Resolved: The United States federal government should substantially increase its security cooperation with the North Atlantic Treaty Organization in one or more of the following areas: artificial intelligence, biotechnology, cybersecurity.

# Affirmative

## 1AC

### Advantage---1AC

#### The Advantage is cyber deterrence---

#### NATO lacks cyber redlines---makes Russian escalation likely.

James Pearson and Jonathan Landay 2/28/22. Reuters. "Cyberattack on NATO could trigger collective defence clause". Reuters. 2-28-2022. <https://www.reuters.com/world/europe/cyberattack-nato-could-trigger-collective-defence-clause-official-2022-02-28/>

Whether or not a cyberattack met the threshold of an attack large enough to trigger Article 5 was a "political decision for NATO Allies to make," they added.

Britain and the United States have warned of potential cyberattacks on Ukraine which could have international consequences should, for example, malicious software designed to target networks in Ukraine start to spread elsewhere. read more

There has also been concern among cybersecurity experts that Russia could team up with some of the gangs and people who release malicious software, such as malware used to hold Colonial Pipeline to ransom in the United States last year.

U.S. Senate Intelligence Committee Chairman Mark Warner said there were no clear guidelines on how NATO (North Atlantic Treaty Organization) should respond, should such an attack take place.

"These are things that have been in hypothetical discussion for a decade, but because we've not come to any universal conclusion on what those standards should be, what level of attribution is needed, we're kind of in a very grey area," he told Reuters.

He posed the hypothetical case of a Russian cyberattack on Ukraine that impacts NATO member Poland, triggering power outages that result in hospital patients dying or knocking out traffic lights, causing fatal road accidents involving U.S. troops deployed there.

"The West may have wanted strategic ambiguity in this area, and that may still be the right choice," he added.

"But have we sufficiently made clear to the Russians the red lines on cyber or frankly to the NATO public, the American public, on red lines on cyber? I don't think we've done that."

Warner said he was "pleasantly surprised" a massive Russian cyberattack had not occurred. But he added that such an attack "becomes even more dangerous with Putin elevating the readiness of his nuclear weapons."

#### Russian cyberwar escalates---the information age creates existential spirals.

Jason Healey 3/9/22. Senior research scholar at Columbia University’s School for International and Public Affairs. Formerly a director for cyber policy at the White House. "Preventing Cyber Escalation in Ukraine and After". War on the Rocks. 3-9-2022. https://warontherocks.com/2022/03/preventing-cyber-escalation-in-ukraine-and-after/

There are multiple ways cyber conflict around the Ukrainian invasion might escalate into a direct conflict between Russia and NATO, possibly as a result of either side’s offensives.

First, Russian offensive cyber operations might spark a wider war. President Vladimir Putin has declared sanctions “are akin to a declaration of war” and may see aggressive cyber attacks as the perfect response, particularly since they are reversible and non-lethal. Russia has been entangled with Western economies for decades, especially in the realms of energy and finance. But now, as ties are being severed quickly and viciously, Russia no longer has to fear the backlash if its cyber forces were to disrupt Western banks or liquified natural gas terminals. If you are dealt out of the game, why not just flip the table?

Russia’s cyber generals may be just as enthusiastic as their Army counterparts. They may assure Putin their forces are ready for battle and can quickly and bloodlessly get the West to back down. Putin could be convinced disruptive attacks against the West are no big deal, a low-cost signal that the West should de-escalate or just the next natural move in a non-escalatory intelligence contest. After all, U.S. research found that in response to cyber attacks, “Americans are less likely to support retaliation with force” compared to a more traditional strike.

This can lead to escalation in two ways. The United States — along with countries like the United Kingdom, France, and the Netherlands — might well decide to defend forward against such attacks. Gen. Paul Nakasone, the commander of U.S. Cyber Command, has insisted his forces “must take this fight to the enemy, just as we do in other aspects of conflict.” His then-deputy has also argued that the United States “cannot cede any territory” to adversaries as the “Russians will keep pushing until we push back on them.”

Worse, Dmitri Alperovitch recently warned that if Russia launches cyber attacks after “[h]aving already exhausted the power of economic sanctions, America and its European allies would have few choices other than to respond to these attacks with offensive cyber-strikes of their own.” Such dynamics can feed a spiraling escalation in cyberspace that might take on a life outside of the control of policymakers.

Second, Western offensive cyber operations might spark war. U.S. cyber espionage and operations against Putin, his cronies, or Russia’s military forces will appear far more ominous to Putin if he believes they are aimed at regime change. Could Putin turn the other cheek if the United States were to electronically raid the cryptocurrency wallets of Russia’s sanctions-avoiding kleptocrats? He might feel the need to escalate his own cyber operations as part of his own version of defending forward.

Escalation could happen on the battlefield as well. According to the New York Times, teams from U.S. Cyber Command are “in place to interfere with Russia’s digital attacks and communications.” Other teams are almost certainly collecting digital intelligence on the location and intent of Russian combat forces. The United States is sharing such intelligence with the Ukrainians but apparently not yet providing any real-time targeting. That may change soon, as the United States seeks to alleviate intensifying attacks on civilians. And with his KGB-bred paranoia, Putin might already see the presence of U.S. defensive and intelligence teams operating on or against Russian military networks as evidence of direct U.S. involvement in the war. Confirming his apparent belief that Ukraine is just a NATO puppet, this might force a response, either inside or outside of cyberspace.

Further, if Western governments have infiltrated Russia’s operational military networks, they may feel pressure to disrupt those networks to prevent civilian massacres. Because cyber capabilities are billed as non-lethal, reversible, and non-escalatory, tub-thumping newspapers may push decision-makers to take shots they might not otherwise: “We can’t create a no-fly zone but can use cyber capabilities to prevent civilian harm.” Some well-meaning national leaders may succumb to this pressure, potentially causing a larger conflict.

Future Risks

Even if Russia and the West avoid direct conflict this time, they might not be so lucky the next. As relations worsen, future disruption of critical Western infrastructure by Russian intelligence, such as the NotPetya and Olympic Destroyer attacks, are less likely to be viewed as mere crimes. Repeated crises bordering on war may further erode the tacit agreements and relative restraint of quieter times. After repeated iterations of intensifying cyber operations, both Russia and the West may feel their backs to the wall with few options left other than military force when the next crisis — physical or cyber — emerges. Under extreme conditions, some of the same characteristics that lead cyber capabilities to be a pressure release might have the opposite effect, a mechanism that Bob Jervis and I have described as the Escalation Inversion.

If Putin believes a direct conflict with NATO is likely and expects its adversaries to take measures to reduce vulnerabilities, he could conclude that the best possibility for success is to launch a massive preemptive cyber attack. Since the U.S. military may seem otherwise unbeatable, this may lead Russia to “compensate with audacity in order to redress the balance.” The more the United States brags about its overwhelming offensive cyber advantage, but frets over weak defenses, the more any adversary might feel the need to target the United States as early and as hard as possible.

If Russia fears war with the United States may happen on Saturday, it might feel the need to get in its cyber punches on Friday. If the United States thinks the same, it may need to start on Thursday. Cyber capabilities may be to World War III as mobilization timelines were to World War I.

Since a cyber sucker punch may also seem less escalatory, adversaries could be tempted to take risks they would not otherwise. In this situation, the sense that cyber is a pressure-release valve becomes positively dangerous: If the system is seen to be stable, then there is less reason to act with restraint, thereby making it less stable. Fortunately, the good news is leading U.S. policymakers appear attuned to this risk.

Avoiding Escalation

How can Washington reduce the risk of cyber attacks escalating into a direct conflict with Russia? First, by recognizing it. Cyber conflict may be an intelligence contest or a pressure release in peacetime and something quite different during or after a major war in Europe. Cyber war may be far easier to stumble into when states fear the wolf at their door.

Second, escalation control requires a better understanding of political psychology — specifically the mindset and desperation of one inscrutable, increasingly isolated, and blood-covered tyrant. There were more than enough expert commentators who believed that Putin would never invade Ukraine because it objectively seemed so irrational. Assessments of cyber escalation must also cover seeming irrationality, including the misperceptions, mistakes, and miscalculations that can lead even the most rational leaders to get caught up in an escalatory spiral that is no longer under their control.

Third, preventing escalation requires military and intelligence leaders to understand and respect cyber capabilities. Cyber capabilities are not “magic invisible weapons” but rather real weapons with massive, cascading consequences. They have a range of advantages and restrictions that sober-minded national leaders should approach as they would any other weapon.

Finally, even if we dodge a bullet this time, we should not become complacent. Personally, I would put the chances of cyber conflict escalating into a Russia–NATO war at less than 10 percent. With luck, escalation will not happen, and I will be written off as a “cyber catastrophist.” “Cyber doesn’t work like that,” we will tell ourselves. “Remember the lessons of the Ukrainian cyber non-war. Cyber doesn’t escalate. It isn’t useful on the battlefield or for coercing other states.”

This will hopefully continue to be true for weeks or even years. But the world is in the first few decades of an information age that will continue for a long time. The existential stakes of cyber conflict rise as more countries become more digitized and more reliant on vulnerable information technology.

#### [OPTIONAL] A single Russian cyber-attack is comparable to nuclear war---shuts down society.

Loren Thompson 14. PhD from Georgetown; Former Deputy Director of the Security Studies Program at Georgetown University and taught graduate-level courses in strategy, technology and media affairs at Georgetown. Taught at Harvard University's Kennedy School of Government. "Cyber Alliances: Collective Defense Becomes Central To Securing Networks, Data". Forbes. https://www.forbes.com/sites/lorenthompson/2014/09/19/cyber-alliances-collective-defense-becomes-central-to-securing-networks-data/

It isn't hard to see why NATO is worried about threats in cyberspace, given Russia's recent use of on-line attacks against Ukraine and other countries in a style of combat that has come to be called "hybrid warfare." However, a report by the Pentagon's prestigious Defense Science Board released last year suggests that the cyber challenge reaches far beyond the use of botnets and distributed denial-of-service tactics. Describing the extensive vulnerability of U.S. military forces to cyber assault, the report then observed,

The impact of a destructive cyber attack on the civilian population would be even greater with no electricity, money, communications, TV, radio or fuel (electrically pumped). In a short time, food and medicine distribution systems would be ineffective; transportation would fail or become so chaotic as to be useless. Law enforcement, medical staff, and emergency personnel capabilities could be expected to be barely functional in the short term and dysfunctional over sustained periods.

These sustained periods, the science board stated, might last "months or years" as government and industry sought to rebuild damaged infrastructure -- a possibility that led the panel to compare the specter of state-sponsored cyber attacks to the threat of nuclear war. So if you think that 56 million payment cards being compromised at Home Depot is about as bad as cyber threats can get, think again. Civilians and soldiers alike have hardly begun to experience how destructive the coming age of information warfare is going to be.

#### [OPTIONAL] Damage ensures nuclear escalates---both sides retaliate.

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

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

#### [OPTIONAL] Lack of clarity about escalation increases the probability of nuclear use.

Leonard Spector 4/25/22. Former senior official at the US National Nuclear Security Administration and a Distinguished Senior Fellow at the James Martin Center for Nonproliferation Studies. “Cyber Offense and a Changing Strategic Paradigm.” The Washington Quarterly, 45:1, 38-56, DOI: 10.1080/0163660X.2022.2054123

This reorientation might seem a positive development by possibly lowering the threat of nuclear conflict. But this optimistic conclusion is not clear-cut. To be sure, the destruction from massive cyberattacks against critical infrastructure would be orders of magnitude less than that caused by nuclear war. It is also true that calibrated infrastructure cyberattacks provide additional pre-nuclear rungs to the escalation ladder, possibly making resort to nuclear arms more remote.6 Massive infrastructure cyberattacks, however, could nonetheless cause catastrophic devastation, leading to years of national hardship and considerable loss of life from the collapse of food, water, medical, and other essential systems.7 Moreover, the very fact that such infrastructure attacks avoid the unbounded cataclysm of nuclear war increases the likelihood that this cyber capability could be used, potentially to the great harm of the targeted state. Nor can the threat of retaliation with nuclear arms to an unrestrained cyberattack be ruled out, a possibility the United States, at least, appeared to invoke in the US 2018 Nuclear Posture Review. 8 China and Russia have also implicitly left the door open to responding with nuclear weapons to such an attack.9

#### Only clear redlines solve---NATO-Russia cyberwar goes nuclear.

Tom O'Connor, Naveed Jamali, and Fred Guterl 6/18/21. Tom O'Connor, award-winning senior writer of foreign policy at Newsweek. Naveed Jamali, Newsweek editor at large; former FBI double agent. Fred Guterl, Special Projects Editor at Newsweek. "Will Putin's hackers launch a cyber Pearl Harbor—and a shooting war?". Newsweek. 6-18-2021. https://www.newsweek.com/2021/07/09/will-putins-hackers-launch-cyber-pearl-harbor-shooting-war-1601791.html

Most Americans seem to assume that a cyber attack, even by an avowed adversary like Russia or Iran, would be answered in kind—that the U.S. would cause an annoying power outage or a brief internet failure. But experts and former intelligence and cyber-security officials tell Newsweek that hackers linked to Russia have launched cyber attacks on the U.S. that have come frighteningly close to the red line: a digital incursion that would prompt a deadly real-life response.

