concepts also rely on intent, capability and credibility. As it stands, a palpable lack of trust among member states hinders collective action on both fronts. Progress in the denial category will be easier and more visible, but countermeasures should be considered as well. NATO has come a long way in terms of working together to shore up technical defenses in cyberspace. The main barrier to further cooperation, however, is the difference in technical and administrative capacities as well as human and financial resources among member states. This, along with differing national views, remains the main barrier to further integration. The alliance is only as strong as its weakest member. When it comes to deterrence-by-denial, therefore, all member states must have the basics in place: computer security laws, national cyber strategies, a police focus on cybercrime, national CERTs, public-private partnerships and capable intelligence agencies. From there, members should enact effective, actionable information-sharing programs. After that, the next step is to develop joint situational awareness. Typically, adversary espionage campaigns target multiple NATO and memberstate organizations simultaneously. Early warning and shared situational awareness can prevent multiple entities in different countries from being breached by the same operation. The end goal for the denial part of the deterrence strategy is, of course, resilience. If NATO and its members can effectively work together to prevent, detect, respond and recover from cyber attacks, this would significantly decrease the benefits and increase the costs for an adversary. NATO collective action should continue in this direction, and joint efforts can help to promote trust and confidence—a key ingredient in further cooperation in deterrence-by-denial, but even more crucial when it comes to deterrence-by-punishment. Preventing adversaries from benefitting from offensive actions, or at least limiting their gains, can help discourage them from conducting such attacks in the first place. Punishing them after the fact is another. While the term has an aggressive connotation, this part of the strategy is defensive and retaliatory in nature. It can refer to a broad spectrum of actions—from naming-and-shaming to nuclear strikes. In the cyber domain, the problem of attribution hinders the goal of effective deterrence. For this reason, NATO and its member states should invest heavily in the technological and analytical capabilities necessary to discern signs of a particular adversary, including in cooperation with the private sector. As numerous cases of attribution to Russian cyber threat actors demonstrate, this is already taking place. Furthermore, member states should complement technical attribution with political and diplomatic attribution. Currently, months and even years pass before politicians and leaders feel comfortable about ascribing blame. For deterrence to work, however, governments must carry out both high-level and private attribution in conjunction with media and private companies as soon as they have conclusive evidence. Calling out threat actors and their state sponsors in diplomatic forums, public discussions and private meetings can motivate them to conduct less aggressive operations. NATO and its member states should also adopt joint approaches to developing and employing offensive capabilities for collective defense purposes. Laudably, many individual allies have already declared that they possess such capabilities and the doctrines for using them. However, considerable mistrust persists among the allies, creating an atmosphere of uncertainty and doubt—which weakens deterrence as a whole. To overcome this hurdle, allies can begin by making political statements about potentially using these capabilities in case of attack, and in accordance with international law as part of a collective defense response. Ultimately, NATO should move toward sharing these capabilities, perhaps by using existing models based on nuclear doctrine. Transparency and straightforwardness in this arena could contribute substantively to deterring adversaries and reinforce collective defense among NATO members. Intent and credibility will play into adversaries’ calculations for any type of countermeasure. For this reason, policy innovations and capability development need to be complemented by effective strategic communication. You cannot achieve deterrence if your adversary doubts that you’ll do what you say— and even less so if it doesn’t think you can do what you say. From this perspective, demonstrations such as the Aurora test in 2007 can be quite useful.21 Other, more subtle means include presentations by top officials at security conferences. Operations against third-party adversaries other than the intended target of deterrence can also deter attacks; few doubt that Russia paid close attention to the Stuxnet case, or that NATO drew conclusions from the Ukraine grid attack. In sum, effective strategic communication— both public and private—can be a key component or complement of a deterrence-by-punishment strategy.

#### The best outcome is adversary perception of NATO willingness to use OCOs aggressively.

Smeets and Lin '18 [Max and Herb; 11/28/18; senior researcher at the Center for Security Studies at Stanford University, PhD in International Relations from the University of Oxford; senior research scholar for cyber policy and security at the Center for International Security and Cooperation and Hank J. Holland Fellow in Cyber Policy and Security at the Hoover Institution at Stanford University; "An Outcome-Based Analysis of U.S. Cyber Strategy of Persistence & Defend Forward," https://www.lawfareblog.com/outcome-based-analysis-us-cyber-strategy-persistence-defend-forward]

From the U.S. standpoint, the optimal outcome is a United States that is more powerful in cyberspace along with a more stable cyberspace. Indeed, from the U.S. standpoint, the former will lead to the latter. A more stable cyberspace will involve norms of acceptable behavior, less conflict and so on. One path towards this rosy outcome is that the strategy does what it is said to do: Creates significant friction and makes it hard for adversaries to operate effectively. Adversaries realize that the U.S. strategy of persistent engagement makes it more difficult to conduct various offensive cyber operations, and they have no strong incentives to escalate as it may trigger a U.S. response in the conventional domain. USCYBERCOM has the advantage from the beginning.

#### Offensive capabilities allow iterative training that increases coordination

Lewis 15 – James A. Lewis, senior vice president and director of the Technology Policy Program at the Center for Strategic and International Studies, “The Role of Offensive Cyber Operations in NATO’s Collective Defence,” 2015, https://ccdcoe.org/uploads/2018/10/TP\_08\_2015\_0.pdf

It could be argued, given NATO’s defensive orientation ( pace Russian fears of diabolic plots), that a purely defensive and technical focus for cyber operations is appropriate. The question, however, is whether NATO can field a credible military force without some public linkage to an offensive cyber capability. Here again, the nuclear precedent offers some suggestions for a way forward. In the NATO phonetic alphabet, “whiskey” (“W”) and “romeo” (“R”) were used by NATO’s command structure in conflict to “warn” capitals that with a deteriorating situation on the ground it would be sending a request to release nuclear weapons for NATO use. Romeo was the actual request for release of nuclear weapons to NATO control. This terminology prepared nuclear capitals to make the decision on release. Just as nuclear weapons remain under national control but senior NATO commanders can request their release, the US and UK could retain control of offensive cyber capabilities but be prepared to make them available to NATO commanders upon request. In practice, national teams could be assigned to support NATO commanders in theatre or could carry out some operations against targets selected by NATO commanders form their national duty station. Such an arrangement needs more than ad hoc coordination. It requires an identified structure for request and release that is regularly practised. It demands offensive cyber operations used for defence purposes to be included in planning and exercises. It would also be beneficial for NATO’s defence mission if the exercise of systems for the use of offensive cyber capabilities in support of defensive operations was made public. Cyber operations necessitate advance planning and practice, particularly for multinational operations that are already inherently complex in their coordination and de-confliction requirements. Offensive cyber operations create conflicts between goals and missions for the use of cyber techniques. The fundamental decision is whether to collect intelligence or to engage in military operations. This creates an immediate problem for NATO, because decisions on intelligence collection will be taken at the national level whereas military operations are in the purview of the NATO military command structure. This consideration would necessarily be part of the decision process in national capitals, which would likely be an iterative process to allow for additional input from the theatre of operations.

### 1NC---Elections Turn

#### OCOs well in advance of threats secures elections.

Sulmeyer '18 [Michael; 2/13/18; Director of the Cyber Security Project at the Belfer Center for Science and International Affairs in the Harvard Kennedy School; "Testimony of Michael Sulmeyer," https://www.armed-services.senate.gov/imo/media/doc/Sulmeyer\_02-13-18.pdf]

In addition to improving defenses and becoming more resilient, we should also consider how best to counter threats abroad before they hit us at home. To that end, let me transition to how I see some potential roles for the military in protecting our elections. I will focus my remarks on roles that the military could play outside of the United States. There are two necessary conditions of posture that I see as critical: 1. Reconnaissance Posture: Our cyber mission forces should be constantly conducting reconnaissance missions abroad to discover election-related threats to the United States and provide indicators and warnings to our forces and decision-makers. There will never be sufficient resources to prioritize all threats equally, so prioritizing threats to our elections and our democratic processes is crucial. If we do not prioritize collecting information abroad about election-related threats, than we cannot hope to disrupt them. 2. Force Posture: Our cyber mission forces must be sufficiently ready to strike against targets abroad identified by reconnaissance as threats to our election. Readiness is a critical issue for our armed forces today, and I would encourage the Senators on this committee to ensure they are asking tough questions about the readiness of our cyber mission forces just as they would about any other area of our military. Our forces must be ready to create different effects against a range of targets. Sometimes, they will not have much notice, so developing tactics that can be employed on the fly is important. If the military’s reconnaissance and forces are postured to focus on threats to our elections from abroad, there are four objectives that our forces should be prepared to pursue. It should go without saying that undertaking these actions would need to be consistent with international law and other relevant U.S. commitments. 1. Preventing Attacks from Materializing: Based on election-focused reconnaissance, U.S. cyber mission forces should develop options to disrupt the activities of those planning to meddle in our elections, and those who are in the early steps of doing so. Because these would be actions conducted by U.S. forces with a relatively long lead time, scenario-based plans should be developed and socialized with decision-makers so they are aware of the viability, risks, and benefits of different options. 2. Preempting Imminent Attacks: Reconnaissance abroad may provide indicators and warnings of an imminent cyber attack against election-related infrastructure, campaigns, and media and social media platforms. Our forces can prepare to neuter those attacks before they commence. Such actions would need to be undertaken rapidly as opportunities to strike may be fleeting, so developing options in advance to deliver effects promptly when so ordered is essential.

#### The success of election interference disintegrates the global liberal order.

Kagan et al. 19 [Frederick; 2019; PhD in Russian and Soviet military history @ Yale, Director of the Critical Threats Project at the American Enterprise Institute, Associate Professor of Military History at the U.S. Military Academy at West Point, “Confronting the Russian Challenge: A New Approach for The U.S.,” http://www.understandingwar.org/sites/default/files/ISW%20CTP%20Report%20-%20Confronting%20the%20Russian%20Challenge%20-%20June%202019.pdf]

The Ideals of the American Republic

The stakes in the Russo-American conflict are high. Russian leader Vladimir Putin seeks to undermine confidence in democratically elected institutions and the institution of democracy itself in the United States and the West.1 He is trying to interfere with the ability of American and European peoples to choose their leaders freely and is undermining the rules-based international order on which American prosperity and security rest. His actions in Ukraine and Syria have driven the world toward greater violence and disorder. The normalization of Putin’s illegal actions over time will likely prompt other states to emulate his behavior and cause further deterioration of the international system. Moscow’s war on the very idea of truth has been perhaps the most damaging Russian undertaking in recent years. The most basic element of the Russian information strategy, which we will consider in more detail presently, is the creation of a sense of uncertainty around any important issue. Russia’s strategy does not require persuading Western audiences that its actions in Ukraine’s Crimean Peninsula or the Kerch Strait, which connects the Black Sea and the Sea of Azov, for example, were legal or justified.3 It is enough to create an environment in which many people say simply, “who knows?” The “who knows?” principle feeds powerfully into the phenomena of viral “fake news,” as well as other falsehoods and accusations of falsehoods which, if left unchecked, will ultimately make civil discourse impossible. The Kremlin’s propaganda does not necessarily need its target audiences to believe in lies; its primary goal is to make sure they do not believe in the truth. This aspect of Putin’s approach is one of the greatest obstacles to forming an accurate assessment and making recommendations. It is also one of the most insidious threats the current Russian strategy poses to the survival of the American republic. The good news is that the war on the idea of truth does not involve military operations or violence, though it can lead to both. The bad news is that it is extraordinarily difficult to identify, let alone to counter. Yet we must counter it if we are to survive as a functioning polity.

### 2NC---OCOs Good

#### Sustained, preemptive offense against the initial cyber threat is necessary against armed attack and armed force.

Bigelow '19 [Brad; June 2019; Principal advisor to Assistant Chief of Staff for Communications, Information Services and Cyber Defence for planning, delivery and operation of CIS and CD capabilities throughout Allied Command Operations and NATO Crisis Response Operations, MS in Space Systems Engineering from the US Air Force Institute of Technology; "What are Military Cyberspace Operations Other Than War?” https://ccdcoe.org/uploads/2019/06/Art\_10\_What-Are-Military-Cyberspace-OperationsOther-Than-War.pdf]

In recent testimony before the U.S. Senate Armed Services Committee, Michael Sulmeyer proposed “two necessary conditions of posture” for U.S. military cyber mission forces to be better prepared to defend the U.S. against foreign attempts to interfere with elections. First, “Our cyber mission forces should be constantly conducting reconnaissance missions abroad to discover election-related threats to the United States and provide indicators and warnings to our forces and decision-makers.” Second, “Our cyber mission forces must be sufficiently ready to strike against targets abroad identified by reconnaissance as threats to our election” (Sulmeyer, 2018). Although Sulmeyer’s proposal was in the specific context of reactions to Russian meddling in U.S. elections in 2016, at a more general level these two conditions apply to any application of military OCO capabilities: first, they are highly dependent upon sustained reconnaissance of potential adversaries and their systems; and second, they need to be maintained at a high level of readiness because there may be little or no warning before they need to be engaged. If a nation intends to use offensive cyberspace capabilities to precede or pre-empt kinetic operations, then operational preparation of the cyber battlefield must become “as routine as reconnaissance or surveillance of potential adversary activity” (Kehler, Lin & Sulmeyer, 2017). What does “operational preparation of the cyber battlefield” involve? Robert Chesney spells it out clearly in his analysis of the 2018 DOD Cyber Strategy: “Intrusions into the systems of potential adversaries in order to secure access of a kind that can be exploited for disruptive or destructive effect if and when the need later arises” (Chesney, 2018).

#### Offensive capabilities are necessary to adapt to changing adversary capabilities – the aff just establishes a cyber Maginot Line that is begging to be pushed back

Lewis 15 – James A. Lewis, senior vice president and director of the Technology Policy Program at the Center for Strategic and International Studies, “The Role of Offensive Cyber Operations in NATO’s Collective Defence,” 2015, https://ccdcoe.org/uploads/2018/10/TP\_08\_2015\_0.pdf

The nature of warfare is changing as opponents seek to circumvent Western military power by using a blend of political action, special forces, proxies and irregular units, unconventional tactics and cyber techniques to find a different way of applying force to gain their ends. What Russia sometimes call “hybrid warfare” will challenge NATO defence planning. A cyber defensive orientation is, however, the equivalent of a static defence, defending fixed positions rather than manoeuvring, and conceding initiative to opponents. The next public iteration of NATO cyber policy should describe how NATO members with offensive cyber capabilities would retain national control, but make these capabilities available to NATO in the event of aggression. NATO should be more explicit in how offensive cyber operations fit into its defensive and deterrent strategy. Finally, it needs to identify and describe a regular coordinating process to be established (similar to the Nuclear Planning Group) in NATO’s Cyber Defence Committee (CDC). NATO would never refrain from using fighter aircraft because they can serve offensive purposes, and say it would rely solely on air defence missiles and damage control to deal with the threat of air attack. Nor would NATO renounce armoured vehicles and rely only on static defence. A defensive approach that forsakes the possibility of offensive action is essentially a cyber Maginot Line. This defensive orientation serves no one’s interest except that of our opponents. Offensive cyber operations are similarly a part of warfare that advanced militaries cannot ignore. The mechanisms for incorporating offensive cyber into NATO will be complicated by national sensitivities, and public presentation will need to be carefully crafted to reinforce a deterrent message; but the next step, however politically difficult, for NATO transformation is to publicly embrace offensive cyber capabilities in planning and exercises. Warfare is evolving as technological and political developments change the requirements for effective operations. Military innovations create a new dynamic for calculating risk among potential adversaries. Forces and concepts that once seemed adequate for stability are called into question. It will be neither easy nor quick for NATO to discuss publicly the role of offensive cyber operations, but it is ultimately unavoidable.

#### Less cyber offense is the worst possible outcome.

Scott '18 [Tennille; 5/25/18; MS in Information Technology from the University of Maryland, MA in Military Operations from the US Army School of Advanced Military Studies, Cyber Operations Officer for the US Army; "The Art of the Cyber Jab: Using Defensive Cyberspace Operations-Response Action at Corps and Below," https://apps.dtic.mil/sti/pdfs/AD1071483.pdf]

Russian aggression in the cyber domain over the past decade show that mere passive response to cyber attack is not sufficient to prevail against a well-rehearsed adversary that combines offensive cyberspace operations with combat operations. Fear of the unknown cannot be an excuse for idleness, and the US cannot afford to be “cyber punching bags” in combat.103 Inactivity is not an option. Lieutenant General Nakasone told senators in a confirmation hearing March 1, 2018 “As cyberspace develops, the longer that we have inactivity, the longer our adversaries are able to establish their own norms – and I think that is very, very important that we realize that.” 104 This sentiment resonates with Moltke in his statement that “omission and inactivity are worse than resorting to the wrong expedient.”105 While DCO-RA may not be a perfect solution, as its analogies in the physical domain demonstrate, perfection is not always necessary. Overcoming an adversary is the art of combining what is possible with what is necessary to achieve defense. At some point the US must stop being the world’s cyber punching bag and counter its adversaries with a few cyber jabs of its own. This research demonstrates that DCO-RA, when fully and properly enabled, is capable of doing just that.

#### The best cyber defense is day-to-day cyber offense.

Bigelow '19 [Brad; June 2019; Principal advisor to Assistant Chief of Staff for Communications, Information Services and Cyber Defence for planning, delivery and operation of CIS and CD capabilities throughout Allied Command Operations and NATO Crisis Response Operations, MS in Space Systems Engineering from the US Air Force Institute of Technology; "What are Military Cyberspace Operations Other Than War?” https://ccdcoe.org/uploads/2019/06/Art\_10\_What-Are-Military-Cyberspace-OperationsOther-Than-War.pdf]

Some have argued that military operations in cyberspace outside the context of armed conflict should be limited to the protection of military networks and information systems. Miriam Dunn Cavelty has flatly stated that “Militaries cannot defend the cyberspace of their country – it is no space where troops and tanks can be deployed because the logic of national boundaries does not apply” (Dunn Cavelty, 2012). Stephen J. Anderson agrees, writing that traditional concepts of national defense cannot be applied in cyberspace: “The US Navy defends the littoral territorial boundaries; air defenses, either through missile defense initiatives or alert aircraft, define airspace boundaries. Those lines are not readily identifiable in cyberspace” (Anderson, 2016). Some go even further, arguing that an active military role in peacetime cyber security undermines investment in alternative mechanisms. In a 2013 post for the Lowy Institute, Ian Wallace wrote that such efforts disincentivized “other longer-term and more sustainable efforts to address the new challenges that cyber brings to security systems” (Wallace, 2013). Yet this debate has evolved significantly in recent years, in large part thanks to increasing evidence of state-sponsored attacks on civilian cyberspace infrastructure. In a recent paper entitled Rethinking Cyber Security, James Lewis has stated that “The primary source of risk in cybersecurity comes from conflict between states” (Lewis, 2018). This assessment is echoed by the Netherlands’ National Cyber Security Centrum, which concluded in its 2018 assessment that “The most significant threats are sabotage and disruption by nation-states” (National Cyber Security Centrum, 2018). As consensus on the state actor threat in cyberspace has grown, so have calls for the military to take a more active role in the defense of cyberspace. In the 2017 U.S. Senate deliberations on increasing the Secretary of Defense’s authority to conduct clandestine military cyberspace operations, Senator John McCain asserted that the need for a strong military role in peacetime was self-explanatory: “It’s the Department of Defense’s job to defend this nation: that’s why it’s called the Department of Defense” (Pomerleau, 2017). This more active role— sometimes referred to as defending forward—is reflected in recent updates to military cyber strategies. The 2018 U.S. Defense Department Cyber Strategy, for example, states explicitly: “We are engaged in a long-term strategic competition with China and Russia” and declares that this requires (and justifies) “action in cyberspace during day-to-day competition to preserve U.S. military advantages and to defend U.S. interests” (U.S. Department of Defense, 2018). Similarly, the Netherlands’ Defence Cyber Strategy 2018, subtitled Investing in cyber striking power for the Netherlands, concludes that the current security environment demonstrates that “a more active contribution from Defence within the existing structures is required” (Netherlands Ministry of Defence, 2018). Jan Kallberg and Thomas S. Cook have gone even further, stating that nations should be prepared not only to use military cyberspace forces in peacetime but to actively foster these capabilities as an alternative to armed conflict: “Cyber is no longer a mere enabler of joint operations, but instead a viable strategic option for confronting adversarial societies” (Kallberg & Cook, 2017).

#### Balance of tech favors offensively disarming adversaries.

Davis '19 [Susan; 4/18/19; General Rapporteur to the NATO parliamentary Assembly Science and Technology Committee; "NATO in the Cyber Age: Strengthening Security & Defense, Stabilizing Deterrence," https://www.nato-pa.int/download-file?filename=sites/default/files/2019-04/087\_STC\_19\_E%20-%20NATO.pdf]

27. Although cyber security and defence capabilities continue to improve, most experts argue that the offence has the advantage in cyber space and that this is unlikely to change soon. Given sufficient time, skills, and resources, attackers could easily perpetrate a cyber attack, finding the targeted system’s vulnerabilities, gaining access, and delivering their payload. This is a key reason why the Alliance must complement dissuasion with strategies of deterrence by punishment. In other words, they must try “to prevent an attack by threatening unacceptable damage so that in the attacker’s cost-benefit calculations the best choice is not to attack” (Morgan, 2009; italicised in original). It should be noted some experts would argue that the offence is not as dominant. For example, the more sophisticated cyber weapons are, the more opportunities the defender has to stop an attacker and the more errors the attacker is likely to make. Additionally, continued organisational deficiencies could be a key reason why the attackers have had the advantage thus far (Slayton, 2017).

#### Norms solves the DA

Aidan Simardone 18, junior research fellow at the NATO Association of Canada, “More than Security: NATO and the Rules-Based International Order in the Post-Cold War Era,” NATO Association of Canada, 5/23/18, http://natoassociation.ca/more-than-security-nato-and-the-rules-based-international-order-in-the-post-cold-war-era/

NATO’s increasing role in supporting the rules-based international order is tremendously valuable. Nevertheless, the Alliance’s record has not been perfect. Questions remain over the legality of its intervention in the Balkans, which did not receive approval from the U.N. Security Council, as airstrikes in Serbia and Libya contradicted international laws on excessive force. Double standards, such as the decision to intervene in Libya but not Syria, are numerous. While these cases may be exceptional, they can give the impression to other states that NATO only values the rules-based international order when it works in its interest. Were states to emulate this perceived self-interest, NATO actions would effectively help to undermine rather than protect the rules-based international order. As NATO moves forward, it must be conscientious of past mistakes and ongoing challenges. Tradeoffs are sometimes unavoidable, such as intervening to stop genocide without U.N. Security Council approval. However, in other cases NATO can take actions that fall closer in line with international laws and norms. Doing so will bolster NATO’s role in supporting the rules-based international order—a role that is becoming more central to NATO and gives vitality to the Alliance.

### 1NC / 2NC---OCOs Good – Nuke Terror

#### OCOs are critical to intelligence gathering – stops nuclear terrorism

Dr. Chris Bronk and Gregory S. Anderson, 17, (Dr. Chris Bronk and Gregory S. Anderson, Dr. Chris Bronk is an Assistant Professor of computer and information systems at the University of Houston’s College of Technology. He holds or has previously held appointments in Rice University's computer science department and Baker Institute for Public Policy and at the University of Toronto’s Munk School of Global Affairs. Until 2006, he served as a career diplomat with the U.S. Department of State on assignments both overseas and in Washington, D.C. He recently published the book, Cyber Threat: The Rise of Information Geopolitics in U.S. National Security Gregory Anderson is a master’s candidate for the Information Systems Security program at the University of Houston and is currently a research assistant under Dr. Chris Bronk and Dr. Arthur Conklin. He earned his bachelor’s degree in Business Computer Information Systems from the University of North Texas., 2017, Published by Army Cyber Institute, The Cyber Defense Review , Vol. 2, No. 1 (WINTER 2017), pp. 93-108, “Engaging ISIL in Cyberspace” https://www.jstor.org/stable/pdf/26267403.pdf, 6-26-2022) SCade

There will no doubt be difficulties incorporating cyber operations components into overall US strategy countering ISIL and other non-state adversaries; however, it is clear national security leadership in Washington will leverage cyber capabilities more significantly. One issue that will continue to dog offensive cyber operations and intelligence activities is the equities question—should the US government turn over knowledge it accrues regarding cyber vulnerabilities to the technology industry so that they may be repaired. For instance, is it more desirable for USCYBERCOM and the National Security Agency (NSA) to keep information regarding broken encryption implementations or software as was alleged in the Heartbleed bug in the OpenSSL software libraries? Issues such as this will be a major policy question to consider.

Ultimately, the cyber conflict against ISIL will serve as a template for future cyber action against terror groups, insurgents, and violent transnational criminal syndicates. Looking backward, we can see the effective application of robust signals intelligence capabilities have been. Consider US support of Colombian operations against the Fuerzas Armadas Revolucionarias de Colombia (FARC). There can be little doubt that the Colombian military and police were made significantly more effective with the addition of US intelligence capabilities. Policymakers are keen to eradicate or at least damage ISIL but will need to ask how cyber weapons can frustrate it as much as anything else can. The more cyber tactics can short-circuit ISIL’s operational capabilities, the better. What is necessary for US cyber operators are clear objectives from senior leadership on what they want to produce. The engineers that build USCYBERCOM’s tools and the hackers that serve as its operational forces can easily enough push back on what they believe is the art of the possible.

#### Terrorism causes nuclear war

Arguello 18—Founder and chair of the NPSGlobal Foundation, and head of the secretariat of the Latin American and Caribbean Leadership Network, degree in physics, a Master’s in business administration, and completed graduate studies in defense and security, previously worked on nuclear projects for the Argentine National Atomic Energy Commission. She is a member of the Steering Committee of the Fissile Materials Working Group, and a Chatham House Associate Fellow. Since 2010, she has participated in all the official non-governmental events at the Nuclear Security Summits [Irma Arguello and Emiliano J. Buis (a lawyer specializing in international law. He holds a PhD from the University of Buenos Aires (UBA), a Master’s in Human and Social Sciences from the University of Paris/Panthéon-Sorbonne, and a postgraduate diploma in national defense from the National Defense School. Currently he is a professor in international law at UBA, and co-director of the UNICEN Center for Human Rights in Azul. He is also a researcher and professor at the NPSGlobal Foundation), February 2018, “The global impacts of a terrorist nuclear attack: What would happen? What should we do?,” Bulletin of the Atomic Scientists, 74:2, 114-119