As the U.S. continues to prove vulnerable to ransomware attacks from shadowy groups believed to be operating out of Russia or other former Soviet bloc countries, those with experience in advising the White House on challenges from the region urge Biden to take the opportunity to send a message.

"What I want is for Biden to very clearly explain what the risk is to Vladimir Putin, that we are not going to back down if we are attacked by Russia," says Evelyn Farkas, who served as deputy assistant secretary of defense for Russia, Ukraine and Eurasia, "and that we're going to be the ones that decide what a 'cyber Pearl Harbor' is, which means Russia doesn't control the escalation dynamic."

At least Japanese leaders knew that bombing Pearl Harbor would inevitably provoke a military response. It's not clear that Russia or the cyber-militants operating within its borders have that awareness now. A shooting war between Russia and the U.S., avoided for more than a half-century, would leave only losers. But cyber warfare is so new that there's no agreed upon, widely understood Rubicon, as was established during the Cold War with the use of traditional weapons of mass destruction. (Think: Cuban Missile Crisis. After that near-catastrophe, the two sides have played it safe.)

The lack of clarity—of a shared algorithm for escalation—is tinder that could easily turn into a deadly fire. In short, there's a growing danger of a response far more devastating than the temporary internet outage or compromised credit score or muddled train schedule that Americans might think would be the worst-case scenario.

Russian President Vladimir Putin doesn't directly run the hackers who've recently infiltrated high-level government networks and paralyzed critical infrastructure. U.S. intelligence believes the digital operatives behind those attacks work with the Russian president's blessing but stay at arm's length—the better to give Moscow plausible deniability. It's part of a familiar pattern: Russian-affiliated groups have long harassed U.S. companies and government agencies and even had a hand in swinging the 2016 election to Donald Trump. The Biden administration has not directly accused the Kremlin of sponsoring these attacks but blames the Russians allowing such activity to continue.

The recent attacks seem to mark an intensification. They tend to be more focused on physical infrastructure like food, oil and gas pipelines, and hospitals, upon which Americans rely every day for their health and economic well-being. The trend has national security analysts worried. It's one thing to make Americans wait in line at the pump or to hit hospitals with ransom bills that drive up the cost of health care. It's something else entirely to cause real economic harm and even loss of life. And yet, hackers seem to be flirting with crossing what national security experts say is a "red line."

The red line was high on the agenda in the June 16 talks between Biden and Putin. Biden handed the Russian president a list of no-go targets upon which a cyber attack presumably might be considered an act of war that demands retaliation. Although it's not clear where that red line is—the White House has not released the list—it's not hard to imagine how easy it would be for hackers acting with some degree of autonomy from Moscow, and not directly answerable to the consequences of their actions, to cross it. To take one example, it's become a truism in cyber-security circles that hackers working with the backing of the likes of Russia and China may have the ability to cause a shutdown of a large swath of the U.S. electrical grid, which could kill millions.

In other words, the next big cyber attack could trigger a war with Russia, and not the virtual kind, but one involving troops, tanks, missiles, aircraft carriers and possibly nuclear weapons. "If a nation-state adversary were to set foot on our homeland and physically destroy our infrastructure, we would view this as an act of war," Brian Harrell, former Assistant Director for Infrastructure Security at the U.S. Cybersecurity and Infrastructure Security Agency (CISA), told Newsweek.

#### Russian cyberwar causes secessionism, undermines European democracy, and destroys NATO.

Brian Frydenborg 12/24/20. MS in Peace Operations from George Mason University's School of Public. BA from Washington and Lee University in Politics and History. Former intern in the United States Senate. "The History of Russia’s Cyberwarfare Against NATO Shows It Is Time to Add to NATO’s Article 5". Real Context News (RCN). 12-24-2020. https://realcontextnews.com/the-history-of-russias-cyberwarfare-against-nato-shows-it-is-time-to-add-to-natos-article-5/

The NATO Alliance has served for over seventy years not only as a foundation of preventing armed attacks from Russia and other major powers against most of Europe and North America, but also a foundation of one of the most peaceful and prosperous eras in world history. But there is one major type of warfare that has been hitting NATO member states intensely for years and increasingly so: cyberwarfare. And virtually all cybercampaigns of this cyberwarfare have been waged by Russia, part of Russian President Vladimir Putin’s overall war against the West, especially NATO but also even Western democracy.

Apart from some Chinese hacking/cyberespionage known to have begun at least by 2003, the first two serious cyberassaults (in these cases carried out much more so as part of geopolitical cyberwarfare campaigns) were Hezbollah’s and Israel’s surprising cyberattacks against each other during their 2006 war and Russia’s less-surprising but far larger cybercampaign against NATO-member Estonia in 2007, just three years after it had joined the Alliance. It was not long after that when it became clear Russia was absolutely a bad-faith actor with which we have needed, since the last years of the George W. Bush Administration and through the Obama and Trump Administrations, to take a much tougher stance, as I have argued before.

Unsurprisingly, then, the two countries that have led in cyberwarfare since are Russia and China, the first being the weaker of the two but also NATO’s (and America’s) clearest top state enemy and the second being the overall stronger of the two, but more restrained and America’s clearest top state rival for global power and influence. Though China has conducted its own massive hacking and espionage operations (not uncommon among major powers) and has its own influence operations, it is Russia that has without question been the dominant aggressor with acts far more hostile than hacking operations focused mainly on espionage. In fact, Russia is unique among major powers in carrying out significant acts of hostile cyberwarfare beyond espionage ever since its Estonia campaign. And while espionage against NATO states is bad for any of those states, espionage has long been viewed as separate from acts of war and should remain in a different category from acts of war in all but the most extreme of cases, a select level in which the latest Russian cybercampaign (detected to be only espionage so far even if at a historic level) seems begging to be included.

Since the Estonia campaign, Russia become dramatically more aggressive against NATO, often skillfully manipulating nationalisms (as I discussed recently) and flooding NATO member states with cyberwarfare, with election interference and boosting secessionism as common features. Notable cybercampaigns have been directed at the United States, the United Kingdom (including the Scottish independence and Brexit referenda), Germany, France, Italy, Spain, the Netherlands, Bulgaria, Norway, Estonia, Latvia, Lithuania, the Czech Republic, Canada, Turkey, Denmark, Romania, Poland, Slovakia, Montenegro, and even (North) Macedonia, unsurprisingly focused there on preventing its recent accession to NATO (and these do not even get into campaigns carried out beyond NATO territory).

These cybercampaigns involve thousands of Russian government paid-trolls and Kremlin-created bots operating thousands of fake accounts that create millions of Tweets, comments, and posts. And the way these operations tend to work is by promoting politicians and political parties coopted or compromised by or even favorable to Russia and Putin’s agenda and slamming their opponents or anyone critical of Russia and willing to stand up to Putin.

Many of the parties getting the most help (including funding) from Russia exhibit the same hackneyed brand of thoroughly boring right-wing ethnonationalism of the type embraced by Putin’s own United Russia party, which has in recent years forged alliances with several major political parties in Europe, including in major NATO states Italy, Germany, and France (and there are suspicions about the UK, where details of this remain redacted in the recent British parliamentary Russia report). Similar political interference efforts are known to extend beyond NATO countries.

Using its primary hybrid mix of disinformation, hacking, and propaganda, and with a network that combines top Kremlin figures, shadowy Russian government operatives, oligarchs in Putin’s pocket, and various state-linked media “outlets,” these operations have had far more effect than most people in NATO countries realize: helping to sway the views of many millions and dramatically distorting public discussion, politics, and policies in countries on everything from Ukraine (see the Hunter Biden “story,” for years a Russian disinformation campaign) and Syria to sanctions and even the current coronavirus pandemic. This model is skilled at preying on ignorance and confirmation bias to turn media outlets and citizens alike in these NATO states into Kremlin allies, whether as unwitting “useful idiots” or witting Fausts. From Donald Trump and France’s Marine Le Pen and Brexit champion Nigel Farage to Fox News’ all-stars and “contrarian” journalists Glenn Greenwald and Matt Taibbi, for a variety of reasons, extremists not only on the right but also on the left embrace or parrot Kremlin talking points and narratives after years of these effective influence operations, shaping debate from both within the halls of government power and newsrooms, corrupting and bending the debate to Russia’s ends. Russian disinformation is thus vastly amplified and passed on further as misinformation by the duped and again as disinformation by the corrupted so that public opinion, media, and even laws and policies become more anti-NATO, more anti-EU, more anti-American, more pro-secession, more pro-Russia, more pro-Putin as a result. And when the Kremlin’s candidates win, they and their allies may spout Russian disinformation to suit their ends, as former FBI counterintelligence agent Asha Rangappa explains is the case with the Trump Administration. They can also can move to obstruct efforts to both investigate Russian infiltration and hold Russia accountable for its cyberwarfare, with clear and indisputable examples of late from the Trump Administration and Boris Johnson’s UK government as illustrated clearly in the Mueller report and the aforementioned British parliamentary report, respectively. Even when the Kremlin’s chosen do not win, these Russian operations still manage to weaken their victorious opponents and skew political atmosphere.

All this has been the case to varying degrees from Washington to Rome, from London to Berlin, weakening NATO and its ability to collectively defend itself. Over time, the degree to which the pendulum has swung to more pro-Russian positions and people has been nothing short of remarkable and very much in part because of Russia’s concerted cyberwarfare effort. And all this further divides the Alliance and even member states’ own societies internally, which itself is also a major goal of Russia’s.

Time to Adapt NATO’s Article 5 for the Cyberwarfare Era

Thus, what Russia and the Soviet Union before it had been unable to do for decades with conventional armed forces Putin is now to a significant degree accomplishing through cyberwarfare. And while the NATO Allice had been incredibly effective in preventing and deterring armed attacks, it has had a dismal record at preventing and deterring cyberattacks, a trend that is only increasingly so as Russia’s cyberassaults become more and more brazen, with Russia’s only-just-detected massive months-long and ongoing cyberespionage campaign (and perhaps much more than cyberespionage, we may discover over time) making this only pathetically more obvious.

While NATO’s Article 5 does not exclude cyberwarfare from being considered a pretext for a collective response, it has not been one in practice and the extreme lack of clarity or cohesion from NATO only has Russia acting on the cyberwarfare front with impunity.

To this end, cyberwarfare—including information warfare—must be explicitly included in Article 5, with “or cyberattack” added after the three instances of “armed attack” in the Article.

I will elaborate much more on how this will work in the future, but for now, even this brief historical overview of the intersection of NATO, Russia, and cyberwarfare makes obvious the dire need for a new approach for NATO to reinvigorate a domain of warfare that has been nothing but a grand embarrassment for the Alliance in the face of sustained Russian aggression. Only with a new, clear, and bold policy that make cyberattacks as off limits as “armed attacks” can NATO continue to secure its members states as it has for most of its history and reverse its loss of power, prestige, and effectiveness Russia’s relentless cyberassaults have already initiated and inflicted.