Though hard to accept, the detonation of a nuclear device – by states or non-state actors – is today a plausible scenario. And while much of the world’s focus has been on the current nuclear weapons arsenals possessed by states – about 14,550 warheads, all of which carry the risk of intentional or unintentional use – the threat of nuclear terrorism is here and increasing. For more than a decade, Al Qaeda, Aum Shinrikyo, and other terrorist groups have expressed their desire to acquire fissile material to build and detonate an improvised nuclear bomb. None of them could fulfill that goal – so far. But that does not mean that they will not succeed in the future. Making matters worse, there is evidence of an illicit market for nuclear weapons-usable materials. There are sellers in search of potential buyers, as shown by the dismantlement of a nuclear smuggling network in Moldova in 2015. There certainly are plenty of sites from which to obtain nuclear material. According to the 2016 Nuclear Security Index by the Nuclear Threat Initiative, 24 countries still host inventories of nuclear weapons-usable materials, stored in facilities with different degrees of security. And in terms of risk, it is not necessary for a given country to possess nuclear weapons, weapons-usable materials, or nuclear facilities for it to be useful to nuclear terrorists: Structural and institutional weaknesses in a country may make it favorable for the illicit trade of materials. Permeable boundaries, high levels of corruption, weaknesses in judicial systems, and consequent impunity may give rise to a series of transactions and other events, which could end in a nuclear attack. The truth is that, at this stage, no country in possession of nuclear weapons or weapons-usable materials can guarantee their full protection against nuclear terrorism or nuclear smuggling. Because we live in a world of growing insecurity, where explicit and tacit agreements between the relevant powers – which upheld global stability during the post-Cold War – are giving way to increasing mistrust and hostility, a question arises: How would our lives be affected if a current terrorist group such as the Islamic State (ISIS), or new terrorist groups in the future, succeed in evolving from today’s Manchester style “low-tech” attacks to a “high-tech” one, involving a nuclear bomb, detonated in a capital city, anywhere in the world? We attempted to answer this question in a report developed by a high-level multidisciplinary expert group convened by the NPSGlobal Foundation for the Latin American and Caribbean Leadership Network. We found that there would be multiple harmful effects that would spread promptly around the globe (Arguello and Buis 2016); a more detailed analysis is below, which highlights the need for the creation of a comprehensive nuclear security system. The consequences of a terrorist nuclear attack A small and primitive 1-kiloton fission bomb (with a yield of about one-fifteenth of the one dropped on Hiroshima, and certainly much less sophisticated; cf. Figure 1), detonated in any large capital city of the developed world, would cause an unprecedented catastrophic scenario. An estimate of direct effects in the attack’s location includes a death toll of 7,300-to-23,000 people and 12,600-to-57,000 people injured, depending on the target’s geography and population density. Total physical destruction of the city’s infrastructure, due to the blast (shock wave) and thermal radiation, would cover a radius of about 500 meters from the point of detonation (also known as ground zero), while ionizing radiation greater than 5 Sieverts – compatible with the deadly acute radiation syndrome – would expand within an 850-meter radius. From the environmental point of view, such an area would be unusable for years. In addition, radioactive fallout would expand in an area of about 300 square kilometers, depending on meteorological conditions (cf. Figure 2). But the consequences would go far beyond the effects in the target country, however, and promptly propagate worldwide. Global and national security, economy and finance, international governance and its framework, national political systems, and the behavior of governments and individuals would all be put under severe trial. The severity of the effects at a national level, however, would depend on the countries’ level of development, geopolitical location, and resilience. Global security and regional/national defense schemes would be strongly affected. An increase in global distrust would spark rising tensions among countries and blocs, that could even lead to the brink of nuclear weapons use by states (if, for instance, a sponsor country is identified). The consequences of such a shocking scenario would include a decrease in states’ self-control, an escalation of present conflicts and the emergence of new ones, accompanied by an increase in military unilateralism and military expenditures.

### 2NC - A2: OCOs escalate

#### OCOs don’t escalate – can be scaled back at any time

Christian Leuprecht, 19, (Christian Leuprecht, He is Department of Political Science and Economics, Royal Military College, Kingston, Canada, 3-27-2019, Taylor &amp; Francis, The Damoclean sword of offensive cyber: Policy uncertainty and collective insecurity, https://www.tandfonline.com/doi/abs/10.1080/13523260.2019.1590960?journalCode=fcsp20, 6-26-2022) SCade

To date, no direct use of OCO capabilities has resulted in the outbreak of traditional conflict, perhaps owing to uncertainties in the novelty of the attacks, the difficulty of attribution, and the reluctance of national cyber actors to retaliate when the path of escalation is unclear (Rid & Buchanan, 2015). Most importantly, however, the actions of armed forces in democratic countries are constrained by the rule of law, which translates into multiple authorities to ensure responsible and acceptable use, and safeguard against escalation. The fine-grained control of OCOs compared to conventional military force provides a way to manage escalation without the direct use of physical or military assets, whose effect in sparking conflict is much better known. In other words, instead of reacting to an escalating conflict by deploying physical military assets to a region, an OCO can be employed covertly to incur more controllable costs on the adversary, with the benefit of plausible deniability (Hare, 2018). Depending on the type of OCO employed, if there is a reduction in tension, the effects of the OCO can be reversed or scaled back

### 2NC---Inevitable

#### Allied OCOs are inevitable

Iftimie ’20 [Ion A.; May; PhD, Eisenhower PhD Candidate Fellow, NATO Defense College, and Senior Advisor, European Union Research Center, George Washington University School of Business; NDC Policy Brief, “NATO's needed offensive cyber capabilities,” no. 10]

At the 2016 NATO Summit in Warsaw, cyberspace was recognized as an operational domain in which NATO military forces must be able to maneuver as effectively as they do on land, at sea and in the air. Since then, Allies have conducted several successful offensive cyber operations1 against non-state adversaries, such as Daesh. Due to technological transformations in recent years, cyber is no longer viewed by NATO and its member states only as a hybrid threat, but also as a weapon in its own right and as a force multiplier2 in current military operations. Over the next two decades, NATO will look for new ways to integrate cyber weapons (or offensive cyber capabilities) into its operations and missions.3

#### The only question is whether they’re unilateral or collectively integrated---unilateral OCOs cause cyber fratricide

Iftimie ’20 [Ion A.; May; PhD, Eisenhower PhD Candidate Fellow, NATO Defense College, and Senior Advisor, European Union Research Center, George Washington University School of Business; NDC Policy Brief, “NATO's needed offensive cyber capabilities,” no. 10]

The lack of integrated offensive cyber A2/AD capabilities undermines both the unity of the Alliance and its mandate of defence and deterrence. On the former, the lack of coordination between Allies during unilateral cyber operations could lead to friction when resulting effects infringe on Allied cyber-physical infrastructures. It could also lead to cyber fratricide, when failure to properly attribute Allied digital personas occurs during these military operations. On the latter, while most Allies are developing offensive cyber capabilities, some remain unable to face the growing number of cyber threats unilaterally.

#### OCOs won’t escalate uncontrollably.

Sørensen ’19 [Heine; March; 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, Mhttps://tinyurl.com/y6cko3at]

One of the greatest reservations against communicating a willingness to take punitive actions concerns the risk of escalation and increased tension due to a more assertive or offensive posture. Yet when looking into possible responses – retaliation in cyberspace, for example – a number of “self-dampening” mechanisms appear to be in place that may be applicable to many types of responses.30 One example is the requirement to establish some level of attribution of aggression on which to base a response. As discussed above, while attribution is rarely impossible, it can be a time-consuming and technically-challenging endeavor. In a high-stakes scenario the time taken to get attribution as right as possible means there will be plenty of time to think twice about actions and consequences, and to lean on diplomatic measures in parallel. An example of a self-dampening mechanism related to the cyber domain is the large investment required to develop credible offensive capabilities. Moreover, an offensive cyber capability is a transitory tool31. The ability to access a computer system or network to cause harm or damage is only temporary and dependent on a very rapid and ongoing patching of vulnerabilities. At the same time, wielding the cyber instrument despite the downside of “burning” the capacity might have a de-escalatory effect by communicating capability and credibility to the opponent with a view to discouraging future hostile attacks. Targeting in any domain – including cyberspace – must also follow relevant rules, law and due-process which will self-limit the range of targets and actions available. A final “escalatory showstopper” is related to the challenge of identifying and developing targets of adequate strategic significance – not too much, not too little – to achieve the desired effect. Responding to hybrid aggression by applying “middle range” punitive actions that are proportionate to the aggression threatened or suffered will also self-limit the escalatory potential. It is unlikely to be in the interest of any hybrid aggressor to pursue an escalatory spiral above and beyond where they were looking to compete in the first place: on the hybrid level. Nevertheless, one way to mitigate the risk of escalation – while enhancing civilian oversight and interagency coordination – would be to establish rules of engagement for punitive actions on the hybrid level32 . This would provide decision-makers with common guidelines to pursue punitive actions that fall below the “use of force threshold”. Moreover, this could actually bolster the credibility of punitive actions by signaling to hybrid aggressors the intent to take pre-prepared punitive actions when deemed necessary: in other words, a “playbook” for countering hybrid threats.

### 1NC---AT: Russia War

#### No Russia war – they won’t risk it

Woolf 21 – Amy F, Specialist in Nuclear Weapons Policy in the Foreign Affairs, Defense, and Trade Division of the Congressional Research Service at the Library of Congress, received a Master’s in Public Policy from the Kennedy School of Government at Harvard University in 1983. “Russia’s Nuclear Weapons: Doctrine, Forces, and Modernization”, CRS, <https://sgp.fas.org/crs/nuke/R45861.pdf>, 09-13-2021

One analyst has postulated that **Russia may actually** **raise its nuclear threshold** **as it bolsters** its **conventional forces**. According to this analyst, “**It is difficult to understand why** **Russia would want to pursue military adventurism** **that would risk all-out confrontation** **with a technologically advanced and nuclear-armed adversary like NATO**. **While** **opportunistic**, **and possibly even reckless**, **the Putin regime does not appear to be suicidal**.” 144 **As a study from** the **RAND** Corporation **noted**, **Russia has “invested considerable sums in developing and fielding long-range conventional strike weapons since the mid-2000s to provide Russian leadership with a buffer against** **reaching the nuclear threshold**—**a set of conventional escalatory options that can achieve strategic effects without resorting to nuclear weapons**.”145 Others note, however, that Russia has integrated these “conventional precision weapons and nuclear weapons into a single strategic weapon set,” lending credence to the view that Russia may be prepared to employ, or threaten to employ, nuclear weapons during a regional conflict.

#### Their impact starts at 0.38%

Rodriguez 19 – Lusia, research fellow at the Forethought Foundation for Global Priorities Research, she also researched nuclear war at Rethink Priorities and as a visiting researcher at the Future of Humanity Institute, holds an M.A. from The Heller School for Social Policy and Management at Brandeis University. “How likely is a nuclear exchange between the US and Russia?”, Effective Altruism Forum, <https://forum.effectivealtruism.org/posts/PAYa6on5gJKwAywrF/how-likely-is-a-nuclear-exchange-between-the-us-and-russia>, 06-19-2019

My previous posts address how bad a nuclear war is likely to be, conditional on there being a nuclear war (see [this post on the deaths caused directly by a US-Russia nuclear exchange](https://forum.effectivealtruism.org/posts/pMsnCieusmYqGW26W/how-bad-would-nuclear-winter-caused-by-a-us-russia-nuclear), and [this post on the deaths caused by a nuclear famine](https://forum.effectivealtruism.org/posts/dtQ5hpYjniYKWhmhx/would-us-and-russian-nuclear-forces-survive-a-first-strike)), but they don’t consider the likelihood that we actually see a US-Russia nuclear exchange unfold in the first place. In this post, **I get a rough sense of how probable a nuclear war might be by looking at historical evidence**, **the views of experts**, **and** **predictions made by forecasters**. **I find that, if we aggregate those perspectives**, there’s about a 1.1% chance of nuclear war each year, and **that the chances of a nuclear war between the US and Russia, in particular, are around 0.38%** per year.

Table

Description automatically generated

### 2NC---AT: Russia War

#### No way Russia fights NATO – it’s strong now and they know they’d lose. Even if they raise the stakes, they’d never pursue adventurism because NATO is way stronger, Putin isn’t suicidal, and there is no public appetite for war – prefer our ev – it’s a review of security analysts who conclude the total likelihood of war is less than one percent, which means any risk of our DA should massively outweigh – that’s Woolf & Rodriguez

#### No Russia impact – too many constraints AND neither side risks war.

Mueller 21 – John, Adjunct Professor of Political Science and Senior Research Scientist at the Mershon Center for International Security Studies at Ohio State University, Senior Fellow at the Cato Institute, and member of the American Academy of Arts and Sciences. “The Stupidity of War: American Foreign Policy and the Case for Complacency, Chapter 6: The Rise of China, the Assertiveness of Russia, and the Antics of Iran”, Cambridge University Press, pg. 150-157, 03-04-2021

Russian Assertiveness The notion that a **major war among** **developed** **countries is** **wildly unlikely** **has** **frequently** **been taken to have been challenged by the** experience of the **armed dispute between** **Russia and** neighboring **Ukraine** **that began in 2014**. It resulted in the peaceful, if extortionary, transfer of Crimea, a large peninsular chunk of Ukraine, to Russia, and then in a sporadic, and ultimately stalemated, civil war in Ukraine in which ethnic Russian secessionist groups in a portion of Ukraine’s east were supported by Russia. The fear, in particular, is that Russia’s successful expansion – justified, it says, in part by the desire to protect persecuted ethnic Russians in a neighboring land – will cause, or tempt, it to expand elsewhere reflecting the manner in which Hitler expanded in order, he said, to protect ethnic Germans from persecution particularly in areas to his east. Indeed, NATO planners busily check roads in Western Europe to see if they are suitable for military transport in the event that Russia launches a full-scale invasion of the continent.50 And in 2018, at the badgering of President Donald Trump, NATO countries all agreed to increase their defense spending to 2 percent of gross domestic product by 2024, something he implied was a triumph although it merely reaffirmed a commitment they had made at the time of the Crimean takeover in 2014. 51 In the settlement that led to the unification of Germany in 1990, the United States verbally promised that, although East Germany would now become part of a NATO country, there would be no further expansion of the alliance to the east.52 A few years later, however, NATO began just such an expansion very much against many agitated concerns by specialists. Among these was George Kennan who warned that “the Russians will react quite adversely” and called the policy “a tragic mistake,” pointing out that “there was no reason for this whatsoever. No one was threatening anyone else.”53 The expansion was carried out with good intentions. and there were many statements seeking to mollify Russian concerns including offering it a sort of adjunct position in the alliance with the possible further prospect of actual membership.54 Nevertheless, although the Russians were powerless to stop the expansion, they greeted it with considerable dismay and opposition, voiced not just by Communists and by ultra-nationalists, but by very many in the Western-oriented elite. This should have been a warning. But it wasn’t. As Christopher Fettweis observes, “In the 1990s, Russian protests regarding NATO expansion – although nearly universal – were not taken seriously, since U.S. planners believed the alliance’s benevolent intentions were apparent to all.”55 The situation was strained further in 1999 when NATO bombed Serbia, a country with considerable historical links to Russia, securing the secession of the Kosovo province as Russia stood by helplessly, a development discussed in Chapter 3. Russia sometimes sees this as precedent for its Crimean seizure. As he was taking office as president of Russia in 2000, Vladimir Putin did tell a British interviewer, “Russia is part of European culture and I can’t imagine my country cut off from what we often refer to as the ‘civilized world’.”56 However, the strains from NATO expansion and from the Kosovo experience were already in place, and they gradually escalated in the new century as Putin’s regime became increasingly autocratic and as the United States, and particularly Secretary of State Hillary Clinton, together with its West European allies issued strong support for anti-Putin protests that took place in Russia in 2011–12. 57 Russia’s concern about NATO enlargement focused especially on the possible Westernization of Ukraine, the large new country to its west that had previously been part of the Soviet Union. One American observer who had served in the Obama administration supplies an arresting parallel: “The United States would hardly sit by idly if Russia formed an alliance with Mexico and Canada and started building military installations along the US border.”58 Unlike the neighboring countries to its west in what had previously been known as “East Europe,” Ukraine, although fairly open and democratic, had become a basket case economically despite an enormous potential. A few statistics may serve. After the breakup of the Soviet Union in 1991, Ukraine’s per capita GDP was higher than Poland’s; 25 years later, it was less than onethird that of Poland.59 In a study comparing 25 post-Communist countries, Ukraine comes out dead last in economic growth.60 Ukraine is now the poorest country in Europe.61 In this, it was like other, smaller counties that essentially lie between Russia and Western Europe: Moldova, Georgia, Armenia, Azerbaijan, and Belarus. These countries have been characterized not by the substantial political liberalization and economic development that has variously taken place in Poland, Hungary, the Czech Republic, Slovakia, Latvia, Lithuania, Estonia, Bulgaria, and Romania, and in countries that emerged out of Yugoslavia after its breakup in 1991. Rather, the “in-between” countries, led by the most important, Ukraine, suffer from a set of what Samuel Charap and Timothy Colton call “post-Soviet pathologies”: dysfunctional governmental institutions, economies lacking functioning markets, a rule of law that is weak or absent, patronal politics, close links between political power and control of major economic assets, and “pervasive corruption.”62 In the case of Ukraine, this phenomenon has been exacerbated by outside efforts from Russia and from Europe to influence the country. These have made it easier for Ukraine to avoid desperately-needed reforms.63 Among these are huge economic distortions concerning energy. The world average for energy consumption per dollar of GDP is 10 British thermal units. For the US it is 7.5, for the UK 3.8, for Ukraine 56.3. 64 Things came to a head when mass protests by Western-oriented Ukrainians broke out in the capital city, Kiev. Their duly elected president, who was perhaps even more corrupt than his equally duly elected predecessors, had been juggling various opposing aid offers from the West and from Russia. When he more or less accepted the (higher) Russian bid, protests broke out, and these endured through the cold and snowy winter of 2013–14 heightened by sporadic violence by security forces and by elements within the protest movement, particularly those from the highly anti-Russian far right.65 In February 2014, Ukraine’s president fled to Russia abruptly leaving the extravagant private zoo he had created behind.66 In the subsequent chaos, parliament removed provisions that had previously allowed the use of Russian as an official language under some conditions.67 Largely ignored in these development were the interests of Russian speakers in the country, some 30 percent of the population, who are concentrated in the east and south and were decidedly unsympathetic to the Kiev protests.68 This was particularly the case in the large Crimea peninsula to the south where Russia, by an agreement brokered when the Soviet Union split up in 1991, maintains a substantial naval base for its Black Sea Fleet. Putin was alarmed at the developments in Kiev where anti-Russian ideologues now occupied one-third of the cabinet seats. He was also deeply concerned that the new government might abrogate or fail to renew the lease on the naval base, seen to be vital national asset.69 And he was doubtless miffed that Western leaders had boycotted the winter Olympics he had hosted a few months earlier.70 He bolstered troop strength at the naval base, and soon men in green uniforms without insignia (known as “little green men”) were fanning out in Crimea occupying military and government facilities.71 Crimean Russians often felt neglected over the years by government in Kiev, and they feared after the fall of the president that they would be violently persecuted.72 The local Crimean authorities organized a referendum on secession and on March 16, 2014, a vote, boycotted by many, was held in which 97 percent of those who voted supposedly supported leaving Ukraine and joining Russia. Backed enthusiastically by his parliament and by the citizenry of Russia, Putin graciously accepted the request. Meanwhile, in Donbas – areas abutting Russia in eastern Ukraine – local Russians, emboldened by the events in Crimea, organized a secession movement, setting up their own ad hoc governments. Ukrainian armed forces, led initially mainly by volunteer paramilitaries, were sent to put them down.73 Aided by infiltrators from Russia, the secessionists were able to hold them to a stalemate. Over 10,000 were killed in the violence.74 Ukraine cut off financial subsidies, electricity, and water supplies to Crimea, and tourism, an important Crimean industry, dropped precipitously. But Russia, at considerable cost, worked to alleviate these problems, and in 2018 a 12-mile $3 billion bridge – the contract went to one of Putin’s buddies, a former judo partner – had been constructed to link Crimea with Russia, a country that, otherwise, ranks ninety-fourth in the world in infrastructure. Putin drove the first truck across the span himself.75 Efforts to integrate Crimea into Russia have been extensive, and Russian retirees (especially military ones) are encouraged to move there even as those opposed to the Russian takeover often emigrate to Ukraine. If the goal of Russia was to keep Ukraine from seeking to embrace the West while, in Robert Person’s words, “establishing a pliant pro-Russian regime in Kiev,” its efforts failed miserably.76 As one observer predicted at the time, “Far from dissuading Ukrainians from seeking a future in Europe, Moscow’s moves will only foster a greater sense of nationalism in all parts of the country and turn Ukrainian elites against Russia, probably for a generation.”77 Or as Daniel Treisman observed in the aftermath, “If Putin’s goal was to prevent Russia’s military encirclement, his aggression in Ukraine has been a tremendous failure, since it has produced the exact opposite.”78 In addition, **Russia’s** **experience in the 2014 conflict** and crisis in Ukraine **suggests that** **countries cannot engage in** such **enterprises without** **automatically** **paying a substantial** **economic price – it is something like an** **economic doomsday machine**. Because of its antics, **Russia suffered a decline in the** **value** **of its currency**, **capital flight**, **a drop in its** **stock market**, **and a decline in** **foreign investment**. And, perhaps most importantly, **there was a** **very substantial drop** **in confidence by investors, buyers, and sellers** throughout the world, a condition that is likely to last for years, even decades.79 As Charap and Colton stress, “Moscow is at serious risk of permanently alienating the entire EU, which as a bloc has long been Russia’s largest trading partner and direct investor.”80 One prominent British observer puts it even more starkly, suggesting that the events “mark the end of an era, the end of the hope that Russia could be incorporated into a united and peaceful Europe.”81 As part of this, Russia’s behavior has set off a determined effort by Europeans to reduce their dependence on Russian energy supplies – a change that could be permanent. And **the** **costs** **of** the conflict and of supporting its new distant dependencies **have been visited by Russia on itself**. Crimea was less well off economically than most of Ukraine and required subsidies from Kiev.82 And the Donbas region was heavily subsidized by Ukraine as well.83 These **burdens** **have** now **shifted to Russia**. **There have been** other **economic costs** as well. Economic **sanctions** have been **visited on Russia** **by other states**. Although especially costly to Europe, they were embraced after rebels in eastern Ukraine (perhaps accidentally) shot down a civilian airliner with a missile presumably supplied by Russia.84 Unrelated to the crisis, there was a severe drop in prices for oil on the international market, a development that is especially harmful to Russia: for every decline of $25 in the price of oil, Russia experiences a nearly 2 percent decline in GNP, and oil and gas sales fund about 36 percent of the Russian annual budget. The economic pain inflicted by the oil price drop has been much greater – perhaps four times greater – than that of the sanctions.85 There is **likely** as well **to be a** **special political cost for Putin**. Since he came to power in 2000, there has been a steady improvement in Russia each year in GDP per capita. That process was reversed in 2014. From 2014–17, real disposable income fell by 15 percent.86 Aspirational purchases as for homes and cars have shifted to ones devoted to daily needs.87 And Russia’s Stabilization Fund, built up when oil prices were high and meant to fund pension payments and to support the ruble, was significantly depleted and may run out of money entirely. Over time, **some** may **see this as a** **break** **with his promise to** **provide** **the** **stability and order** **necessary to allow economic progress** to take place.88 The **developments in Ukraine** in 2014 **were** **unsettling**, of course. However, **it is** **impressive** that **the United States and** Western **Europe** **never even came close to seriously considering the use of direct force** to deal with the issue. Although the crisis created, as Steven Pinker notes, “just the kinds of tensions that in the past had led to great-power wars,” nothing like that took place.89 In fact, **the West behaved in much** **the same way it would have** behaved **if it had** **not possessed** **a great and expensive** **military capacity**. Indeed, President Barack Obama, who presided over the episode, was given to taunting his hawkish critics: “Now, if there is somebody in this town that would claim that we would consider going to war with Russia over Crimea and eastern Ukraine, they should speak up and be very clear about it.”90 The **events** **inspired concerns** that **Putin had or has wider intentions**.91 The **natural** **next step**, suggest some, **would be some sort of invasion of the** **Baltic states** of Latvia, Lithuania, and/or Estonia. **Each**, like Ukraine, **has a Russian minority** which, in many cases, has not blended in well with the majority culture and might even consider itself to be persecuted. West Point’s Robert Person has **looked at** the **parallels** **and finds them wanting**.92 To begin with, **Ukraine has** what Person calls “**a** **deep symbolic meaning** **for Russia**.” It had been part of the Russian empire since the sixteenth century and is often considered to be “the cradle of eastern Slavic civilization.” Moreover, Crimea did not become part of Ukraine until it was “gifted” to that Soviet republic in 1954 by Nikita Khrushchev in a process that was quixotic and arbitrary and never actually made official even by the regulations of Soviet or Communist law.93 And, of course, Crimea’s Russian naval base added special significance. **By contrast**, continues Person, **Latvia**, **Lithuania**, **Estonia**, unlike Ukraine, **have frequently enjoyed an** **independent status**, **and Russians “have** **long recognized** that **the Baltics are** **culturally and historically different** **from Russia**.” Moreover, **Russians** **in the Baltics** **do not seem to have** **separatist** **interests** not least in part **because they have** much **higher standards of living** **than** do their **counterparts o**n **the other side of the border**. And **because the Baltic states are members of the** **European Union** **and its associated** **Schengen zon**e, **their citizens would no longer** **enjoy the** associated **ease of travel to the continent** if they became part of Russia.94 In all, then, **the** **notion** **that Putin’s Russia is on an** **expansionary mission**, so commonly voiced at the time of the 2014 events, **seems to** **have little substance**.95 It has **not even sought to** **officially annex** **separatist areas in eastern Ukraine**. A special issue of the journal Daedalus, published in 2017, ran a series of essays dealing with Russia’s future. None envisioned territorial expansion.96 Definitions of superpower status common during the Cold War generally stressed the possession of stocks of nuclear weapons. If that criterion continued to be embraced, Russia should still probably be considered a superpower. However, as Dmitri Trenin points out, **Russia “has** **few formal allies**, **no satellite states**, **and** ... **no ideology** to compare with the comprehensive dogma of Marxism-Leninism.” Moreover, “although it is still a nuclear superpower, **it lags** **far** **behind the United States in non-nuclear military** **capabilities**. **Economically, Russia** – with its estimated 1.5 percent of the global gross domestic product – **is a dwarf**.”97 Its GDP ranks twelfth in the world, but is only one-fifteenth that of the United States and about half that of California. Moreover, GDP growth in Russia has been weak with recent figures at about 1.8 percent per year, and it relies heavily on selling energy abroad: nearly 50 percent of its exports are in oil and gas. Its **population is** **shrinking** and may, according to medium-term projections, be reduced to 125 million by 2094 from the current level of about 148 million. **For an economy that is** **more people-intensive** **than other advanced economies, this** **spells trouble**. As Barack Obama pointed out derisively, if undiplomatically, in his final news conference as president, “Their **economy doesn’t produce** **anything that anybody wants** **to buy**, except oil and gas and arms. They don’t innovate.”98 The (rather **bizarre) Russia suffers from** the same problems as the “in-between” counties as discussed above while **being** **burdened** in addition **by a much larger military budget – although** **weak GDP growth** **has** also **been reflected in a** **shrinking** **military budget**, down about 5 percent in 2018 from 2017. Like China, it has **devolved into a form of** **crony capitalism** **where** **property rights** **are insecure**, **capital flight** **is common**, **corruption** **is rampant**, **and** **economic stagnation** **is likely**. As Anders Aslund concludes, the state has been captured by a small group of top officials with the topmost being Vladimir Putin, who has 20 palaces, four yachts, 58 aircraft, and a collection of watches worth $600,000. 99 **Ukraine episode** of 2014 **seems**, like the Korean invasion of 1950, **to** **be a one-off – a** **unique**, **opportunistic**, **and** probably **under-considered** **escapade that** **proved to be unexpectedly costly to the perpetrators**. As with the Korean case, **massive extrapolation is** **unjustified and ill-advised**. That is, the Ukrainian venture, contrary to much initial speculation, does not seem to be a game-changer.100 As Trenin points out, **Moscow’s** **most important objective** **is to reassert its role as a** **great power** **with a global reach**. However, **it does** **not** **seek to impose its own model on** **the world**. In all this, **neither side** **envisions a** **real shooting war** **against its adversary** **and neither wants** to allow **the situation to become** **uncontrollable**.101

#### No conventional invasion NOR escalation

Veebel 19 – Viljar, Department of Political and Strategic Studies, Baltic Defence College. “Researching Baltic security challenges after the annexation of Crimea”, Journal on Baltic Security, Vol. 5, No. 1, Pg. 41-52, <https://sciendo.com/pdf/10.2478/jobs-2019-0004>, 04-30-2019