#### European secessionist conflicts go nuclear.

Barry Blechman et al. 15. Dr. Barry M. Blechman is co-founder and a Distinguished Fellow of the Stimson Center. Alex Bollfrass, Former Nonresident Fellow. Laicie Heeley, Former Fellow with Stimson’s Budgeting for Foreign Affairs and Defense program "Reducing The Risk Of Nuclear War In The Nordic/Baltic Region. Stimson Center". Stimson Center. 12-15-2015. https://www.stimson.org/2015/reducing-risk-nuclear-war-nordicbaltic-region-0/

Europe is currently experiencing escalating political and military tensions that are rekindling fears of war between Russia and NATO. Any such conflict would inherently include a risk of nuclear weapons use. The Stimson Center, partnered with Project High Hopes, is examining the results of such nuclear exchanges and, more importantly, developing initiatives to avoid such catastrophes.

Vladimir Putin has revealed that he was prepared to use nuclear weapons in the Ukraine crisis and would protect ethnic Russian populations through any means necessary. There are significant ethnic Russian populations in Estonia and Latvia with a history of disagreements and some conflict with the national governments. Any armed conflict between a Russian secessionist movement and a Baltic government could provide Russia an excuse for military intervention, which could easily devolve into a war with NATO and a risk of nuclear use.

Illustratively, one could imagine a scenario we call Escalation in Estonia, beginning with the seizure by pro-Russian rebels of local government buildings. Responding to an Estonian request, NATO mobi-lizes against the rebels, and Russian troops move across the border. Desperate to end the conflict before more NATO forces can arrive, in conformity with its doctrine “escalate to deescalate,” the Russians launch two nuclear-armed missiles on NATO forces. NATO, in turn, responds with two nuclear bombs delivered by US B-2 bombers on Russian military headquarters within Estonia. As a result, Tallinn is largely destroyed and nearly 100,000 civilians and military service men and women could be expected to die as a result of the conflict and its aftermath.

#### AND Russia promotes illiberal leaders---collapses international order.

Homeland Security Newswire 17. "Russian hacking, cyberattacks, elections". No Publication. 3-3-2017. https://web.archive.org/web/20190221152350/http://www.homelandsecuritynewswire.com:80/dr20170303-russias-interference-in-u-s-european-elections-could-be-act-of-war-nato-commander?

Bradshaw, who will become NATO commander later this month, said Russia posed a “hybrid threat” to NATO members.

“It’s not just the threat of overt military attack, but it’s a raft of other measures, including covert, paramilitary, and non-military activities, some of which will be coordinated by the intelligence arms of Russia,” General Bradshaw added.

“And we as NATO need to have our antenna tuned to the signs that this sort of hostile activity is going on.”

He accused the Kremlin of “showing a proclivity to disobey the rules of international relations” with its military incursion into Crimea and alleged backing for rebels in eastern Ukraine.

“We need to put in place thoroughly effective and convincing deterrence so that everybody knows where the red lines are,” General Bradshaw said.

“We are effectively building and sustaining military capability so that we never have to use it.”

Bradshaw’s comments come against the backdrop of growing calls in the United States for a thorough investigations of the Russian government’s broad campaign to secure the election of Donald Trump as U.S. president – and the nature and scope of contacts between several Trump’s surrogates and high-level campaign aides and operatives of the two Russian intelligence services – the FSB and the GRU. These two organizations were behind the hacking campaign against the computer systems of the Democratic Party and the Hillary Clinton’s campaign.

The unanimous conclusion of the seventeen agencies making up the U.S. intelligence community was that “We assess Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the U.S. presidential election,” in the words of a report released by the Office of the Director of National Intelligence.

“Russia’s goals were to undermine public faith in the US democratic process, denigrate Secretary Clinton and harm her electability and potential presidency.

“We further assess Putin and the Russian Government developed a clear preference for President-elect Trump.”

A recent report by the House of Commons Foreign Affairs Committee said the “rise of fake news” emanating from Russia was a cause of growing concern, pointing to the role of state-owned outlets Russia Today and Sputnik in spreading Russian propaganda and fake news masquerading as journalism.

European intelligence agencies have said that Russia’s success in helping elect Trump to the presidency of the United States has emboldened Moscow to replicated in Europe the methods it used in its interference in the U.S. presidential campaign. European security services have already seen signs of Russia’s hacking and disinformation campaign aiming to help far-right, ethno-nationalist, and populist politicians win the coming elections in France, the Netherlands, and Germany.

As is the case with Trump, these politicians – Marine Le Pen and the National Front in France, the AfD (Alternative für Deutschland) in Germany, and Geert Wilders and his Party of Freedom in the Netherlands – aim to weaken the West by undermining or dismantling the two central pillars of Western post-Second World War security and prosperity – the system of military alliances, including NATO, and the liberal international economic order, including the EU and the WTO.

Not coincidentally, as is the case with Trump, the three European political movements being helped by Russia are openly pro-Russian and critical of Western economic and political sanctions taken to punish Russia for its actions in Crimea and Ukraine.

#### Illiberal leaders escalate hotspots and fracture institutions---ends the cooperative world order which is key to solve every global existential threat.

Cassidi Beck 20. Masters Thesis in Political Science at Stellenbosch University. “The Rise of Strongmen Leaders: A Threat to Global Security”.

With the rise of Strongmen like Orban, Putin and Erdogan, where these populists have accessed government, a subsequent erosion of liberal democratic principles has been followed (Albertazzi & Mueller, 2013:350). Authoritarian countries are openly challenging global rules and ideas about freedom and making the case that their socio-political systems work better than liberal democracy. These Strongmen pose a “substantial negative effect on democratic quality” (Huber & Schi`mpf, 2017:146 as they “increasingly reject liberal values” (Cederman, 2019:61).

Even if one disagrees with Francis Fukuyama’s thesis, there is still evidence that highlights that, despite its shortcomings, democracy inherently has important tenants that other regimes do not offer. Democracy stresses the intrinsic importance of transparency, civil liberty, rule of law, horizontal accountability, and minority rights. It guarantees fundamental rights and civil liberties – freedom to pursue one’s legitimate interests, to hold political, social and cultural beliefs, and to be able to express them without interference from the state (Albertazzi & Mueller, 2013:350; Mounk & Fao, 2018). High-minded defenders of liberal democracy argue that there is something uniquely legitimate about the political system. Its democratic element, they claim, ensures citizens’ equality, while its liberal element ensures citizens’ freedom. As such, the genius of liberal democracy is that it can honour both these values simultaneously. It allows each citizen access in the public sphere while giving them the ability to have a private life; “only liberal democracy can fulfil some of the deepest and most universal human aspirations” (Mounk, 2018:129-130).

Thus, in conclusion, the use of Fukuyama’s original essay The End of History and the Last Man is not to disagree with or critique his thesis. It is rather a reflection on his thesis and posits that political events currently arising pose an obstacle to this perceived future. Rather, to highlight that current events, specifically the rise of political Strongmen, are incompatible with a future that was believed to be marked by democracy, stability and security. The turbulence of current geopolitics does not have to be read as a rebuttal of Fukuyama’s original thesis, however, an assessment of Strongman leadership and the fluctuations such leadership may bring towards geopolitics are an important contrast to what Fukuyama predicted. The next section will examine more specifically the possible outcomes these Strongmen could have on geopolitical security – the ramifications of their tendency to erode democratic institutions, to violate human rights, promote nationalistic populism and break the principle of sovereignty and international law.

4.3. The Strongman’s Ramifications for Geopolitical Security

Although the rise of the Strongman and their illiberal democracy offers an alternative to democracy, their actions, policies and leadership style indicate that they pose a risk to geopolitical security. In an increasingly connected and globalised world, what appears to be local in nature is in fact global in impact as most elements contain global dimensions (Kaldor, 2001). These rising and existing Strongmen across the globe and their leadership style has the potential of negative ramifications for global security. The actions undertaken by leaders such as Putin, Orban and Erdogan towards democratic institutions, human rights and international law, as well as their nationalistic populism will likely have a far-reaching impact. As noted in Chapter Three, in a regional capacity these leaders have not only undermined their nations’ democracy but have also created an environment of hostility and insecurity. Reflecting on Chapter Three, the next section will examine how these Strongmen’s ability to create regional instability could possibly lead to geopolitical instability and insecurity.

4.3.1. A New Global Order

US Hegemony or “the American century” was born amid the collapse of the Berlin Wall in 1989 and the end of the Cold War (King, 2017:215; Zakaria, 2019:10). Following the collapse of communism, it seemed the West’s model of liberal democracy and free-market capitalism, supported by a clear set of US-sponsored international rules, would spread across the globe. Under the guise of the Washington Consensus, it laid the foundations for recommendations on how nations should interact with one another on the premise of creating wealth and championing liberal democracy (Banos, 2017:92; Rose, 2019:11). In the advocating of the Washington Consensus, the foundation of international law was said to be based on the principles of mutual respect for sovereignty and territorial integrity; non-aggression towards others, non-interference in the internal affairs of others, equality and mutual benefit, peaceful co-existence, respect for human rights and basic freedoms and national self-determination (Banos, 2017; King, 2017; Rose, 2019:11).

However, politically and economically, the West’s vision has seemed to reach its limits, as geopolitical and ideological rivals undermine the foundations of the liberal world order (Frankopan, 2018:52; Kazan & Park, 2019; Russell-Mead, 2018:15). Mounting opposition from emerging superpowers, increasing resistance to globalisation and the core tenants of liberal democracy from emerging political movements, and the rise of political Strongmen across the world, could lead to the creation of a new world order. This rebalancing of power with Strongmen at the helm could have potential implications for global security, as nations like Russia, Hungary and Turkey forge their own political orthodoxy (Banos, 2017:121; Frankopan, 2018:147; Weiss, 2019:92).

Evidence suggests that the new world order, one not championed by a liberal consensus, could potentially lead to a more insecure geopolitical future. This argument extends from the Strongman’s tendency to reject the international rules-based system, as previously noted by Putin, Erdogan and Orban’s dismissal of international law, treaties and the core principle of sovereignty. While the new world order will still be based on a foundation of rules, scholars argue that with Strongmen becoming more prominent and powerful, the resulting new norm will be characterised by geopolitical competition, doubts about security commitments to allies, challenges to the fundamentals of the global trading regime and the abandoning of the promotion of freedom and democracy; these will become the defining features of a new foreign policy (Daalder & Lindsay, 2018:72; Haass, 2019:30; Kazan & Park, 2019). As Orban, Putin and Erdogan have shown, there will be little regard for democratic institutions and tenants, civil rights and political freedoms will be restrained while international law and the principle of sovereignty will hold little value. This could have the potential of escalating rivalries and thus create unstable implications for global security (Frankopan, 2018:144).

This new global order could also potentially see the end of important international institutions and treaties, such as the Trans-Atlantic partnership, the EU, the World Trade Organisation and the International Monetary Fund. International institutions are important as they provide the framework within which countries can happily engage with each other and, help co-ordinate the actions of different countries in order to set stable expectations (Blackwill & Harris, 2016:74; Frankopan, 2018:237). Treaties and international institutions also help to foster security as they provide frameworks through which countries interact, creating cooperation, helping to foster mutual understanding and stability (Haass, 2019:30; Frankopan, 2018:222; King, 2017:225). They also help foster global security as through their creating of cooperation they help to ensure a global response to the creation of solutions for global problems.

Many global issues and threats such as climate change, the refugee crisis, growing terrorism and rising socioeconomic inequalities require the harmonizing of domestic and foreign policies and the willingness of countries to work together. Therefore, without established and agreed upon institutions, the way in which states interact with each other could potentially be characterised as strained and difficult. Future security threats demand a more pluralistic response that can be best accomplished by combining resources (Drozdiak, 2017:91; Frankopan, 2018:74). Prosperity and well-being may depend on global solutions. However, under the guise of leaders like Orban, Putin and Erdogan, many politicians and governments are taking steps to diminish co-operation with each other, disengaging from bilateral agreements and international co-operation. Instead these leaders erode confidence in international institutions and perceptions of stability as they “operate on a tornado of impulses” (Frankopan, 2018:157). As the Strongman is more likely to choose aggression and isolationism over collaboration and cooperation, the world could possibly descend into further conflict as frictions are elevated (Haass, 2019:30; Kazan & Park, 2019; King, 2017:244).

A world order led by Russia under Vladimir Putin, with the support of Turkey’s Erdogan and Hungary’s Orban, would possibly be one characterised by competition over cooperation, protectionism rather than free trade, authoritarianism rather than democracy. Henceforth, evidence suggests that the possible thawing of the liberal democratic world order could be problematic to geopolitical security (Mounk, 2018:114).