3 Studies on potential nuclear escalation scenarios **The question whether Russia would use** its **nuclear forces in the Baltic region has** **also intrigued many** academics and military experts recently. One of the most radical discussions in this field is a blog post by Loren B. Thompson, ‘Why the Baltic states are where nuclear war is most likely to begin’. He argues that the likelihood of nuclear war between Russia and the United States is probably growing and is the reason why it is most likely going to start is a future military confrontation over three Baltic countries. Thompson describes eight reasons why nuclear weapons could potentially be used in future warfighting scenarios with regard to the Baltics and argues that according to the bottom-line scenario, the East–West conflict escalates into the use of nuclear weapons in the Baltic area, and neither side of the conflict understands what actions might provoke nuclear use by the other. Thompson comes to a somewhat surprising conclusion – at least in the eyes of the Baltic countries – that the United States needs to reassess the situation, suggesting that it would make no sense to tie security of the United States to countries of ‘such modest importance that are situated in such unpromising tactical circumstances’ (Thompson, 2016). Potential nuclear conflict escalation scenarios are in more detail discussed in another publication, a NATO playbook entitled ‘Preventing escalation in the Baltics’ by Ulrich Kühn. The author argues that the risk of escalating a wider conflict between Russia and NATO is dangerously high particularly in the case of the Baltic countries because it would be difficult for NATO to defend the region. Kühn suggest three possible escalation scenarios, i.e., deliberate escalation, inadvertent escalation, and accidental escalation. All three scenarios also involve nuclear threats; however, two of the scenarios stop short of actual Russian nuclear-weapon usage (Kühn, 2018). The analysis provides an interesting hypothetical construct for the experts at both the transatlantic and local levels, as it points to many practical issues in regard to the nuclear deterrence from the NATO’s political decision-making process to the role of domestic policies in tackling such a crisis. Conflict escalation scenarios that involve nuclear capabilities are discussed also in other studies. For example, in a study called ‘Reducing the risk of nuclear war in the Nordic/Baltic region’ by Barry Blechman and co-authors, two scenarios of conventional war ending in the exchange of nuclear weapons are constructed (namely, ‘Escalation in Estonia’ and ‘Regional War’). Although the authors emphasize that the scenarios are purely illustrative and **the probability of nuclear use is** **low**, they argue that it is useful to reduce these risks even further and suggest two initiatives, such as a strengthening of the Alliance’s conventional military capabilities and particularly the ability to move quickly into the Baltic region, as well as to establish a Baltic nuclear weapons free zone, or at least examining the possibility to do so (for further discussion, see Blechman et at., 2015). Jüri Luik and Tomas Jermalavičius in their article ‘A plausible scenario of nuclear war in Europe, and how to deter it: A perspective from Estonia’ point to various alarming signs, e.g., Russia’s large-scale exercises incorporate limited nuclear strike scenarios against NATO as part of Russia’s ‘escalation to de-escalate’ strategy; Russia is expanding the range of its tactical delivery systems, the country’s political rhetoric includes nuclear threats toward the West, and so on. They emphasize that the Alliance’s range of response options to such threats and limited nuclear war scenarios has shrunk considerably and that the Alliance lacks a collective will to call those threats a bluff (Luik and Jermalavičius, 2017). A large part of the research in this field more or less considers it likely that Russia could use its nuclear forces in the Baltic region. However, there are also articles that oppose this conviction. For example, Viljar Veebel and Illimar Ploom in ‘The deterrence credibility of NATO and the readiness of the Baltic states to employ the deterrence instruments’ disagree with the idea that the Baltic countries could be under potential nuclear attack, which could in turn evolve to a nuclear war. They argue that **although Russia and NATO as potential conflict parties have a striking capability, it would be** **irrational for both of them** **to execute a nuclear strike** **even as a measure of last resort**. The authors stress that **it is** **hard to believe** **that Russia** **has** **any rational motivation**

#### Russia war never escalates—empirics

**Zeeberg 18** – Amos, freelance science journalist based in Tokyo, “Why Hasn’t the World Been Destroyed in a Nuclear War Yet?”, Nautilus (not the league champ), http://nautil.us/blog/-why-hasnt-the-world-been-destroyed-in-a-nuclear-war-yet, 01-15-2018

But **after all these nuclear near-misses, one starts to wonder if it really is plain dumb luck. The Nash equilibrium accurately describes a certain kind of rational, perfectly logical approach to choices under conflict.** And exactly in keeping with game theorists’ advice, **the USSR and U.S. went to great lengths to make sure their arsenals would be feared** as legitimate threats. **Yet each time they had an opportunity to make good on those threats—to launch a crushing response to an apparent attack or mercilessly exploit a weakness**, as many armchair analysts recommended—**something held them back: a disobedient soldier, a circumspect engineer, an optimistic leader. The two nations** were engaged in a battle of wills, staring each other in the eyes, and they **both blinked. Repeatedly. Maybe, when millions of lives hang in the balance, people are not so rationally cold-hearted as those old game-theory models imply. Or maybe they’re using a different kind of rationality.**

### 1NC---Cyber Impact

#### No catastrophic cyberattacks – 25 years of empirics prove they stay low-level and non-escalatory

Lewis 20 – James Andrew, senior vice president and director of the Technology Policy Program at the Center for Strategic and International Studies. “Dismissing Cyber Catastrophe”, Center for Strategic & International Studies, <https://www.csis.org/analysis/dismissing-cyber-catastrophe>, 08-17-2020

A **catastrophic cyberattack was** first **predicted in the mid-1990s. Since then, predictions** of a catastrophe **have appeared regularly** and have entered the popular consciousness**.** As a trope, a cyber catastrophe captures our imagination, but as analysis, **it remains entirely imaginary and is of dubious value as a basis for policymaking.** There has never been a catastrophic cyberattack. To qualify as **a catastrophe**, an event **must produce damaging mass effect, including casualties and destruction.** The **fires that swept across California** last summer **were a catastrophe. Covid**-19 **has been a catastrophe**, especially in countries with inadequate responses**.** With man-made actions, however, a catastrophe is harder to produce than it may seem, and **for cyberattacks a catastrophe requires organizational and technical skills** most **actors still do not possess.** It requires planning, reconnaissance to find vulnerabilities, and then acquiring or building attack tools—things that require resources and experience. To achieve mass effect, either a few central targets (like an electrical grid) need to be hit or multiple targets would have to be hit simultaneously (as is the case with urban water systems), something that is itself an operational challenge. It is easier to imagine a catastrophe than to produce it. The 2003 East Coast blackout is the archetype for an attack on the U.S. electrical grid. No one died in this blackout, and services were restored in a few days. As electric production is digitized, vulnerability increases, but many **electrical companies have made cybersecurity a priority.** Similarly, at water treatment plants, the chemicals used to purify water are controlled in ways that make mass releases difficult. In any case, it would take a massive amount of chemicals to poison large rivers or lakes, more than most companies keep on hand, and any release would quickly be diluted. More importantly, **there are powerful strategic constraints on those who have the ability to launch catastrophe attacks. We have** more than **two decades of experience** with the use of cyber techniques and operations for coercive and criminal purposes and have a clear understanding of motives, capabilities, and intentions**. We can be guided by the** methods of the **Strategic Bombing Survey**, which used **interviews** and observation (**rather than hypotheses**) to determine effect**.** These methods apply equally to cyberattacks. The conclusions we can draw from this are: Nonstate actors and most states lack the capability to launch attacks that cause physical damage at any level, much less a catastrophe. There have been regular predictions every year for over a decade that nonstate actors will acquire these high-end cyber capabilities in two or three years in what has become a cycle of repetition. The monetary return is negligible, which dissuades the skilled cybercriminals (mostly Russian speaking) who might have the necessary skills. One mystery is why these groups have not been used as mercenaries, and this may reflect either a degree of control by the Russian state (if it has forbidden mercenary acts) or a degree of caution by criminals. **There is** enough **uncertainty** **among potential attackers about the United States’ ability to attribute** **that they are unwilling to risk massive retaliation** **in response to a catastrophic attack. (They are perfectly willing to take the risk of attribution for** **espionage** **and** **coercive cyber actions.)** No one has ever died from a cyberattack, and only a handful of these attacks have produced physical damage. **A cyberattack is not a nuclear weapon, and** **it is intellectually lazy to equate them to nuclear weapons.** Using a tactical nuclear weapon against an urban center would produce several hundred thousand casualties, while a strategic nuclear exchange would cause tens of millions of casualties and immense physical destruction. These are catastrophes that some hack cannot duplicate. The shadow of nuclear war distorts discussion of cyber warfare. **State use of cyber operations is consistent with their broad national strategies and interests.** **Their primary emphasis is** on **espionage and political coercion.** The **United States** has **opponents** and is in conflict with them, but they **have no interest in launching a catastrophic cyberattack** **since it would certainly produce an equally catastrophic retaliation.** Their goal is to stay below the “use-of-force” threshold and undertake damaging cyber actions against the United States, not start a war. This has implications for the discussion of **inadvertent escalation**, something that **has** also **never occurred.** The concern over escalation deserves a longer discussion, as there are both technological and strategic constraints that shape and limit risk in cyber operations, and the **absence of inadvertent escalation suggests a high degree of control for cyber capabilities by advanced states.** **Attackers**, particularly **among the United States’ major opponents** for whom cyber is just one of the tools for confrontation, **seek to avoid actions that could trigger escalation.** The United States has two opponents (China and Russia) who are capable of damaging cyberattacks. **Russia has demonstrated its attack skills on the Ukrainian power grid, but** neither **Russia** nor China **would be well served by a similar attack on the United States.** Iran is improving and may reach the point where it could use cyberattacks to cause major damage, but it would only do so when it has decided to engage in a major armed conflict with the United States. Iran might attack targets outside the United States and its allies with less risk and continues to experiment with cyberattacks against Israeli critical infrastructure. North Korea has not yet developed this kind of capability. One major failing of **catastrophe scenarios** is that they **discount** the **robustness** and resilience **of modern economies.** These economies present multiple targets and configurations; **they are harder to damage through cyberattack than they look, given the growing** (albeit incomplete) **attention to cybersecurity; and experience shows that people compensate for damage and quickly repair or rebuild.** This was one of the counterintuitive lessons of the Strategic Bombing Survey. Pre-war planning assumed that civilian morale and production would crumple under aerial bombardment. In fact, the opposite occurred. Resistance hardened and production was restored.1 This is a short overview of why catastrophe is unlikely. Several longer CSIS reports go into the reasons in some detail. Past performance may not necessarily predict the future, but **after 25 years without a single catastrophic cyberattack**, we should invoke the concept cautiously, if at all. **Why then, it is raised so often?** Some of the explanation for the emphasis on cyber catastrophe is hortatory. When the author of one of **the first reports** (**in the 1990s**) to sound the alarm over cyber catastrophe was asked later why he had warned of a cyber Pearl Harbor when it was clear this was not going to happen, his reply was that he **hoped to scare people into action.** "Catastrophe is nigh; we must act" was possibly a reasonable strategy 22 years ago, but no longer. The resilience of historical events to remain culturally significant must be taken into account for an objective assessment of cyber warfare, and this will require the United States to discard some hypothetical scenarios. **The long experience of living under the shadow of nuclear annihilation still shapes American thinking and conditions the United States to expect extreme outcomes. American thinking is also shaped by the experience of 9/11**, **a wrenching attack that caught the United States by surprise.** Fears of another 9/11 reinforce the memory of nuclear war in driving the catastrophe trope, but when applied to cyberattack, these scenarios do not track with operational requirements or the nature of opponent strategy and planning. The contours of cyber warfare are emerging, but they are not always what we discuss. Better policy will require greater objectivity.

#### Russia demonstrating restraint---no cyberattack

Marie Baezner and Patrice Robin, June 2017, (Center for Security Studies ETH Zurich), “Cyber-conflict between the United States of America and Russia”, CSS Cyber Defence Hotspot Analysis, ETH Zurich, Page 13, https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/184547/Cyber-Reports-2017-02.pdf?sequence=1/ceng

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.

#### Lack of visceral damage removes public pressure to kinetic war

Borghard and Lonergan 19 – Erica, Assistant Professor at the Army Cyber Institute at the United States Military Academy at West Point and a research fellow at the Saltzman Institute of War and Peace Studies at Columbia University, PhD in political science from Columbia University. Shawn, Research affiliate of the Army Cyber Institute at the United States Military Academy at West Point and a cyber officer in the US Army Reserve currently assigned to 75th Innovation Command, PhD in political science from Columbia University. “Cyber Operations as Imperfect Tools of Escalation”, Strategic Studies Quarterly, Vol. 13, No. 3, pg. 122-145, <https://www.jstor.org/stable/26760131?seq=1#metadata_info_tab_contents>, xx-xx-2019

Willingness to Engage in Cross-Domain Escalation

Just as the limited ability of offensive cyber operations to generate meaningful and sustained costs against a target reduces their appeal as tools of escalation, it also diminishes the likelihood of cross-domain escalatory responses to a cyber incident. Cyber operations can cause significant economic and, in some instances, second-order effects on human life (such as cyberattacks against a power grid). However, they have not yet produced the physical violence and horrors of kinetic warfare or even terrorism that would engender a visceral public reaction to prod decision-makers into escalatory responses—particularly responses that would cross a key threshold from cyber to kinetic force. In other words, both the tangible and psychological costs of cyber operations may check domestic political willingness (or pressure) to escalate via cross-domain instruments in response to adversary cyber operations.