An extension of this new global order and how it could potentially lead to increased geopolitical security is that the Strongman’s disregard for democratic norms is contributing to a growing sense of license among autocrats worldwide (Diamond, 2019:20). As more Strongmen come to power and are able to enact their policies, their ‘successful run’ at authoritarianism is making it easier for it to thrive elsewhere. Albright (2018:246) argues that herd mentality is powerful within international affairs and if one leader can follow a specific form of leadership, other leaders around the world are likely to observe and mimic. Thus, with growing assertiveness, disregard for international law yet few consequences and increased economic success, more leaders are turning towards the ‘Strongman playbook’. Strongmen such as Putin, Orban and Erdogan look to others for help in endorsing their regime, favouring one’s authoritarian adversaries over democratic allies (Albright, 2018:246; Mounk, 2018:2). Nudging followers away from the consensus and support for democratic norms, these leaders portray an image that this type of illiberal, autocratic leadership is acceptable (Lendvai, 2017:198). Once where a nation may have consistently held another nation and its leadership in discontent, once in power, the strongman may reverse this decision and instead seek to build a trusting, cooperative relationship (Kearns, 2018:4). For instance, despite the actions of some states towards the negation of human rights and democracy, Russia under Putin has increasingly used its power status to shield other authoritarian states from international demands to protect human rights and block interventions that would force governments to end abuses (Weiss, 2019:95). By allowing nations to continue with their erosion of human rights and political freedoms of its citizens without consequences, it signals to other authoritarian states and Strongman leaders that their actions are acceptable. This then can potentially lead to the possibility of an increased scale across the globe of human rights abuses as autocratic states are not fearful of harmful consequences. Henceforth, this could have serious implications for geopolitical security as more states negate human rights.

When these actions come from democratic countries that have before been strong advocates of democracy, this reversal can have a harmful effect (Albright, 2018:218), particularly in countries where there are already few checks on executive power. The issue with a leader showing these characteristics, especially in a free, liberal and democratic society, is that it signals to other leaders all over the world with these autocratic tendencies are acceptable. If one leader can argue that the press always lies, or the democratic institutions are erroneous, it becomes difficult to fault another across the globe when they make the same claim (Albright, 2018:5; Nance, 2018).

For example, on the invasion of the Ukraine and the illegal annexation of Crimea, leaders across the globe praised Russia’s decision. The leader of the Hungarian fascist party Jobbik praised Putin and Greece’s Golden Dawn praised Russia for defending Ukraine from “ravens of international usury” and France’s Front National lauded Putin’s courageous position against the international lobby (Snyder, 2018:149). With Putin’s actions, and the endorsement he received from other nations, the impression is given that breaking international laws and sovereignty is acceptable.

Together, these Strongmen are creating an alliance of nations led by strong authoritarian leaders who will increasingly pose a risk to the liberal, democratic world order as democratic states fail to stand up to this alliance or prove to be more successful (Lendvai, 2017:214; Nance, 2018). The current world order has not completely eroded but is spearheaded by the rise of Strongmen into political power. The possibility of a new global order emerges – one that appears to create significant geopolitical insecurity. While the Washington Consensus may be faulted, it did help foster a global environment of cooperation and consideration between states, while helping to promote the principles of liberal democracy. A stable world order requires a stable distribution of power and broad acceptance of the rules that govern the conduct of international relations (Haass, 2019:22). However, what the Strongmen champion poses a risk to increased geopolitical insecurity as their policies and ideologies are often centred on conflict, isolationism and protectionism. Instead, they foster a world of unbalanced power and the formulation of their own rules. Further, as more and more nations create a coalition of Strongmen, it will become increasingly difficult to not only stand up to them but also to foster democracy and stability (Kazan & Park, 2019). In a world of ‘complex interdependence’ (Rose, 2019:19), nations cannot fully operate in isolation and such attitudes that fail to acknowledge this and instead foster relationships based on self-interest can only create instability.

#### [OPTIONAL] Defense is insufficient---only deterrence introduces a cost---that prevents election hacking and preserves global democracy.

The Rt Hon Jeremy Hunt MP 19. Foreign & Commonwealth Office. "NATO Cyber Defence Pledge conference: Foreign Secretary's speech". GOV.UK. 5-23-2019. https://www.gov.uk/government/speeches/foreign-secretary-speech-at-the-nato-cyber-pledge-conference

Deterrence in cyber age

Together, NATO countries have become better at defending themselves against dangers in cyber space.

But we should not be content with just making ourselves tougher targets – crucial though that is. Our primary goal must be to deter this kind of behaviour from happening in the first place.

NATO is the most successful military alliance in history precisely because of our collective power of deterrence, and that prevented nuclear war and helped to keep the peace for 70 years. Our profound insight is that strength is the surest guarantee of peace – and when we stand together, no aggressor can hope to win a war so it never makes sense to start one.

The challenge today is therefore to apply the eternal verities at the heart of NATO’s success to the Alliance’s newest operational domain. And that means deterrence – strengthening our joint ability to deter those who would harm our citizens in cyberspace.

We have already made important progress.

In 2014 the Allies agreed that a cyber attack could result in the invoking of Article V of the Washington Treaty, meaning that the incident would then be treated as an attack on every member of NATO.

The North Atlantic Council would take any such decision on a case-by-case basis. Britain was the first ally to offer our offensive cyber capabilities to NATO. Another 8 countries have since done the same.

Then in 2016, NATO leaders endorsed the Cyber Defence Pledge, recognising the ‘new realities of cyber threats’.

But we can and must do more to improve our response. In particular, we should be more emphatic about what we consider to be unacceptable behaviour and the consequences for any breach of international law.

Interference in free elections

At particular risk are the democratic processes in all of our countries.

In the cyber age, authoritarian states possess ways of undermining free societies that dictators of earlier times would have envied. Time and again, we have seen attempts by states to interfere in democratic elections, often through the use of proxies.

In 2014, Russian hackers calling themselves ‘CyberBerkut’ sought to disrupt the presidential election in Ukraine, including by tampering with the voting system and delaying the final result.

In 2016, the Russian state interfered in the presidential election in the United States with the aim of damaging one party’s candidate.

Free elections are at the heart of our way of life. The leaders and ministers of NATO countries have been raised up by the decisions of millions of voters, expressed through the ballot box. We can all be cast down in the same way.

But recent events demonstrate that our adversaries regard democratic elections as a key vulnerability of an open society. If cyber interference were to become commonplace, the danger is that authoritarian states would damage public confidence in the very fabric of democracy.

We cannot afford to wait until one of our adversaries succeeds in changing the result of an election. We must be crystal clear that any cyber operations designed to manipulate another country’s electoral system and alter the result would breach international law – and justify a proportionate response.

Together, we possess options for responding to any attacks that fall below the threshold for Article V. We should be prepared to use them.

Deciding to do nothing would be an important decision in itself – and the consequences could be escalatory.

The more we communicate our resolve to act, the more we lower the risk of miscalculation. The more we work together to develop an array of appropriate response options – and signal our willingness to employ them – the greater our power of deterrence.

As always, we need to balance clarity about our determination to act with constructive ambiguity about exactly what we would do in specific circumstances.

The EU gained one further option last week when we adopted a new sanctions regime, allowing the imposition of travel bans and asset freezes on those who carry out ‘cyber attacks with a significant effect’.

In conclusion let us remember that throughout history, every new technology has created risks and hazards. The problems have often seemed daunting; the responses costly or uncertain. Yet so far, despite such challenges, we have always been equal to dealing with every advance.

So it must prove this time as we strengthen and adapt NATO’s power of deterrence – our priceless asset – to meet the challenge of the cyber age.

#### [OPTIONAL] Global democratic crisis increases hostility---only countering autocratic power projection can solve.

Larry Diamond 17. Senior Fellow at the Hoover Institution, Stanford University. He coordinates the democracy program of the Center on Democracy, Development, and the Rule of Law (CDDRL) within the Freeman Spogli Institute for International Studies (FSI). "How to Reverse the Degradation of Our Politics". American Interest. https://www.the-american-interest.com/2017/11/10/reverse-degradation-politics/

The world is facing a gathering crisis of liberal democracy. As I argued here last month, freedom and democracy have been retreating in many countries, including in Europe. Authoritarian regimes like Russia and China are pushing anti-democratic values with increasing energy, resourcefulness, and determination. If they succeed, the world will be a very different place—and for the United States, a more hostile one.

The United States and its liberal democratic allies must develop a new global strategy to counter the power projection of expansive autocracies, and to reboot an international campaign to promote democratic values and ideas. But we also need to renew the core of what we are fighting for: the worth of our own democracy.

#### Immediate US proposal of unambiguous cyber-Article 5 response is key---alternatives destroy deterrence and NATO leadership.

Stephen Jackson 16. Juris doctor degree from George Mason University School of Law and is currently a Research Associate at the Center for Infrastructure and Protection at the George Mason University School of Business. "NATO Article 5 and Cyber Warfare: NATO's Ambiguous and Outdated Procedure for Determining When Cyber Aggression Qualifies as an Armed Attack". Center for Infrastructure Protection & Homeland Security. 8-16-2016. https://cip.gmu.edu/2016/08/16/nato-article-5-cyber-warfare-natos-ambiguous-outdated-procedure-determining-cyber-aggression-qualifies-armed-attack/

At the outset of the North Atlantic Treaty Organization’s (NATO) founding, the original 12 Western nations included Article 5 within the Washington Treaty, which codified the concept of collective self-defense, first featured in the Charter of the United Nations of 1945.[1] NATO Article 5 provides that “an armed attack against one or more of [the NATO allies] in Europe or North America shall be considered an attack against them all….”[2] In the event of an armed attack against a NATO Party, “each of them, in exercise of the right of individual or collective self-defence recognized by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith . . . such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.”[3] Although only formally invoked once,[4] Article 5 is the main pillar of NATO, and serves as a deterrent against hostilities by non-NATO nations and non-state actors.

Since NATO’s creation in 1949, the manner in which nations engage in warfare has changed dramatically. This evolution includes incorporation of cyberspace into conducting warfare and securing national defense. For instance, Deputy Assistant Secretary of Defense Aaron Hughes recently testified before the Congress that “[the Department of Defense] relies heavily on cyberspace for virtually everything we do.”[5] Possibly the most blatant use of cyberspace in modern warfare occurred on December 23, 2015, when the Ukrainian power grid experienced major disruption from a sophisticated external cyber attack, largely rumored to be linked to the Russian Federation’s hostile occupation and annexation of Crimea.[6]

In an expression of NATO’s current abilities to counter advanced armed attacks, the Heads of State and Government of the North Atlantic Council issued the Wales Summit Declaration (Wales Declaration) on September 5, 2014. In the Wales Declaration, the Heads of State and Government outlined the threat of cyber threats and attacks, reaffirming NATO’s policy of “prevention, detection, resilience, recovery, and defence.”[7] The Wales Declaration further stated that the norms of international law, which include humanitarian law (jus in bello) and the UN Charter, directly apply to the realm of cyberspace.[8] At the core of these international norms is the concept of collective self-defense incorporated in NATO Article 5 and UN Charter Article 51. The Wales Declaration concluded by providing that NATO Article 5 in fact applies to cyber attacks, as determined by the North Atlantic Council on a “case-by-case basis.” Less than a year later, NATO Secretary General Jens Stoltenberg reiterated that a cyber attack could amount to an armed attack and trigger Article 5’s collective defense provisions.[9]

Although NATO has declared Article 5’s application to certain cyber attacks, the manner in which the North Atlantic Council will assess each cyber attack remains ambiguous. The lack of predetermined standards for assessing cyber attacks poses issues for NATO countries, which all hold various and differing internal criteria for countering cyber attacks. To remove this ambiguity, NATO should strive toward adopting a uniform standard for assessing individual cyber attacks to determine whether each attack rises to the level of an armed attack. Without adopting these measures, the North Atlantic Council will likely face internal strife among member nations while simultaneously facing external pressures during a major cyber event.

NATO Article 5: An Outdated Tool in the Age of Cyber Aggression

As with any international treaty, the Washington Treaty is a product of its historical and technological context. Directly after World War II and at the dawn of the Soviet Union, the NATO allies sought to counter Soviet aggression in the Euro-American region. After the Soviet Union disbanded, NATO began preventing non-state actors from infiltrating NATO territories while also expanding its operations to regions like the Middle East.[10] Although NATO continues to use the express language of Article 5 to govern all forms of armed attacks, cyber attacks pose a new and unique obstacle. Cyber attacks are different than traditional methods of warfare because while they often have devastating consequences for the targeted nation or private entity, they rarely result in physical events like the cyber event in Ukraine.

Secretary General Stoltenberg’s announcement regarding the application of international law to cyberspace signifies that the doctrine of jus in bello, which regulates the proper conduct for waging war, also governs how nation states use cyber attacks. Traditional principles of jus in bello include the rules of proportionality and distinction, which dictate how a nation targets oppositional force while avoiding unnecessary civilian casualties.[11] If NATO seeks to enforce the application of international law to cyberspace, the North Atlantic Council will face much difficulty in using Article 5 to define when a cyber attack reaches the threshold of an armed attack based on these doctrines.

Article 5 is useful for assessing state and non-state actions used in traditional warfare. However, the NATO allies drafted Article 5 in light of the technology and tactics of the World War II era. While NATO continued to successfully adapt Article 5 to the evolving challenges post-Soviet Union, it cannot properly invoke the principle of collective self-defense against cyber attacks without at least new definitions for the various forms of cyber events. In particular, without unambiguous guidelines for identifying from where a cyber attack originated, NATO will face difficulty in both locating the origin of a cyber attack and determining whether the cyber attack was sanctioned by the host nation. Also, without proper definitions for the various forms of cyber attacks, NATO will likely encounter unnecessary debate between NATO allies over any cyber attack against a NATO country. Furthermore, without removing ambiguity in identifying cyber events that equate to a traditional armed attack, the North Atlantic Council will face difficulty in deciding upon a proper and proportionate armed response in accord with the principles of jus in bello.

Currently, almost every NATO ally has an individual national security and defense strategy related to cybersecurity.[12] These strategies vary in detail and scope, and lack uniformity in defining the elements of which cyber attacks warrant an aggressive response. Some scholars argue that the International Court of Justice accurately determined that collective self-defense is triggered when an act “inflicts substantial destruction upon important elements of the target state,” even if the attackers used non-traditional weaponry like airplanes or cyber attacks.[13] For instance, this “scale and effects” test does not adequately address the technical differences between using cyberspace to create either a kinetic disruption to a power plant or the potential to dismantle an entire financial infrastructure with zero physical effects. The potential for a single cyber attack to result in major disturbance, with or without any physical element, is sufficient to warrant specific guidelines. However, as long as the North Atlantic Council assesses individual cyber attacks on a case-by-case basis without predetermined specialized rules, the various interests of all 28 NATO nations will pose obstacles for a swift and efficient NATO response.

The Adoption of Cyber Attack Guidelines to Supplement Article 5

To properly dissuade and combat future cyber attacks, NATO should adopt cyber attack guidelines to reduce ambiguity and address the uniqueness of cyber aggression. In doing so, NATO will afford all member nations a unified procedure in which the North Atlantic Council may examine cyber attacks. This does not necessarily mean that bright line rules should be adopted. According to Department of State Coordinator for Cyber Issues M.E. Painter, “[a]s a general matter, states have not sought to define precisely (or state conclusively) what situations would constitute armed attacks in other domains, and there is no reason cyberspace should be different.”[14] Instead, Coordinator Painter argues that nations like the United States should define specific “norms of responsible behavior” for cyberspace that embrace traditional international law while adapting them to the intricacies of cyberspace.[15]

While Coordinator Painter speaks on behalf of the United States Government, his ideas of broad norms created specifically for regulating cyberspace is an important concept that NATO must at least consider for a framework dictating proper identification of cyber attacks, understanding whether a cyber attack rises to an armed attack under Article 5, and what are the proportional responses to such attacks. The United Nations has already embraced this line of thinking by issuing its annual Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE Report). The most recent UN GGE Report included several U.S. recommendations for how nations should and should not utilize information and communications technologies.[16]

Following the United Nations’ example, NATO should also form cyber attack guidelines that illustrate a set of norms related to cyberspace, but focus solely on cyber attacks, Article 5, and jus in bello. NATO can form the first coherent set of international guidelines for cyber attacks,[17] which is vital for maintaining dominance in the international sphere. NATO should begin its formation of the guidelines by analyzing the Tallinn Manual on the International Law Applicable to Cyber Warfare (Tallinn Manual). Issued in 2013 for the benefit of NATO, experts in international law comprised “black letter” rules incorporating traditional jus in bello principles to cyber warfare.[18] Although the Tallinn Manual is not binding legal authority, it offers international organizations the best attempt at combining international law with the new realm of cyberspace. In consulting the Tallinn Manual, NATO should begin to draft binding authority for the North Atlantic Council in the form of an amendment to the Washington Treaty, or at least a persuasive document codified within NATO’s Military Committee or Allied Command Operations. By codifying principles similar to those included in the Tallinn Manual, NATO would drastically reduce the ambiguity surrounding the current case-by-case analysis identified in the Wales Declaration.

The formation of binding cyber attack guidelines for all NATO members and the North Atlantic Council will not be an easy task. As stated earlier, each NATO nation has independently formed its own set of standards for combating cyber aggression. Individualization among members will assuredly create friction in drafting these guidelines. However, NATO would be wise to begin the process before these individualized standards become too offensive for a uniform NATO procedure.

Conclusion

The evolution of modern warfare shows that as weaponry becomes more advanced, nations attempt to curtail their devastating effects. To this point, international treaties and protocols, like the Geneva Protocol prohibiting asphyxiating and poisonous gases in battle,[19] tend to follow atrocities on the battlefield. Though only in the early stages of use for military purposes, cyberspace offers a unique opportunity to break the trend of following devastating events. By adopting a set standard before a major cyber attack is used against a NATO member, NATO may curtail these potential attacks by offering non-NATO members a clear set of rules. These rules may serve as a deterrent for these cyber attacks while simultaneously limiting the time in which NATO may effectively and proportionately respond.

#### [OPTIONAL] Unclear cyber policy is the death nail for NATO’s collective defense---only the plan can solve.

Steffen Westerburger 15. Graduate of the University of Nijmegen in The Netherlands; Majored in International Relations. "Rethinking NATO Article 5: Challenges to Collective Security in the Cyber Era". American Security Project. https://www.americansecurityproject.org/rethinking-nato-article-5-challenges-to-collective-security-in-the-cyber-era/

First, the Alliance should consider reformulating Article 5 of the Treaty. Currently the article only speaks of ‘an armed attack’ against one or more of the members. Cyber-attacks do not necessarily ‘fit the picture’ of conventional, armed attacks. Therefore the definition should be changed. Collective self-defense mainly functions as a deterrent against potential adversaries. To maximize the impact of the deterrent, its underlying doctrine should leave no room for guessing. It should specifically include cyber-attacks.

Second, the Alliance should come up with a clear doctrine on what constitutes an attack that would qualify the invocation of Article 5, and what would be an accepted retaliatory action. Although this is important concerning conventional attacks as well, it becomes even more pressing for cyber-attacks. Everyone understands it is unacceptable to bomb a country as a reaction to petty cybercrime, but what if an actor succeeds in shutting down important parts of the economy of a country – for example the New York Stock Exchange? An option could be to openly formulate clear redlines to maximize the deterrent. Some however say that a dose of strategic ambiguity is more important, arguing that formulating clear redlines would invite potential adversaries to push up to the red line. In this case developing the doctrine is still important, but would then be for internal use only.

Third, the Alliance should further focus on information sharing and mutual assistance concerning the cyber domain. Putting cyber on top of the agenda will give a clear signal to all NATO members, especially those who are lagging behind. It is time to not only invest in our conventional capabilities; we have to start improving our cyber capabilities as well.

cyber threat

Whereas Article 5 mainly relies on deterring potential adversaries, it is important to understand the notion of deterrence in the cyber field. In the conventional field, deterrence is pretty straightforward: you just count the numbers of soldiers, rockets, tanks, fighter jets etc. In the cyber field this is more difficult; how do you actively show what you are capable of, without giving away strengths and weaknesses? That is why the three aforementioned steps are important: it makes clear NATO takes cyber threats seriously and will not hesitate to act.

Only when the Alliance collectively pursues an active cyber policy, they will be able to successfully prepare themselves for cyber threats to their national security. The idea of collective self-defense will only survive as long as it proves to be successful in defending its members against all possible threats. Cyber-attacks will be among the biggest challenges of the next decades. Let us make sure we are prepared.

#### NATO credibility solves global existential conflict---only allied coordination can prevent emerging threats.

Netherlands Ministry of Foreign Affairs 3/21/22. "What does NATO do? Foreign Affairs in plain language". https://www.government.nl/latest/news/2022/03/21/what-does-nato-do-netherlands-safety

Safety and security in the Netherlands

A safer world also means a safer Netherlands. Why? Take for instance terrorism, nuclear weapons or cyberattacks. These threats have one thing in common: they don’t stop at borders.

So our own safety and security often starts abroad. That’s why it’s important to have good relations with other countries. And to protect stability in the world together. The Ministry of Foreign Affairs works hard to do this. NATO also plays an important role. But what exactly is NATO?

What is NATO?

NATO stands for ‘North Atlantic Treaty Organization’. It is a military alliance of 30 countries in Europe and North America. Its headquarters is in Brussels. The Netherlands is a member of NATO. NATO was set up in 1949, not long after the end of the Second World War. Its aim: to protect the security and freedom of all the countries that are members (the Allies). And right now, that Alliance is perhaps more important than ever.

Worldwide security challenges

The world is a less safe place than before. Even in areas near the Netherlands. Take for instance the war in Ukraine started by President Putin. Or China: a growing global economic and military power that is flexing its muscles more and more often. Technological developments also lead to new threats, like cyberattacks. Or the use of modern weapons, like drones, that can attack targets without humans having to risk their lives.

And climate change can also lead to more conflicts, or make conflicts worse. Countries need each other so they can prevent and combat these global threats.

NATO and diplomacy

NATO is a defensive military alliance. You might think NATO is all about military action. But there is another very important step that comes first. NATO’s main priority is diplomacy. By talking to each other and with other countries, we try to solve conflicts without using force.

Within NATO, the Allies work together and make agreements. For instance on protecting democratic values. Examples are: being able to hold free and fair elections, equal rights for everyone, and freedom of expression.

Within NATO, military and non-military experts meet to exchange information about what is happening in the world. In this way, NATO prepares itself for the challenges and threats of today and of the future. With military and diplomatic action.

NATO in the world

NATO also helps other countries – that aren’t members of NATO – with their security. For instance by helping them train their soldiers. NATO soldiers can also be sent to deal with a crisis. This is important for the Netherlands too. Because the world is becoming more and more closely connected. And our safety and security is also connected to that of other countries.

### Plan---1AC

#### Thus, the plan---

#### The United States federal government should increase its security commitment under Article 5 of the North Atlantic Treaty to include responding to cybersecurity threats, including information warfare.

### Solvency---1AC

#### Solvency---

#### Only the clear policy solves deterrence and global credibility---the US NATO commitment is the largest signal.

Brian Frydenborg 9/24/21. MS in Peace Operations from George Mason University's School of Public. BA from Washington and Lee University in Politics and History. Former intern in the United States Senate. "NATO Is in a Cyberwar with Russia and Must Expand Article 5 to Include Cyberwarfare or Risk Losing and Diminishment". Small Wars Journal. 9-24-2021. https://smallwarsjournal.com/jrnl/art/nato-cyberwar-russia-and-must-expand-article-5-include-cyberwarfare-or-risk-losing-and

Introduction

Article 5 of NATO’s foundational 1949 North Atlantic Treaty demands that if an “armed attack” is carried out against even just one member state, all other member states “shall” consider that attack (and any armed attack) on a member state “an attack against them all” and “will assist,” up to and “including the use of armed force.” This bedrock is the centerpiece for over seven decades of the Pax Americana: the U.S.-led global system of military power, alliances, collective defense, and ability to project combined strength anywhere on the planet. For it to continue in these roles, NATO must adapt to current and future threats by adding cyberwarfare—including information warfare—to Article 5.