#### No cyber war or retaliation

Rodet 18 – Jasmine, Master’s Degree in Cyber Security, Strategy, and Diplomacy from the University of New South Wales, Cyber Security Program Manager at Fortescue Metals Group. “The Threat of Cyber War is Exaggerated”, linkedin.com/pulse/threat-cyber-war-exaggerated-jasmine-rodet/, 11-11-2018

For the regular person on the street, the term ‘cyber war’ is more likely to bring to mind the 1983 movie “WarGames” and the **doomsday articles** that **appear regularly in the media about the ‘cyber battlefield’ and** an **impending World War III**. This essay argues that **the threat of cyber war is exaggerated** **and** although it can, by definition, be stated that we are already in a state of cyber war, the impact on states is **negligible** compared to conventional war domains. The argument is presented in 3 steps. The first step is to define cyber war and cyber weapons, referencing scholars and experts in the area of conventional war and the cyber domain. The second step is to explore who has been exaggerating the threat of cyber war and what their motivations might be. The third is to explore the evidence and quantify the probability and impact that cyberwar has had on states to date. ‘Cyber war’ is a term often used interchangeably in media with cyber-crime, cyber-attacks, cyber-conflict and cyber-incidents, creating confusion amongst the public and scholars alike. Clausewitz (1989, 75), in his book, On War, defines war as ‘an act of force to compel the enemy to do our will’. Rid (2012, 7) on the other interprets Clausewitz use of ‘force’ as meaning ‘violent’ force. According to Rid, if an act is not potentially violent, it is not an act of war. However, Stone (2013, 107) describes ‘cyber war’ as a politically motivated act of force, not necessarily lethal and not necessarily attributable. The definition by Powers and Jablonski states more simply that cyber war is the utilisation of digital networks for geopolitical purposes (Nocetti 2016, 464). Neither of the latter two definitions requires violence to qualify as cyber war. Under these definitions, the Stuxnet cyber-incident in 2010 and the Estonia incident in 2007 would constitute an act of cyber war, and as such we could say that nations have been at cyber war in the past and are likely to continue to engage in cyber war in years to come. For this essay, I will use Stones definition to argue that even though states may engage in cyber war, the concept of cyber war is exaggerated. It seems that **cyber war is deliberately exaggerated in the media and by politicians for financial and political gains**. There are countless examples in the media and in politics of the exaggeration of the threat of cyber war and the language used plays a big factor in creating a sense of fear in the community. The Four Corners report, Hacked, is a classic example where the reporter, Andrew Fowler describes the current situation in Australia as ‘… a secret war where the body count is climbing every day’ (Fowler 2013). The documentary reveals nothing violent or lethal about cyber incidents. The documentary is actually about hackers working from locations overseas, having targeted key Federal Government departments and major corporations in Australia. In another example, NATO may be interpreted as exaggerating the threat of Cyber War when they invited Charlie Millar to present at their Conference for Cyber Conflict at the NATO Cooperative Cyber Defence Centre of Excellence in 2017. Millar is an independent security evaluator, and his presentation was titled ‘Kim Jong-il and me: How to build a cyber army to attack the US’. He later presented similar content at Def Con 2018. His presentation described the steps he would take to mount a cyber war, including the types of people he would engage, how much he would pay them, what his strategy would be and how much it would cost in total. Who stands to gain from the exaggeration and hype? Logically, **one group would be those that gain financially from the sale of cyber protective services and software**. According to Valerino, 57% of technical experts surveyed said that we are currently in a cyber arms race and 43% said that the worst-case scenarios are inevitable (Valeriano and Ryan 2015). Translate this into sales and Gartner projects worldwide security spending will reach $96 Billion in 2018, up 8 Percent from 2017 and to top $113 billion by 2020 (Gartner 2017). Additionally, **there may be political motivations to exaggerate the threat of cyber war**. Cyberspace is not well understood by the general public and fear is natural. In the US’s cyber security debate, observers have noted there is a tendency for policymakers, **military leaders, and media**, among others, **to use frightening ‘cyber-doom scenarios’ when making a case for action on cyber security** (Dunn 2008, 2). There is some evidence to suggest that more recently in the political arena; we may be maturing in our understanding of the real threat of cyber war. The Tallinn Manual, an academic, non-binding study on how international law applies to cyber conflicts and cyber warfare, was written at the invitation of the Tallinn-based NATO Cooperative Cyber Defence Centre of Excellence. It was first published in 2013 with the title ‘The Tallinn Manual on the International Law of Cyber War’. In 2017, it was re-released with the revised title ‘Tallinn Manual 2.0 on the International Law of Cyber Operations’. The change in title from ‘war’ to ‘operations’ signifies a more moderate use of language from NATO and is an acknowledgement that cyber incidents generally fall below the threshold at which International Law would declare them to be a formal act of war. Experience over the 4 short years from 2013 to 2017 has demonstrated that cyber incidents tend to have a low-level impact on the target state. As the book’s authors put it ‘the focus of the original Manual was on the most severe cyber operations, those that violate the prohibition of the use of force in international relations, entitle states to exercise the right of self-defence, and/or occur during armed conflict’ while the new version ‘adds a legal analysis of the more common cyber incidents that states encounter on a day-to-day basis and that fall below the thresholds of the use of force or armed conflict’ (Leetaru 2017). To get a better sense if cyber war is exaggerated, we must also consider the probability of cyber war in the future. The probability of cyber war should be weighed up against the probability of conventional war. Where tensions are already high, for example, between North Korea and the US or Russia and Estonia, I would argue that cyber war is more likely than conventional war. This is due to factors including; cyber warfare is less costly than conventional warfare, states are less rational in their decision space in the cyber realm, states find cyber attribution very difficult to achieve so attacks can be undertaken covertly and cyber war is considered ‘a challenge’ and central to the hackers’ ethos (Junio 2013, 128). Further, Sanger describes in his book, The Perfect Weapon, cyber weapons (such as cyber vandalism, Distributed Denial of Service (DDOS), intrusions and advanced persistent threat (APT)) as the ‘perfect weapons’ for the following reasons; They are cheap: When compared to Nuclear weapons, there are only a handful of nations globally that can afford the technology to create a nuclear weapon. They are easily accessible: Unlike a Nuclear bomb that requires uranium, a highly protected metal, in the production process, a cyber weapon can be created with minimal investment and highly available IT infrastructure. They can be dialled-up or dialled-down relatively easily. A ballistic missile, the force of the explosion cannot be adjusted as easily as a DDOS attack. A DDOS attack can be adjusted to last an hour, a few days or a few weeks. They have a huge range in how they are used: Sabotage as with Stuxnet, Espionage as with the Chinese industrial spying on the US, North Korea’s infiltration of Sony, the Iranians attack on Las Vegas Sands Corp. casino operators. The significant factor is that cyber weapons can and are being used every day for discrete, **low-level cyber conflicts** to undermine and disrupt rivals, but historically it **has not progressed to open conflict, nor has it warranted a military response** (Sanger 2018). **Additionally, massive cyber operations would necessarily impact the civilian population and violate the immunity of non-combatants. The conditions of war dictate that this is “taboo” and to date, rival states have shown restraint in their use of cyber weapons for this reason** (Valeriano and Ryan 2015). **It appears that the threat that cyber weapons represent to national security is overstated and the threat of cyber war is overstated**. **The US and** likely **other highly networked nations appear reticent** about using cyber weapons for significant cyber conflict **given their vulnerabilities**. Ironically, NSA programs such as PRISM have made the US more of a target given the sheer volume of sensitive information stored in one place. Regardless of US defences, there is no way to make this information completely secure from intrusion, and as such, the very act of storing the information makes them more vulnerable. Rid (2012) is among some academics who argue that **cyber war** has never and **will likely never eventuate**. The benefits of being on this side of the debate mean that public funding can be allocated away from offensive cyber security initiatives to other, potentially more important initiatives, such as public health and housing. The government is constantly under pressure to prioritise public spending and it is imperative that they have realistic, accurate projections regarding the risk of cyber war, the probability and the impact, to allow them to focus spending on the most important areas.

#### No nuclear retal

Tucker 18 – Patrick, Technology Editor for Defense One, MA from Johns Hopkins University, BA from Sarah Lawrence College, Former Deputy Editor for The Futurist. “No, the US Won’t Respond to A Cyber Attack with Nukes”, Defense One, <https://www.defenseone.com/technology/2018/02/no-us-wont-respond-cyber-attack-nukes/145700/>, 02-02-2018

**No, the US Won’t Respond to A Cyber Attack with Nukes** Defense leaders won’t completely rule out the possibility. **But it’s a very, very, very remote possibility**. **The idea that the U.S. is building** new **low-yield nuclear weapons to respond to a cyber attack is “not true,”** military leaders told reporters in the runup to the Friday release of the new Nuclear Posture Review. “The people who say we lowered the threshold for the use of nuclear weapons are saying, ‘but we want these low-yield nuclear weapons so that we can answer a cyber attack because we’re so bad at cyber security.’ That’s just fundamentally not true,” Gen. Paul Selva, vice chairman of the Joints Chiefs of Staff, said Tuesday at a meeting with reporters. **It’s an idea** that **military leaders have been pushing back against since the New York Times ran a** Jan. 16 **story headlined, “Pentagon Suggests Countering Devastating Cyberattacks With Nuclear Arms.”** When would the U.S. launch a nuclear attack in response to a non-nuclear event? The Defense Department says **the threshold hasn’t changed since** the **Obama** administration’s own nuclear posture review in 2010, but a draft of the new review that leaked online caused a bit of drama in its attempts to dispel “ambiguity.” The new review gives examples of “non-nuclear strategic attacks,” Robert Soofer, deputy assistant secretary for nuclear and missile defense policy, told reporters on Thursday. “It could be catastrophic attacks against civilian populations, against infrastructure. It could be an attack using a non-nuclear weapon against our nuclear command-and-control [or] early-warning satellites. But **we don’t talk about cyber**.” In his own conversation with reporters, Selva broadened “early warning” systems to include ones that provide “indications of warning that are important to our detection of an attack.” He also emphasized, “We never said ‘cyber.’” **There’s a reason for that**. While **cyber attacks** on physical infrastructure can be very dangerous, they **are unlikely to kill enough people to provoke a U.S. nuclear response**. An National Academies of Science and Engineering analysis of the vulnerability of U.S. infrastructure makes that point. **A** major **cyber attack could cut off electrical power**, resulting in “people dying from heat or cold exposure, etc.,” said Granger Morgan, co-director of the Carnegie Mellon Electricity Industry Center and one of the chairs of the report. “A large outage of long duration could cover many states and last for weeks or longer. Whether and how many casualties there could be would depend on things like what the weather was during the outage.” **It’s** a huge problem but **not an event resulting in tens of thousands of immediate deaths**. Contrast that with a nuclear attack on a city like Moscow, even one using a device of 6 kilotons, much smaller than the ones the United States used against Japanese targets in World War II. The immediate result: there would be 40,000 deaths, according to the online nuclear simulation tool NukeMap. **Russia** has **demonstrated** a **willingness** to take down power services with cyber attacks, as they did in Ukraine on Christmas Eve 2015. **But** these **attacks were brief and occured in the context of actual fighting**. In other words, **the worst** cyber physical **attack** that **top experts believe credible likely does not meet the threshold that the Defense Department has set out for deploying a nuclear weapon**.

#### Cyberwar falls short of kinetic attacks---stabilizing

Erica D. Lonergan, 04-15-2022, (Erica D. Lonergan is Assistant Professor in the Army Cyber Institute at West Point and a Research Scholar at the Saltzman Institute of War and Peace Studies at Columbia University. Previously, she served as Senior Director on the U.S. Cyberspace Solarium Commission.), “The Cyber-Escalation Fallacy”, Foreign Affairs, https://www.foreignaffairs.com/articles/russian-federation/2022-04-15/cyber-escalation-fallacy/ceng

A third lesson of cyber-operations over the past decade is that U.S. officials should adopt a more flexible mindset in their response to them. Rather than focusing on retaliatory action, the United States should devote more resources to enhancing resilience—the ability to absorb and rapidly recover from disruptive occurrences. Embracing this type of approach means accepting that cyberattacks are likely to take place and, more important, that the overwhelming majority of them will not have cataclysmic effects. Over the past several years, the United States has improved its resilience to such attacks, expanding the agencies responsible for working with and maintaining critical infrastructure, such as the Cybersecurity and Infrastructure Security Agency. The U.S. government has also created the Office of the National Cyber Director to harmonize its cybersecurity efforts and collaborate with the private sector. But these entities are still relatively new, and efforts to implement meaningful regulation of the private sector to promote resilience still have a long way to go. A CYBER ESCAPE VALVE? Just because cyber-operations have not yet caused escalation does not mean that they will never do so. If conflicts such as the war in Ukraine lead to greater instability in the international system and increased great-power competition, the risks of cyber-escalation may grow. The opposite is also possible, however: in a more unstable world, cyber-operations may provide an important outlet for recurring tensions, given their lack of physical violence and relatively limited effects. As international politics become more dangerous, cyberspace can offer a way for states to respond to perceived aggressions without causing physical destruction or loss of life, thus providing a kind of stability in itself. Ultimately, escalation is in the eye of the beholder—it depends as much on the target’s perception of an event as on the perpetrator’s intent or the reality of the strategic context. Therefore, a further priority of U.S. policymakers should be to improve their understanding of how adversaries interpret Washington’s activities in cyberspace and leverage that knowledge to conduct cyber-operations that minimize the risk of escalation. During a crisis, for instance, the United States may want to avoid conducting cyber-operations in a manner that an adversary might perceive as a precursor to conflict or to a military strike, especially if that is not the intent. If there is a pressing strategic or military imperative to conduct these types of operations, they should occur in tandem with efforts to communicate their purpose to avoid misunderstandings. For too long, policymakers have drawn the wrong lessons from cyber-operations. The absence of escalation across decades of strategic interaction in cyberspace—a record that has only been reinforced in the conflict in Ukraine—should cause policymakers to reevaluate long-standing assumptions about the cyber-domain. In doing so, they may be able to see how cyber-actions are but one of a number of strategic tools that, properly understood, can limit the risk of conflict as much as increase it. Of course, the potential for cyberattacks to temporarily paralyze large information networks or even whole sectors of an economy should not be discounted. But in a world in which armed conflict continues to destroy entire cities and wreak terrible human costs, both civilian and military, cyber-operations should be regarded less as another form of hard power than as a way for states to pursue strategic goals by other means.

#### Ukraine proves

John Mueller, 03-22-2022, (John Mueller is a Political Scientist at Ohio State University and a Senior Fellow at the Cato Institute. His most recent book is The Stupidity of War: American Foreign Policy and the Case for Complacency.), “The Cyber-Delusion”, Foreign Affairs, https://www.foreignaffairs.com/articles/russia-fsu/2022-03-22/cyber-delusion/ceng

When Russian forces launched their invasion of Ukraine last month, governments and experts worldwide warned about the danger of catastrophic cyberattacks. Indeed, in the days leading up to Moscow’s invasion, hackers defaced Ukrainian websites, unleashed malware on government systems, and targeted the country’s banking system—albeit with limited effect. Although no cyber-Armageddon has materialized, officials increasingly fear that Russia might eventually step up its efforts and even target the United States. Russia’s invasion is no doubt catastrophic. But in reacting to it and preparing for what comes next, leaders in Washington and elsewhere should eschew the alarmism that has long warped cybersecurity policy. Mike Mullen, then chairman of the Joint Chiefs of Staff, claimed in 2011 that “the single biggest existential threat out there, I think, is cyber.” The following year, his successor, Martin Dempsey, noted that “a cyberattack could stop our society in its tracks.” Former Defense Secretary Leon Panetta sternly warned in 2012 of an impending “digital Pearl Harbor.” Nicole Perlroth, a cybersecurity reporter at The New York Times, has routinely asked insiders when “a cyber-enabled cataclysmic boom will take us down” and has always been told “18 to 24 months.” She began her survey well over 100 months ago. This contemporary approach to cyberthreats resembles the aftermath of 9/11, when almost all experts believed an even larger terrorist attack would soon take place. Then, as now, the threat is overblown. Although occasionally dramatic, cyberattacks have turned out to be a comparatively minor and manageable threat. Far too much discussion around the issue focuses on worst-case scenarios, fails to contextualize the problem, and neglects to weigh the costs of cyberattacks against the enormous value of the Internet and artificial intelligence. Most commentary, moreover, does not fully appreciate the ability of the business sector—by far the most tempting of targets for malevolent hackers—to develop effective countermeasures. Over the past decade, the global obsession with digital threats has taken various forms, with a particular focus on the potential military implications of emerging cyber-capabilities. To be sure, the military needs to worry about keeping its communications and command and control operations secure from hostile attackers. Any disruptions, however, are more likely to be instrumental or tactical than strategic. Despite statements to the contrary, the U.S. military itself seems to have recognized this reality. When Panetta proclaimed in 2013 that cyber was “without question, the battlefield for the future,” political scientist Micah Zenko observed at the time that the Pentagon was spending less than one percent of its budget on cybersecurity, and an assessment from 2019 suggests it may be more like one-tenth of one percent. If those funds prove adequate for the challenge, it would be something of a bargain. Cyber also supposedly enhances a state’s ability to carry out such ancient endeavors as espionage, propaganda dissemination, and sabotage. Analysts have even coined a new term, “hybrid warfare,” that usually includes these three enterprises—although, since the term does not include direct armed conflict, it might more plausibly be called “denatured warfare.” Cyber’s contribution to these three areas, however, is relatively limited. Should invading hackers engage in digital espionage against the United States, for instance, they are likely to find that most of what they come across is already well known, and that much of the rest is not worth knowing in the first place. Wikileaks’ 2010 publication of thousands of classified U.S. government documents demonstrated the degree to which governments worldwide have fallen victim to over-classification. When Bill Keller, the editor in charge of poring over the documents at The New York Times, was asked whether the reporting team found anything they didn’t already know, he responded “no” without hesitation. Much the same holds for concerns over the theft of intellectual property. Not only is this practice centuries old, but systematic stealing has often proved unwise because it distracts governments from homegrown innovation. Cyber-propaganda efforts, in turn, are more likely to increase the overall amount of available information and disinformation—an age-old problem in warfare—than to provide a decisive advantage. The achievements of cyber-sabotage have also been quite modest. The United States and Israel famously used a computer virus known as Stuxnet to hamper Iran’s progress toward developing a nuclear weapon. Although observers hailed the operation as a dangerous new development in modern conflict, the damage proved temporary. Iran quickly rebuilt its centrifuges, and the attack actually proved counterproductive, as it encouraged Tehran to accelerate its nuclear program. There have also been efforts by the United States to physically interfere with missile development in North Korea. Yet, much like the Iranians, Pyongyang eventually solved whatever the problem was, and the attacks had little long-term effect on their program. Cyber-alarmists have also warned about hackers disabling major infrastructure such as power grids—potentially crippling entire countries. Grids do go down occasionally, but the culprits are typically squirrels and lightning. Regardless of the source, such disruptions are usually brief and bearable, and engineers are increasingly designing systems that are resilient to such threats. Estonia, for instance, the victim of a major and oft-discussed cyberattack in 2007, is now the home of NATO’s Cooperative Cyber Defence Centre of Excellence.

#### Status quo solves NATO cyber ambiguity

Khatuna Burkadze, 2018, (Khatuna Burkadze is a graduate of the Fletcher School of Law and Diplomacy, Tufts University. Professor Burkadze has been a Fulbright scholar at the MIT Center for International Studies as well as a visiting professor at Columbia University, Bard College and the Fletcher School of Law and Diplomacy. She has successfully completed programs on negotiations and security studies at Harvard University and George C. Marshall European Centre for Security Studies. Dr. Khatuna Burkadze has also implemented projects sponsored by NATO and the European Union which sought to increase awareness of both organizations inside Georgia. Dr. Khatuna Burkadze is an alumnus of the U.S. Department of State’s Program on American Foreign Policy as well as the author of dozens of articles and book chapters.), “A Shift in NATO's Article 5 in the Cyber Era?”, 42 Fletcher F. World Aff. 215 (2018), https://heinonline.org/HOL/LandingPage?handle=hein.journals/forwa42&div=32&id=&page=/ceng

NATO'S CYBER DEFENSE AND INTERNATIONAL LAW The U.N. Charter and the North Atlantic Treaty (the founding treaty of NATO) were adopted in 1945 and 1949 when the creation of cyberspace was a matter of the future rather than a consideration of the times. Currently, it is clear that information and communication technologies have transformed the nature of war and changed historical understanding of armed attacks. Traditional applications of the use of force prohibition fail to adequately safeguard shared community values threatened by Computer NetworkAttacks (CNA)." The use of force is strictly limited in international law according to the U.N. Charter. Consequently, the central questions are the following: Could a cyberattack be equated to an armed attack according to international law? If a cyberattack equates to an armed attack, how should the principle of collective defense of NATO be interpreted to give member states legal guidance on the concept of a cyberattack? Do we need amendments in Article 5 of the North Atlantic Treaty to clearly define what constitutes a cyberattack? Answers to these questions can provide insights for defining rules of cyber operations in case of cyberattacks. The definitions of the use of force and armed attack are not provided in the U.N. Charter. In this regard, in its argument on a case concerning Nicaragua, the International Court of Justice rejected a narrow interpretation of "use of force" that limits the term to the employment of either kinetic force or non-kinetic operations generating comparable effects. The Court held that a state's arming and training of guerrilla forces engaged in hostilities against another state qualified as a use of force, a position that has since become widely accepted.'" The logic of the holding leads to the conclusion that non-destructive cyber operations may amount to a use of force. For example, providing malware to a rebel group and training its members to employ that malware in a destructive manner would seemingly qualify.20 However, every unfriendly act does not cross the use of force threshold. The International Court of Justice held that financing guerrillas, albeit an unlawful "intervention," did not fall into the same category. Therefore, cyber operations intended to economically coerce another state to engage in, or desist from, a particular course of action would not amount to a use of force; nor would financing a rebel group's cyber operations. Beyond these directly parallel examples, uncertainty remains as to where the threshold lies.2 1 The NATO Cooperative Cyber Defense Center of Excellence launched a major research project in late 2009 to examine the public international law governing cyber warfare2 2 and cyber operations, resulting in the Tallinn Manual 1.0 and Tallinn Manual 2.0. These two documents provide international experts' analysis on how existing international law applies to cyber warfare and cyber operations. Through Tallinn Manual 1.0, the International Group of Experts developed a nonexclusive list of factors that would likely influence the characterization of cyber operations by a state as a use of force: severity, immediacy, directness, invasiveness, measurability, military character, state involvement, and presumptive legality. Additional factors found meaningful by the Experts included, inter alia, the prevailing political environment, the nexus of an operation to prospective military force, the attacker's identity, the attacker's track record with respect to cyber operations, and the nature of the target. These and other factors operate in concert as states make case-by-case determinations. Of them, severity alone can qualify a cyber operation as a use of force.23 In this regard, the Group unanimously agreed that any cyber operation causing greater than de minimis damage or injury suffices. For instance, they concurred that the damage to Iranian nuclear facilities in 2010 resulting from the Stuxnet virus crossed the threshold.24 As for the concept of cyberattacks and cyberwarfare, there are no widely accepted definitions. The U.S. Department of Defense defines "computer network attacks" as "actions taken by using computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."2 5 Yale Law Professor Oona Hathaway and her colleagues have devised a broader definition of a "cyberattack." In a 2012 article, they wrote: "A cyberattack consists of any action taken to undermine the functions of a computer network for a political or national security purpose." The article goes on to say that "any action" includes "hacking, bombing, cutting, inflecting, and so forth," as long as the action has the objective of undermining or disrupting a computer network. The word "purpose" seems to apply to the intent of the attacking party.26 According to the Tallinn Manual's Rule 30. "A cyberattack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."27 In this regard, Professor Antonia Chayes, in an article titled, "Rethinking Warfare: The Ambiguity of Cyber Attacks," highlights that a cyber operation can constitute an attack even before the damaging consequences of such an operation become evident, citing the example of implanting malware that will be activated at a later time, but for which the intended consequences meet the requisite threshold of harm as an event that could be defined as an attack "irrespective of whether the malware is activated" this is a direct parallel to implanting. In a similar vein, a cyberattack that has been launched but defeated still amounts to an attack. The Manual does warn that great care should be exercised when identifying the perpetrator of the attack.28 Professor Chayes emphasizes that these definitional iterations help to refine the issues, although they cannot be expected to answer all questions. They do serve to narrow differences in approach somewhat and to begin to assure that officials are addressing common issues. However, the lack of internationally accepted distinctions among "cybercrime," "cyberattack," and "cyber war" make concerted international action more difficult to achieve. The definitions alone do not delineate civilian and military roles, nor do they designate a legal framework under which to operate, since the issue of whether an attack warrants a military response-even in the military domain-remains ambiguous. Economic attacks may be handled through a variety of international means, judicial and diplomatic. But crippling economic attacks without serious casualties might not be sufficient to warrant acts in selfdefense under Article 51 of the U.N. Charter nor, as in the case of Estonia, a collective response under Article 5 of the North Atlantic Treaty. As for NATO's official position on interconnection between the existing international legal regulations and cyberspace, the Wales Summit Declaration (issued by the Allies in Wales on 4-5 September 2014) emphasizes: "Our policy recognizes that international law, including international humanitarian law and the U.N. Charter, applies in cyberspace. Cyberattacks 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 cyberattack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis."30 This means that, on the one hand, member states of the Alliance agreed that international law applies to cyberspace but, on the other hand, in the case of a cyberattack, a decision about invoking Article 5 will be made by the members of NATO based on the particular criteria. Therefore, the principle of collective defense is not an automatic mechanism. The exact criteria by which cyber incidents may trigger an Article 5 invocation of collective defense have not been determined. However, the North Atlantic Council is very likely to consider the following elements in its deliberations. " Scope: Is the incident widespread across a geographic area or industrial sectors? The wider the attack is, the more likely NATO action will be; " Duration: Is the incident a single event or does it last over time as part of a longer campaign? NATO is more likely to act for extended incidents; " Intensity/Scale: Has the incident caused death or substantial property destruction? If not, NATO is unlikely to declare collective defense; " External Actor: Is the incident directed from a foreign or domestic adversary? NATO is unlikely to act against a purely domestic foe.31

### 2NC---Cyber Impact

#### No Cyber Impact – Attacks won’t escalate – attribution and retaliation deter it, actors don’t have the skills to take down anything that matters – companies are bolstering security now, their evidence is based in 9/11 fear-mongering – prefer OURS which is verified by 25 years of empirical data – that’s Lewis

#### No large-scale cyber-attacks or retaliation

Nye 19 – Dr. Joseph S, University Distinguished Service Professor and Former Dean of the Kennedy School of Government at Harvard University. “Can cyberwarfare be regulated?”, The Strategist, <https://www.aspistrategist.org.au/can-cyberwarfare-be-regulated/>, 10-03-2019

Cyber technology, of course, lacks the clear devastating effects of nuclear weapons, and that poses a different set of problems, because there is no crystal ball. During the Cold War, the great powers avoided direct engagement, but that is not true of cyber conflict. And yet **the threat of cyber Pearl Harbors has been exaggerated. Most cyber conflicts occur below the threshold established by the rules of armed conflict. They are economic and political, rather than lethal. It is not credible to threaten a nuclear response** **to cyber theft** of intellectual property by China **or cyber meddling** in elections by Russia. According to American doctrine, **deterrence is not limited to a cyber response** (though that is possible). **The US will respond to cyberattacks across domains or sectors, with any weapons of its choice, proportional to the damage that has been done. That can range from naming and shaming to economic sanctions to kinetic weapons**. Earlier this year, a new doctrine of “persistent engagement” was described as not only disrupting attacks, but also helping to reinforce deterrence. But the technical overlap between intrusion into networks to gather intelligence or disrupt attacks and to carry out offensive operations often makes it difficult to distinguish between escalation and de-escalation. Rather than relying on tacit bargaining, as proponents of “persistent engagement” sometimes emphasize, explicit communication may be necessary to limit escalation.