Cyberwarfare a Defining Part of Modern Warfare

Most cyberattacks against NATO states are carried out by Russia. A key element of these involve what is called “information warfare” (“a new face of war,” quoting a RAND Corporation report), heavily involving disinformation and that includes “warfare” to indicate these are hardly benign/normal influence operations but those that have always been part of any serious conventional war in modern times.

The ever-evolving concept of warfare in our digital age, then, does not have to include shots being fired from guns, and it is naïve to not consider cyberwarfare as simply another form of war in the twenty-first century that uses force in the digital realm to achieve results in some of the same spirit as traditional armies: attack, defense, deception, sabotage, destruction, and to pressure actors to change behavior. Clausewitz most famously wrote that “war is merely the continuation of policy [or politics] by other means” and would have well understood cyberwarfare to be war and well within that “other means” category.

Russia and China are the two countries that have led in cyberwarfare. Bolder but weaker Russia is NATO’s—and America’s—foremost enemy (even if unofficially but obviously in a de facto sense), while China is stronger but more reserved as the West’s clearest top rival. China has carried out and been a leader in non-weaponized hacking and espionage (admittedly common among all major states), but has not, say, publicly released disinformation or stolen information in a manner timed to seriously interfere with NATO countries’ elections (as Russia has). And though China has its own complex influence operations, Russia undoubtedly has led by far in cyberattacks more hostile than espionage (uniquely so among major powers) since its game-changing 2007 Estonia cybercampaign.

[Figure Omitted]

Figure 1. Where the political warfare fits within the implements of power. “All activities are illustrative, rather than an exhaustive list of possible actors.” From RAND's The Growing Need to Focus on Modern Political Warfare

Russia officially considers NATO a “threat,” and since that 2007 Estonia cybercampaign, has been far more aggressive and threatening towards NATO states, often stoking internal divisions and flooding them in cyberattacks, including election interference and boosting secessionism, with notable cybercampaigns being carried out against over twenty NATO member states (apart from campaigns against non-NATO states).

Furthermore, de facto, undeclared wars are the most common type of war in modern history even if the term “war” is not used. America, for example, has a long history of undeclared war going all the way back to the nation’s earliest days involving conflict with Native Americans and also the 1798-1800 Quasi-War, then popularly termed “The Undeclared War with France.” As one scholar notes, “the legal state of war is possible without actual fighting.”

The Nature of Russian Cyberwarfare Confronting NATO

Thus, it is hardly extreme to consider NATO and Russia in an undeclared cyberwar and, therefore, a state of undeclared war. NATO Review, NATO’s flagship journal, even in 2017 published analysis noting that Russia was waging “non-kinetic political war on the West,” as I have also maintained.

Russia’s weapons in its undeclared war on NATO are not tanks, bombs, bullets, or jets; rather, they are illicit financing, trolls, bots, and fake news, with the Kremlin often fomenting, funding, and promoting the rise of far-right ethno-nationalist extremists, all while disparaging those in the center and mainstream left. Putin’s party, the banally nationalist United Russia, has even formed formal and informal alliances with significant like-minded political parties in major NATO countries.

These campaigns, relying on hacking, disinformation, propaganda, and other cyber-methods, are coordinated through major components of the Russian government and close Putin allies in and out of the Kremlin, often using thousands of fake accounts to artificially boost their impact, which, in turn, are bolstered within the target states by agents and local allies along with unwitting true believers long dubbed “useful idiots.” In many NATO countries—including the U.S.—Putin is even liked by far-rightists. Domestic media, then, can become loud voices augmenting Russia’s propaganda, especially right-wing media outlets, but also some on the far-left. Repeated enough, top traditional outlets latch onto this disinformation, sometimes mainstreaming it, other times critiquing yet still propagating, as I have previously explained.

Reigning as the supreme disruptor on social media, Russia spews a “firehose of falsehoods” that has been massively effective, distorting and gaslighting public discussion to wildly amplify Russia’s preferred narratives beyond any natural organic reach, influencing many millions, thus helping to create an atmosphere where disinformation is sometimes consumed even more than actual news and doubt about even basic truths becomes widespread.

And once Putin’s favored are in office partly because of Russian disinformation, they in turn further spread Russian disinformation from the highest levels of their governments, even mimicking Kremlin tactics and adopting policies favorable to Russia, even covering up Russia’s trail (both America’s 2019 Mueller report and the British Parliament’s Intelligence & Security Committee’s exceptional Russia report released last year note damning examples of obstruction in their respective governments).

Most notably for NATO, the American presidential candidate Putin twice ordered Russian election interference on behalf of had expressed hostility to NATO repeatedly during the campaign, even contemplated leaving the Alliance as president, and may still have done so if reelected.

Cyberwarfare a Larger Threat Now to NATO than Terrorism

By far, the most damaging, destabilizing, and effective attacks NATO countries since 9/11 have been Russian cyberattacks, campaigns that have been able to affect political outcomes and internal dynamics in numerous NATO countries to suit Putin’s agenda.

Russian cyberwarfare efforts against the U.S. have included election interference—beginning with what I called back in December 2016 the First Russo-American Cyberwar—that has already caused damage to America, its democracy, and its reputation that is hard to exaggerate, with effects not only still being felt by the U.S. but guaranteed to still be felt for some time. Russia is also clearly and repeatedly promoting unrest and division, recently pushing both disinformation about the coronavirus and bogus conspiracy theories of fraud 2020 U.S. presidential election. In the run-up to that election, the Russians targeted the main political rival of their preferred incumbent, just as in 2016.

These efforts produced results: multiple respectable surveys and any casual look at social media show that vast numbers of Americans—even key leaders—are supporting this disinformation, even spreading nonsense about both the 2020 presidential election, damaging faith in the very foundations of democracy coronavirus (including millions doubting coronavirus vaccines, literally helping kill Americans). There are also global effects on opinion of America and the rest of the West along with international views on coronavirus and vaccines.

Most recently coming to light are the devastatingly far-reaching SolarWinds operation; a cyberattack against USAID that ensnared some 150 government agencies, non-profits, think tanks, and human rights groups globally that have criticized Russia; a recent attack on top U.S. cybersecurity firm FireEye; and the Colonial Pipeline and JBS meat plant ransomware attacks, with Russia playing a role with these ransomware groups similar to how the Taliban gave al-Qaeda safe harbor, resulting in the 9/11 attacks—incidentally, the only time NATO ever invoked Article 5.

In contrast, physical terrorist attacks in NATO countries since 9/11, while tragic, have still had comparatively limited effects. Even Russia’s own 2018 Novichok chemical weapon attack on British soil in Salisbury against Russian military intelligence officer turned spy for the UK Sergei Skripal had more symbolic an effect than anything else, dwarfed by the damage from Russian efforts to move the 2016 Brexit vote in the direction of Leave or the effect of Russia’s campaign to amplify Scottish secessionism (now increasingly likely and sooner rather than later, an outcome that would obviously dismember and damage a UK already acutely damaged by Brexit). To quote journalist George Packer, “antisocial media has us all in its grip.”

Falling Short

NATO currently has a Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia. Yet even presently, one-sixth of NATO— Albania, Canada, Iceland, Luxembourg, and North Macedonia—are not members of this Centre, though, encouragingly, Canada and Luxembourg are going to join, new states were recently added, and non-NATO states Austria, Finland, Sweden, and Switzerland are “Contributing Participants,” a status available to those outside of NATO; Australia, Ireland, Japan, South Korea, and—most recently—Ukraine will join that second group. There is also set to be a new military cyberdefense command center fully operational in 2023 at NATO’s military base in Belgium.

NATO considers “cyber defence…part of NATO’s core task of collective defence” and has since 2014, when the Alliance first specifically articulated the possibility of invoking Article 5 in reaction to cyberattacks (but only “on a case-by-case basis”). NATO has since “pledge[d] to ensure the Alliance keeps pace with the fast evolving cyber threat landscape and that our nations will be capable of defending themselves in cyberspace as in the air, on land and at sea,” repeatedly reiterating that Article 5 being invoked in response to a cyberattack is a possibility, including just this September 2020 and in June 2021.

Yet official working papers, conferences, interviews, statements, and raising possibilities are no substitute for a concrete, clear policy, and NATO simply does not have this.

The vague idea seems to be that if a cyberattack was “serious” enough, Article 5 could be activated, but this seems myopic: death by a thousand cuts is still death and has the same effect as decapitation, so tolerating many smaller attacks, thereby transmitting a clear indication that there will not be a collective Article 5 response to them, is just bad policy. It is also most decidedly not the case for armed attacks, in which any by a nation-state or sponsored by one would trigger Article 5. Years of unrelenting cyberwarfare has done more damage to NATO than any Soviet Army did during the Cold War, in part, because of Article 5: the USSR and then Russia did not dare use armed force to strike any NATO country for fear of Article 5’s unequivocal guarantee of a collective response, even in 2015 when NATO-member Turkey shot down a Russian military jet over Syria.

Yet when it comes to cyberwarfare, NATO is practically inviting Russia to attack and get away with it, with the Alliance quite consistently demonstrating an unwillingness, even inability under its existing framework to collectively respond to Russia’s cyberaggression. As the aforementioned UK Russia report noted, “Russia is not overly concerned about individual reprisal” against its aggressive acts, including its cyberattacks, with even the U.S. demonstrably inspiring little hesitation.

Clearly, pretending cyberwarfare is not war and allowing cyberwarfare in real-world practice to be kept out of NATO’s Article 5—leaving individual members states flailing independently and ineffectively against an organized, determined, and capable de facto enemy content to stand down its conventional military against NATO while unleashing its cyberunits upon it with impunity—has failed.

At the end of New York Times cybersecurity reporter Nicole Perlroth’s recent book This Is How They Tell Me the World Ends—the indispensable, terrifying, definitive account of the development of cyberwarfare and the mess in which we currently find ourselves—the author warns that “many will say” that “these…critical assignments of our time” to deter and defend ourselves from cyberwarfare “are impossible, but we have summoned the best of our scientific community, government, industry, and everyday people to overcome existential challenges before. Why can’t we do it again?…We don’t have to wait until the Big One to get going.”

As a main advantage of the West over Russia is that people like the West a lot more than Russia—materializing in close economic, diplomatic, and military ties Russia can only dream of—the easiest way for the West to face and fight this dire and metastasizing cyberthreat from Russia is by leveraging its alliances, and, most of all, this means involving NATO and doing so in a big way.

As there is no statute of limitations on cyberattacks and the just-proposed framework not precluded by the current NATO treaty, NATO would even be in its full rights (and is overdue) to now invoke Article 5 against Russia for its cyberwarfare so that this cyberwarfare will result in far more pain for Russia than any damage it inflicts.

How to Revise Article 5 and the NATO Treaty Overall

With Russia’s rampant cyberwarfare only intensifying and its obvious pattern as a hostile bad-faith actor, it is absolutely necessary for a paradigm shift in the international system for deterring cyberattacks. Because NATO is the premier Western defensive alliance, crystalizing cyberwarfare’s relationship to Article 5 is a must, the only way for NATO to maintain credible collective defense in the twenty-first century.

To this end, “or cyberattack” must be added after every occurrence of the words “armed attack” in Article 5 (e.g., “The Parties agree that an armed attack or cyberattack against one or more of them…”).

In a longform, earlier version of this proposal, I have proposed a new detailed Article 15 that defines cyberwarfare in the Article 5 context and who/what would be covered. Any attacks that cause damage and harm would be included, as would digital information warfare/disinformation campaigns. Yet fairly standard espionage operations will not be included (say, China’s hacking) unless either the scale is so exceptional (as was the case with Russia’s unprecedented SolarWinds hack) or if what is hacked is weaponized or threats to weaponize that information are made.

By “weaponized,” I mean any action that tries to coerce, influence, or target publicly. Targets that would trigger Article 5 include all NATO citizens, residents, or entities—public sector or private—or anyone operating on NATO member state territory, as NATO cannot tolerate its territory being used for any such attack. Any attacks targeting family, friends, or connections of these folks for the same purposes would also be covered. This would apply to all state or state-sponsored cyberattacks, while terrorist or non-state actors would also be covered under certain actions but other activities would default to being handled by normal counterterrorism and/or law enforcement agencies.

Conclusion

Expanding Article 5 is necessary and overdue. The early twenty-first century’s second decade has been something of a Wild West, with Russia using the lawlessness of the cyber domain to its devastating effect. The time for lawlessness is over, and revising NATO’s Article 5 as suggested herein will not only clarify the rules for NATO enemies and rivals, but also for the members of a NATO Alliance itself that is in desperate need of clarity and strength on this issue. It will also make NATO once again an alliance that instills fear in the minds of Russian leaders (as it did with Stalin and subsequent Soviet leadership) who would engage in reckless acts of aggression against NATO or its states, even if “just” through cyberwarfare.

#### The plan is key to NATO credibility and defense---the alliance must adapt to the changing mode of war.

Brian E. Frydenborg 6/7/21. MS in Peace Operations from George Mason University's School of Public. BA from Washington and Lee University in Politics and History. Former intern in the United States Senate. "Already in a Cyberwar with Russia, NATO Must Expand Article 5 to Include Cyberwarfare". Real Context News (RCN). 6-7-2021. https://realcontextnews.com/already-in-a-cyberwar-with-russia-nato-must-expand-article-5-to-include-cyberwarfare/

SILVER SPRING—Alliances between nations must adapt to retain power over time, and in no area has warfare evolved more in recent years than in cyberwarfare. Article 5 of NATO’s founding 1949 North Atlantic Treaty mandates that if an “armed attack” is carried out against a member state, all member states (currently thirty, including the most powerful Western nations) “shall” consider that attack and any armed attack on even just one member state “an attack against them all” and “will assist” it, up to and “including the use of armed force.” As the centerpiece for over seventy years of the West’s Pax Americana, global military power, system of alliances and collective defense, and ability to project combined strength anywhere on the planet, NATO must adapt to the present by adding cyberwarfare—including information warfare—to Article 5.

Cyberwarfare As Modern Warfare

An obvious point in favor of including cyberwarfare in Article 5 is that, by far, the most effective, damaging, and destabilizing attacks against NATO countries since 9/11 have been cyberattacks, most carried out by Russia. The term “information warfare” (“a new face of war,” quoting a RAND Corporation report) refers to a key element of this cyberwarfare and includes the word warfare to indicate these are hardly benign, normal influence operations and are, indeed, the types of operations that have always been part of any serious conventional war in modern times. Even in the nineteenth-century, von Clausewitz wrote that “War is…an act of force to compel our enemy to do our will.”

The ever-evolving concept of warfare in our digital age, then, does not have to include shots being fired from guns, and it is naïve to not consider cyberwarfare as simply another form of war in the twenty-first century that uses force in the digital realm to achieve results in some of the same spirit as traditional armies: attack, defense, deception, sabotage, destruction, and to pressure actors to change behavior. Clausewitz most famously wrote that “war is merely the continuation of policy [or politics] by other means” and would have well understood cyberwarfare (sometimes just termed cyberwar) to be war and well within that “other means” category.

The two countries that have led in cyberwarfare are Russia and China, the first (and weaker, but bolder) being NATO’s (and America’s) clearest top state enemy (even if unofficially but clearly in a de facto sense), the second (and stronger, more reserved) being America’s clearest top state rival in a holistic sense, as China has engaged and led in much non-weaponized hacking and espionage (admittedly common among major powers), but has not, say, brazenly released stolen information or disinformation in a way timed to significantly interfere with NATO member states’ elections (as Russia has). And though China has its own sophisticated influence operations, Russia undisputedly has led by far in acts more hostile than espionage (uniquely so among major powers) since its watershed 2007 Estonia cybercampaign (such campaigns might better be termed cyberassaults than cyberattacks, the latter a broader, far more common term which can even apply to a single high school student’s cyberattacks against his own school district).

Russia officially views NATO as a “threat,” and since that 2007 Estonia cybercampaign, has become far more aggressive and threatening towards NATO, often playing with internal NATO nationalisms and blanketing NATO nations in cyberattacks, including election interference and bolstering of secessionist campaigns, with notable cybercampaigns being carried out against over twenty NATO member states (leaving aside its campaigns waged against non-NATO states).

[FIGURE OMITTED]

Furthermore, de facto, non-declared wars are the most common type of war in the modern era even if the term “war” is not specifically used. America, for example, has a long history of undeclared war going all the way back to the Articles of Confederation and the early days of the Washington Administration involving conflict with Native Americans and also the John Adams Administration’s 1798-1800 Quasi-War, then popularly termed “The Undeclared War with France.” Furthermore, as one scholar notes, “the legal state of war is possible without actual fighting.”

Taking all this into account, then, it is hardly unreasonable to consider Russia and NATO in a state of undeclared cyberwarfare and, therefore, a state of undeclared war. One of NATO’s flagship publications, NATO Review, even published analysis in 2017 acknowledging that Russia was waging “non-kinetic political war on the West.”

In fact, as I have argued for some time, a truly deep look would expose Putin and his Kremlin conducting a clear de facto war to destroy NATO, the West, the EU, and Western democracy; to fracture trans-Atlantic and European unity and even the unity of individual Western nations; and to foment, fund, and favor the rise of far-right ethno-nationalists and secessionists friendly to Russia and hostile to the U.S. and NATO in NATO countries and elsewhere, all while savaging those in the center and mainstream left not preferred by Putin. The parties Putin helps usually have much in common with Russian President Vladimir Putin’s banally nationalist United Russia party, which has struck up mixes of formal and informal alliances with several significant European political parties in major NATO states.

Though there have been military moves by Russia in Ukraine and Georgia—two NATO aspirants—the main weapons in its undeclared war on NATO are not tanks, bombs, or jets; rather, they are bots, trolls, and fake news.

#### Certainty and severity are key---lack of threshold invites Russian cyberwar and erodes Article 5.

Brian E. Frydenborg 6/7/21. MS in Peace Operations from George Mason University's School of Public. BA from Washington and Lee University in Politics and History. Former intern in the United States Senate. "Already in a Cyberwar with Russia, NATO Must Expand Article 5 to Include Cyberwarfare". Real Context News (RCN). 6-7-2021. https://realcontextnews.com/already-in-a-cyberwar-with-russia-nato-must-expand-article-5-to-include-cyberwarfare/

Falling Short

Official working papers, conferences, interviews, statements, and raising possibilities on the subject are one thing, but a concrete, clear policy is another, and NATO has nothing of the sort.

The vague idea seems to be that if a cyberattack was “serious” enough, Article 5 would be invoked, but there is no definition of what this threshold would be, and, frankly, this idea seems rather myopic: death by a thousand cuts is still death and has the same effect as decapitation, so tolerating many smaller attacks and sending a clear signal that there will not be a collective Article 5 response to them is simply bad policy.

Consider, too, that Russia would never be able to get away with flying over NATO skies and dropping leaflets of hostile disinformation by the millions onto NATO populations. It could never get away with doing so once or once in a while, let alone consistently and during sensitive times of pivotal political decisions or unrest in the targeted countries, and yet this is exactly the cyber-equivalent of what Russia is getting away with against NATO’s most significant member states and many of its smaller ones, too. And while Russia sending in Spetsnaz special forces to steal sensitive information from U.S. bases in Alaska or use physical weapons to sabotage or destroy government computer systems in Lithuania would be viewed automatically as an Article 5-triggering act of war, the same results over and over again from several years of unrelenting cyberwarfare are not, even though this has done more damage to NATO than any Soviet Army did throughout the decades-long Cold War. This is, in part, because of NATO: the USSR and then Russia did not dare use armed force to attack any NATO state for fear of that explicitly guaranteed Article 5 collective response (even when NATO-member Turkey shot down a Russian military jet over Syria in 2015).

Yet when it comes to cyberwarfare, NATO is practically inviting Russia to attack and get away with it, with the Alliance quite consistently demonstrating its inability and unwillingness under its current framework to respond collectively to Russian cyberaggression. As noted in the aforementioned UK Russia report, “Russia is not overly concerned about individual reprisal” against its aggressive acts, most certainly including its cyberattacks, with even the U.S. clearly inspiring no fear.

Language can often be tricky, and terms like “war” should never be thrown about lightly. But with the advent of the internet and the realities of the modern world, NATO cannot become complacent with preventing traditional warfare while failing to adapt to cyberwarfare. Pretending cyberwarfare is not war and allowing cyberwarfare in real-world practice to be kept out of NATO’s Article 5—leaving individual members states flailing independently and ineffectively against a determined, capable, and organized de facto enemy content to stand down its conventional forces against NATO while unleashing its cyberunits upon it with impunity—has not discouraged Russian cyberwarfare against NATO, it has encouraged it. Article 5 makes no exception for smaller armed attacks, and any serious collective cybersecurity defense should make no exception for smaller cyberattacks.

#### The US must act through Article 5---its key to credibility.

Brian E. Frydenborg 6/7/21. MS in Peace Operations from George Mason University's School of Public. BA from Washington and Lee University in Politics and History. Former intern in the United States Senate. "Already in a Cyberwar with Russia, NATO Must Expand Article 5 to Include Cyberwarfare". Real Context News (RCN). 6-7-2021. https://realcontextnews.com/already-in-a-cyberwar-with-russia-nato-must-expand-article-5-to-include-cyberwarfare/

How to Revise Article 5 and the NATO Treaty Overall

Considering that the West’s main advantage over Russia is that people like the West a lot more than Russia—manifesting itself in close diplomatic, military, and economic ties about which Russia can only fantasize—the easiest way for the West to face and counter this dire and worsening cyberthreat from Russia is by leveraging its alliances, and, more than anything else, this means involving NATO and involving it in a big way.

U.S. President Joe Biden himself penned a recent Washington Post op-ed in advance of his upcoming trip to Europe for a NATO summit and to confront Putin face-to-face, writing: “In Brussels, at the NATO summit, I will affirm the United States’ unwavering commitment to Article 5 and to ensuring our alliance is strong in the face of every challenge, including threats like cyberattacks on our critical infrastructure.”

He can do that by proposing to strengthen Article 5 itself.

With Russia’s rampant cyberwarfare only intensifying and its clear pattern as a bad-faith hostile actor, a paradigm shift in the international system for deterring cyberattacks is absolutely necessary. Since NATO is the premier defensive alliance of the West, formalizing cyberwarfare’s relationship to Article 5 is a necessary leap forward on this much-needed path and the only way forward for NATO to maintain credible collective defense as the twenty-first century progresses.

To this end, “or cyberattack” must be added after each instance of the words “armed attack” in Article 5 (e.g., “The Parties agree that an armed attack or cyberattack against one or more of them…” [emphasis added]).

#### [OPTIONAL] Revising Article 5 solves---changes Russia from offensive to defensive.

Brian E. Frydenborg 6/7/21. MS in Peace Operations from George Mason University's School of Public. BA from Washington and Lee University in Politics and History. Former intern in the United States Senate. "Already in a Cyberwar with Russia, NATO Must Expand Article 5 to Include Cyberwarfare". Real Context News (RCN). 6-7-2021. https://realcontextnews.com/already-in-a-cyberwar-with-russia-nato-must-expand-article-5-to-include-cyberwarfare/

Conclusion: Expanding Article 5 Is Necessary and Overdue

The early twenty-first century’s second decade has been something of a Wild West, with Russia emerging as the biggest beneficiary in terms of cyberwarfare as defined above. While China has also benefitted in terms of massive espionage and acquisition of Western intellectual property, it is Russia that has used the lawlessness of the cyber domain from a collective security standpoint to engage in the most egregious acts (most recently and most notably with the unprecedented SolarWinds) and ransomware attacks), acts that could easily be defined as hostile acts of war.

The time for lawlessness is over, and, with no statute of limitations on cyberattacks and the just-proposed framework not precluded by the current NATO treaty, NATO would be in its full rights (and is overdue) to invoke Article 5 against Russia now for its cyberwarfare so that Russia’s cyberwarfare will cause Russia far more pain than any damage it inflicts.

This has not been the case, but it must be.

Revising NATO’s Article 5 as suggested herein (leaving aside invocation) will not only clarify the rules for NATO enemies and rivals, but also for the members of a NATO Alliance itself that is in desperate need of clarity and strength on this issue. It will also make NATO once again an alliance that instills fear in the minds of Russian leaders (as it did with Stalin and subsequent Soviet leadership) who would engage in reckless acts of aggression against NATO or its states, even if “just” through cyberwarfare.