#### Self-dampening checks escalation

Sørensen and Nyemann 19 – Heine, Senior Lecturer at the Institute for Strategy at the Royal Danish Defence College. Dorthe Bach, Senior Lecturer at the Institute for Strategy, Royal Danish Defence College, 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, <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/783151/20190304-MCDC_CHW_Information_note_-_Deterrence_by_Punishment.pdf>, 03-xx-2019

The Flipside of Deterrence by Punishment – the Fear of Escalation One of the greatest reservations against communicating a willingness to take punitive actions concerns the risk of escalation and increased tension due to a more assertive or offensive posture. Yet when looking into possible responses – retaliation in cyberspace, for example – a number of “self-dampening” mechanisms appear to be in place that may be applicable to many types of responses.30 One example is the requirement to establish some level of attribution of aggression on which to base a response. As discussed above, while attribution is rarely impossible, it can be a time-consuming and technically-challenging endeavor. In a high-stakes scenario the time taken to get attribution as right as possible means there will be plenty of time to think twice about actions and consequences, and to lean on diplomatic measures in parallel. An example of a self-dampening mechanism related to the cyber domain is the large investment required to develop credible offensive capabilities. Moreover, an offensive cyber capability is a transitory tool31. The ability to access a computer system or network to cause harm or damage is only temporary and dependent on a very rapid and ongoing patching of vulnerabilities. At the same time, wielding the cyber instrument despite the downside of “burning” the capacity might have a de-escalatory effect by communicating capability and credibility to the opponent with a view to discouraging future hostile attacks. Targeting in any domain – including cyberspace – must also follow relevant rules, law and due-process which will self-limit the range of targets and actions available. A final “escalatory showstopper” is related to the challenge of identifying and developing targets of adequate strategic significance – not too much, not too little – to achieve the desired effect. Responding to hybrid aggression by applying “middle range” punitive actions that are proportionate to the aggression threatened or suffered will also self-limit the escalatory potential. It is unlikely to be in the interest of any hybrid aggressor to pursue an escalatory spiral above and beyond where they were looking to compete in the first place: on the hybrid level. Nevertheless, one way to mitigate the risk of escalation – while enhancing civilian oversight and interagency coordination – would be to establish rules of engagement for punitive actions on the hybrid level32 . This would provide decision-makers with common guidelines to pursue punitive actions that fall below the “use of force threshold”. Moreover, this could actually bolster the credibility of punitive actions by signaling to hybrid aggressors the intent to take pre-prepared punitive actions when deemed necessary: in other words, a “playbook” for countering hybrid threats.

#### Prefer statistics

Valeriano and Maness 18 – Brandon, PhD, Chair of Armed Politics at the Marine Corps University, Cyber Security Senior Fellow at the Atlantic Council. Ryan, an American cybersecurity expert, Defense Analysis Professor at Naval Postgraduate School. “How We Stopped Worrying about Cyber Doom and Started Collecting Data”, Global Cybersecurity, Vol. 6, No. 2, <https://www.cogitatiopress.com/politicsandgovernance/article/view/1368>, 06-11-2018

6. Expanding Cyber Security Data **Our team has been coding** cyber incident **data since 2010** and serves as a unique example of how the process of collecting cyber security data and evidence can be done. Our first peer reviewed published work appeared in 2014 in Journal of Peace Research (Valeriano & Maness, 2014). In this article we note that **cyber conflict is much more restrained than generally understood** by popular discourse. **Threat inflation is ripe in cyber security**, and the real use of cyber tools seems to be to enhance the power of strong states. The data that Valeriano and Maness (2014, 2015) have built challenges the cyber revolution perspective and does so with the tools of social science, and is a necessary turn given the general tone of the debate. We first determine that a viable data collection method in light of limited resources was to focus on states that are committed interstate rivals (Diehl & Goertz, 2001). This allows us to focus on those actors with an intense history of recent hostilities that should be the most likely users of cyber technology on the battlefield (Maness & Valeriano, 2018). In our research (Maness & Valeriano, 2016; Maness, Valeriano, & Jensen, 2017; Valeriano & Maness, 2014, 2015), we have been able to marshal a massive amount of evidence that is useful in dissecting the actual trends on the cyber battlefield in a geopolitical context. We demonstrate that while **cyber-attacks are increasing in frequency, they are limited in severity**, are **directly connected to traditional territorial disagreements, and** mostly **take the shape of espionage and low-level disruptive campaigns rather than outright warfare**. Given this data-based perspective, we question the dynamics of the cyber security debate and offer a countering theory where **states are restrained from using more malicious cyber actions due to the limited nature of the weapons, the possibly of blowback, the connection between the digital world and civilian infrastructure, and the reality** that **any cyber weapon launched can be replicated and used right back against the attacker**. Given all of these perspectives gleamed from the data, **we must moderate our views** about the transformation that is offered by cyber strategists who stress a more revolutionist tone (Lango, 2016). **Social science** clearly **matters** for contemporary technological policy debates. **Absent rigorous methods**, much of what is in **the field is** basically **guesswork**. Our work really owes an intellectual debt to J. David Singer, who started the effort to quantify war at the University of Michigan with the Correlates of War (COW) project (Small & Singer, 1982). Our project builds on this methodology and uses many of the same coding strategies. We recognize that data is a work in progress and seek to build more and more knowledge through subsequent updates. By gathering the full picture, we can gain the perspective that really matters in these emerging policy debates regarding the cyber battlefield.

#### Cyber weapons haven’t killed anyone in 30 years – Reversible consequences mean attacks don’t provoke war.

Borghard and Lonergan 19 – Erica, Assistant Professor at the Army Cyber Institute at the United States Military Academy at West Point and a research fellow at the Saltzman Institute of War and Peace Studies at Columbia University, PhD in political science from Columbia University. Shawn, Research affiliate of the Army Cyber Institute at the United States Military Academy at West Point and a cyber officer in the US Army Reserve currently assigned to 75th Innovation Command, PhD in political science from Columbia University. “Cyber Operations as Imperfect Tools of Escalation”, Strategic Studies Quarterly, Vol. 13, No. 3, pg. 122-145, <https://www.jstor.org/stable/26760131?seq=1#metadata_info_tab_contents>, xx-xx-2019

Limited Costliness of Offensive Cyber Effects Even under circumstances in which a state may possess the right cyber response capabilities at the desired time, its response may not generate sufficient costs against the target to be perceived as escalatory.41 Fundamental limits on the cost-generation potential of offensive cyber operations stem from the fact that cyber capabilities lack the physical violence of conventional and nuclear ones. Cyber weapons target data; they disrupt, manipulate, degrade, or destroy data resident on networks and systems or in transit.42 Moreover, aside from those cyber capabilities that permanently destroy data and for which there are no backups to which a target can revert, cyber effects are temporary and often reversible. The utility of military instruments of power for the purposes of coercion or brute force inheres in their abilities to inflict—or credibly threaten to inflict—significant damage and harm against a target state (its civilian population or its military forces) to achieve a political objective.43 Cyber weapons could be (and have been) used to disrupt an adversary’s networks and systems—overwhelming them such that they temporarily lose the ability to function or the target loses confidence in their reliability—or even to produce destructive effects by destroying data resident on these systems or, in rarer circumstances, producing effects in the physical realm.44 While conducting multiple cyberattacks against a targeted state’s critical national infrastructure, for example, could in theory generate significant economic and national security consequences, the temporal aspects of offensive cyber operations as described above limit the ability of even the most capable states to sustain persistent, high-cost effects against multiple strategic targets over time. There is simply no guarantee that a state can generate significant costs against a target in the context of an unfolding crisis. This reality starkly contrasts with the relative predictability and reliability of conventional effects. Indeed, the empirical record has largely validated this claim; “the vast majority of malicious cyber activity has taken place far below the threshold of armed conflict between states, and has not risen to the level that would trigger such a conflict.”45 This is why, in Lin’s parlance, “going cyber is pre-escalatory” and countervalue cyberattacks (those that target civilian, rather than military, assets) occur “all the time now and are at the BOTTOM of the escalation ladder” [emphasis in original].46 Rather than their ability to wreak permanent, destructive effects, cyber operations are often prized for their temporary and reversible nature.47 One metric to assess the cost-generation potential of offensive cyber is in terms of loss of life. By this measure, cyber operations are unlikely to inflict significant harm. While theoretically possible that cyber operations could lead directly to a loss of life, no one has reportedly died to date as a direct result of a cyberattack despite over 30 years of recorded cyber operations.48 Even in hypothetical catastrophic scenarios, the cost in terms of human casualties is minimal. For instance, common worst-case scenarios of cyberattacks revolve around the loss of power stemming from a cyberattack on an electric grid.49 However, even in this instance, the conceivable damage from the loss of power over an extended period is far less than that which could be wreaked using basic, limited conventional capabilities. To draw a comparison, when Hurricane Sandy hit the United States’ eastern seaboard in late October 2012, over 8.5 million people were left without power—with many going weeks and even months before it was brought back online.50 Yet a US National Hurricane Center postmortem of Hurricane Sandy reported that of the 159 people in the United States killed either directly or indirectly, only “about 50 of these deaths were the result of extended power outages during cold weather, which led to deaths from hypothermia, falls in the dark by senior citizens, or carbon monoxide poisoning from improperly placed generators or cooking devices.”51 If a cyberattack took out power of a similar magnitude and duration of Hurricane Sandy, it is conceivable that an equivalent number of casualties would result. The 2015 synchronized cyberattacks against Ukrainian power companies, attributed to Russia, was the first known example of an offensive cyber operation targeting a state’s power grid. Its cost was ultimately low—service was temporarily disrupted to 225,000 customers for several hours, and energy providers operated at a limited capacity for some time after service was restored.52 There were no reported casualties from this power outage. While any casualty resulting from a cyberattack would certainly be lamentable, even worst-case scenario figures are minor in comparison to the cost in human lives stemming from other, even limited, kinetic military operations.

#### Attacks are too risky and patching vulnerabilities solve

Valeriano et al. 18 – Brandon, PhD, Chair of Armed Politics at the Marine Corps University, Cyber Security Senior Fellow at the Atlantic Council. Benjamin Jensen, Associate Professor at Marine Corps University and a Scholar-in-Residence at American University, School of International Service. Ryan Maness, an American cybersecurity expert, Defense Analysis Professor at Naval Postgraduate School. “Cyber Strategy: The Evolving Character of Power and Coercion”, Oxford University Press, pg. 211-214, xx-xx-2018

What do the insights in this book tell us about the future of cyber exchanges between rivals? To paraphrase the acclaimed science fiction writer William Gibson, the future is already here, it is just not evenly distributed. The next 10 years will likely see an acceleration in the use of what Soviet thinkers called active measures and what George Kennan called political warfare. We are not optimistic that the current US administration will be able to sustain, much less lead, a multilateral cyber order that constrains the worst tendencies of rivals engaged in strategic competition. Yet, given the unique nature of cyber operations, we still assess **minimal risks** to covert action in cyberspace unleashing inadvertent escalation in the military domain. The world is witnessing the reawakening of an old strategic practice: political warfare. The connectivity of the modern world puts a premium on coercive diplomacy in the shadows. From election tampering and fake news disseminated across multimedia in Ukraine (2014), the United States (2016), and France (2017), states such as Russia use cyber operations to enable covert influence campaigns short of war. These operations extend beyond undermining democracies, and are also creating rifts among autocratic allies. In June 2017, an APT group linked to the United Arab Emirates (UAE) triggered a diplomatic crisis in the Persian Gulf by taking control of a Qatari news website. After hacking the online news feed, the group planted false information showing the emir praising Iran and calling for good relations with Israel while (contradictorily) backing Hamas and the Muslim Brotherhood (Bing 2017a). The intrusion was followed by a massive DDoS attack on Al-Jazeera, the Qatari owned media outlet (Kirkpatrick and Frankel 2017). In effect, UAE operatives conducted a classic psychological warfare operation that undermined the integrity of an alliance network. The news agencies in multiple Gulf States ran with the false story, leading to a diplomatic and economic blockade of Qatar by Saudi Arabia, Bahrain, Egypt, Jordan, and the UAE. Cyber incidents like these show how states are mixing the old with the new. Much like the early Cold War, emerging cyber operations combine espionage, propaganda, economic warfare, and sabotage in an effort to signal resolve and shape adversary foreign policy (Valeriano, Maness, and Jensen 2017). The character of war and strategic competition is changing. The new Cold War is online. The connectivity of the digital domain amplifies the effects of political warfare. Social media helps rival states reach key constituencies in their competitor’s domestic populations, a phenomenon on display in the Russian purchases of ads on Facebook and Twitter during the 2016 US election. The extension of commerce and governance online creates vulnerabilities for states. Rivals can target economic capacity in a manner that used to require states to wage open, economic warfare. They can conduct sabotage through malicious code, as opposed to explosive satchel charges. The question that remains is, why are we not seeing more concessions as a result of cyber coercion? The answer lies in the unique character of cyber operations. Cyber instruments are a use-it-and-lose-it coercive instrument that come with an **inherent amount of risk**. To gain network access for higher-cost and compellence-producing degradations, states must first infiltrate and map their rival’s networks. This access gives them a position of advantage. They can extract information and monitor their rival, even if imperfectly. The decision on whether or not to execute a follow-up attack has to be balanced with the costs of losing network access. Once you convert your initial infiltration into an attack vector, **you lose the access**. In theory, this additional cost shifts the cost-benefit calculus associated with cyber operations **in favor of restraint** or using **lower-level cyber disruptions** that do not burn exploits because to do otherwise is quite risky. This “use it and lose it” dynamic is amplified by the shadow of the future unique to political warfare in the digital domain. For leading powers such as United States that have multiple cyber rivals (Russia, China, Iran, North Korea), the cost associated with burning a vulnerability is increased. Once a cyber operation is outed, states and the private sector move to **patch the vulnerability**. There are not an infinite number of vulnerabilities. Therefore, every attack, in theory, **decreases the number of future attacks you can launch** against a rival. For the United States, this condition means that if it chooses to launch a cyber degradation action against China, that specific attack vector will likely be lost in exchanges with Russia. Therefore, while the world is likely to see an increase in election hacking, false flag operations, DDoS attacks targeting key companies, and ransomware, there is unlikely to be an increase in political concessions. The risk of 21st-century cyber disruption and intrigue lies more in proliferation risks. A further constraining feature on launching cyber operations is the fact that, unlike a limited missile strike, the **rival can copy the code** and **increase its own cyber capabilities**. Rivals learn from and can emulate cyber coercive instruments at a faster rate than they can from military competition. States find it is easier to replicate code associated with a rival’s cyber offensive operation than they do building a fifth-generation aircraft based on stolen plans.