Member states recognizing that they are in a state of war—cyberwar, but still war—with Russia and unambiguously making cyberwarfare a key plank of the Alliance’s main collective defense mechanism is essential, then, to keeping NATO the force for deterring aggression it has been for many decades.

Projecting such strength, both on paper and in practice, will serve as a real-world check against further Russian cyberattacks when inaction and lack of clarity has not, enhancing the security of every NATO member state and perhaps even eventually forcing Russia to a point where productive engagement, not adventuristic brinksmanship, is its chosen priority.

## Case---Arguments

### AT: Attribution---2AC

#### NATO cooperation makes attribution possible.

Siim Alatalu 18. Member of NATO Cooperative Cyber Defence Centre of Excellence’s Strategy Branch, where he is in charge of cyber strategy and policy research and training related to NATO and the EU, as well as providing subject matter expertise to the Centre’s other flagship projects. Prior professional career includes several advisory and managerial positions at the Estonian Ministry of Defence since 2001. “NATO’s responses to Cyberattacks.” https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP\_148.pdf

Thirdly, NATO’s particular advantage in cyber defence could stem from cooperation with its partner countries and with other international organisations, especially the European Union. Neither the Alliance nor the Union is an island on its own when it comes to cyber threats and vulnerabilities. The EU can do a lot in areas that are relevant for NATO, such as cybersecurity certification of devices imported into and used in European markets. Dependence on non-EU and non-NATO software could become a critical national security concern, as illustrated by for instance the Kaspersky case in the US.24 As highlighted by the recent attributions, there could be a global will for cooperation between NATO and non-NATO countries as any of them could become a target, as well as a bridgehead for further spreads of malicious cyber activities, as demonstrated by the WannaCry and NotPetya attacks.

#### Attribution is possible---new tech and cooperation solve

Susan Davis 19. United States, General Rapporteur. Science and Technology Committee (STC). NATO in the Cyber Age: Strengthening Security & Defence, Stabilising Deterrence. . 148 STC 19 E rev. 1 fin. https://www.nato-pa.int/download-file?filename=/sites/default/files/2019-10/REPORT%20148%20STC%2019%20E%20rev.%201%20fin%20%20-%20NATO%20IN%20THE%20CYBER%20AGE.pdf

15. However, in recent years, governments, private companies, and research organisations have increased their ability to attribute attacks at higher levels of confidence. Forensic tools have improved, and private and state analysts have built up databases and characteristic patterns for known intruders. On a technical level, truly harmful cyber attacks are very complicated and involve many moving pieces. Thus, the more complicated the cyber attack, the more likely the attacker is to commit mistakes along the way, enabling a forensics expert to trace the origin of the attack (Lindsay, 2015). Indeed, governments within the Alliance and beyond are increasingly attributing malicious cyber incidents to states and their proxies. Such transparency on cyber incidents is increasingly collective, coordinated in policy and time, and independent of the scale, nature, or impact of the incident (Giles and Hartmann, 2019). The Rapporteur supports this emerging policy of naming and shaming perpetrators and encourages further conversations at the NATO level.

16. Even if states and their proxies could be confident they will remain anonymous, truly convincing strategic rationales for large-scale surprise attacks are lacking. Anonymous cyber attacks are not well-suited for coercion, for example. Coercion only works if the attacked entity knows whom to yield or make concessions to. As one analyst points out succinctly, “[p]urely anonymous coercion is almost impossible because communicating and understanding the power to hurt implies that there is someone doing the hurting and a target concerned about avoiding getting hurt” (Lindsay, 2015). As a result, if an opponent wishes to coerce through cyber attacks, he cannot hide himself. This would defeat the purpose. How can the victim give in to demands if it does not know who the attacker is? (In contrast, cyber criminals want to stay anonymous when, for example, they attempt to extort money from victims.)

### AT: Drag Into Conflicts---2AC

#### No drag in.

Michael Horowitz 10. Assistant professor of political science at the University of Pennsylvania and a senior fellow at the Foreign Policy Research Institute. He has also held fellowships at the Olin Institute for Strategic Studies at Harvard, the Belfer Center for Science and International Affairs at Harvard, and the Weatherhead Center for International Affairs at Harvard. “A Common Future? NATO and the Protection of the Commons”. Transatlantic Paper Series No. 3 October 2010. https://csl.armywarcollege.edu/SLET/mccd/CyberSpacePubs/Trans-Atlantic\_Papers\_3-Horowitz.pdf

Concerns that specific standards might drag member states into conflict are most likely overstated, as NATO members have only invoked Article 5 once, in response to the attacks on September 11, 2001. The high threshold for invoking Article 5 means countries are unlikely to do so unless they are in grave danger.48

#### Entanglement fear is backwards---empirical studies.

Michael Beckley 15. Assistant Professor of Political Science at Tufts University. "The Myth of Entangling Alliances". War on the Rocks. 6-9-2015. https://warontherocks.com/2015/06/the-myth-of-entangling-alliances/

Since World War II, however, U.S. leaders have reversed course and signed defense pacts with more than 60 countries. As a result, the United States is legally obligated to defend a patchwork of nations that spans five continents, contains 25 percent of the earth’s population, and accounts for nearly 75 percent of global economic output. To what extent does this massive commitment entangle the United States in wars it would otherwise avoid?

This is a pivotal question for U.S. foreign policy — and one that increasingly divides U.S. policymakers from many of the nation’s most prominent international relations scholars.

U.S. political leaders almost uniformly support allied engagement, and President Barack Obama recently reaffirmed U.S. commitments to defend allies during crises between North and South Korea, Iran and Israel, Russia and Ukraine, and China on the one hand and Japan and the Philippines on the other.

A growing number of scholars, however, argue that such commitments are dangerous and should be abandoned. According to these scholars, America’s alliances are not assets but rather “transmission belts for war” that “risk roping the United States into conflicts over strategically marginal territory.” Several scholars even compare the U.S. alliance network to the tangled web of European security commitments that helped catalyze World War I. To avoid getting sucked into foreign wars, these scholars argue, the United States should scale back its alliance network or scrap it altogether — measures that, if implemented, would constitute the biggest shift in U.S. grand strategy in two generations.

Are these fears of entangling alliances warranted? To find out, I analyzed every U.S. military conflict since 1948 (the year the United States signed its first peacetime alliance) and asked a basic question: To what extent was U.S. involvement driven by formal alliance commitments?

The results, which are published in an article in International Security, are surprising: U.S. entanglement almost never happens. Over a 65-year period in which the United States had more than 60 formal allies, there have been only five ostensible episodes of U.S. entanglement — the 1954 and 1995/96 Taiwan Strait Crises; the Vietnam War; and the interventions in Bosnia and Kosovo in the 1990s — and even these cases are far from clear-cut. In each case there were other important drivers of U.S. involvement, U.S. policymakers carefully limited support for allies, allies restrained the United States from escalating its involvement, the United States deterred adversaries and allies from escalating the conflict, or all of the above.

Against this limited evidence of entanglement, I find many cases in which alliances restrained the United States, or in which the United States restrained its allies or sidestepped costly commitments. I only examine U.S. military conflicts and therefore cannot evaluate fully the prevalence of such cases of peace, but even within my biased sample, there are at least four cases in which alliances prevented U.S. escalation, and another seven cases in which the United States reneged on security commitments and/or restrained an ally from attacking a third party.

Of course, the United States has fought alongside allies on numerous occasions. But in most cases, U.S. actions were driven by an alignment of interests between the United States and its allies, not by alliance obligations. In fact, in many cases, U.S. policymakers were the main advocates of military intervention and cajoled reluctant allies to join the fight.

At worst, therefore, alliances have had a mixed effect on U.S. involvement in military conflicts — some alliances at times have encouraged U.S. military involvement, others have discouraged it, and some have simply been ignored by U.S. policymakers. The risk of entanglement is not trivial, but historically, U.S. policymakers have managed this risk by inserting loopholes into alliance agreements, shirking costly commitments, maintaining a diversified alliance portfolio that generates offsetting demands from different allies, and using explicit alliance commitments to deter adversaries and restrain allies from initiating or escalating conflicts.

Ultimately, this indicates that allied engagement does not preclude, and may even facilitate, U.S. military restraint. When the United States has overreached militarily, the main cause has not been entangling alliances but rather what Richard Betts calls “self-entrapment” — the tendency of U.S. leaders to define national interests expansively, to exaggerate the magnitude of foreign threats, and to underestimate the costs of military intervention.

Scrapping alliances will not correct these bad habits. In fact, disengaging from alliances may simply unshackle the United States and enable it to intervene recklessly abroad while leaving it without partners to share the burden when those interventions go awry.

### AT: Europe Says No---2AC

#### NATO follows on---they rely on US defense.

Justin V. Anderson, Jeffrey A. Larsen, and Polly M. Holdorf 13. Justin V. Anderson is a Senior National Security Policy Analyst with SAIC in Arlington, . Dr. Anderson received his PhD in war studies from King’s College London. Jeffrey A. Larsen is a Senior Scientist with Science Applications International Corporation (SAIC) in Colorado Springs, CO. A retired Air Force Lt Colonel, Dr. Larsen earned his PhD in politics from Princeton University. Polly M. Holdorf (Annotated Bibliography) is a National Security Analyst with Toeroek Associates, Inc. at the US Air Force Academy . “Extended Deterrence and Allied Assurance: Key Concepts and Current Challenges for U.S. Policy”. https://www.usafa.edu/app/uploads/OCP69.pdf

From the end of the Second World War to the present day, many U.S. allies have generally (if sometimes reluctantly) accepted U.S. leadership in regard to alliance policymaking and strategizing. This reflects the fact that the United States represents the strongest member within a defense pact. Furthermore, many U.S. allies believe their defense requirements exceed what they can independently develop or afford; they depend on their alliance with the United States to meet their remaining needs. As a result, many U.S. allies rely on U.S. extended deterrence and assurance strategies to guarantee their national defense. Over time, these U.S. strategies – and the forces associated with them, particularly if deployed on an ally’s home territory – often become part of an ally’s long-term foreign policy and defense planning.

As a result, once the general strategy for its assurance, and the extension of deterrence to its key adversaries, is established between the United States and a foreign ally, the latter often proves resistant to any significant change to either. Allied objections stem from concerns that any changes imply an alteration in the U.S. political resolve or military capabilities that are critical for their defense against foreign adversaries. Many allies are well aware, for example, that foreign deployments are frequently a target on Capitol Hill; both during the Cold War and afterward, Senators reviewing the U.S. defense budget have perennially pressed for allies to shoulder a greater share of the burden for their defense. In addition, although conflicts and contingencies have occasionally raised the number of U.S. troops posted overseas, in general over the past 20 years the United States has slowly but perceptibly reduced the numbers of forces permanently stationed abroad.

As a result, any change to U.S. strategies, regardless of how these changes are depicted, may lead allies to question whether their status has somehow changed within the eyes of U.S. leaders. Allies may wonder if their defense concerns are still important to Washington; if they are surprised or unprepared by a shift in U.S. policy or strategy, they may conclude their views on these changes were not considered or deemed important. Changes in the U.S. military capabilities deployed in-country or in-theater may also raise issues for allies, as many are unable to replace these forces using resources available to their own militaries.

In addition, allies resist change because many have an acute sense that U.S. extended deterrence and assurance strategies operate within a complex network of political relationships at the domestic, regional, and international levels – and as a result, any changes to these strategies can cascade throughout the entire system, often with negative impacts for their own country (or political regime, in cases where these strategies touch on sensitive local issues). They prefer maintenance of the status quo over changes that may give rise to some uncertainty – whether in their own country, in the minds of adversaries, or both – regarding whether the United States remains a reliable and predictable security partner.

Most U.S. allies, however, also regard the United States as critical to the deterrence of significant or existential threats to their national security. As discussed in the historical survey above, they will debate but rarely flatly oppose U.S. proposals to change extended deterrence or assurance strategies. Significantly, withdrawals from defense partnerships or alliances featuring the United States are rare – and even when they occur, the states involved often seek to retain some kind of defense relationship with Washington. As a result, allied resistance to alterations in extended deterrence and assurance strategies does not make change impossible, but does underline the importance of close communication and consultation between Washington and allied capitals in advance of altering or amending these strategies. Viewed over the time period discussed in Part 3, their interest in maintaining the status quo represents a phenomenon that was sometimes overlooked within the U.S. strategic community – despite dramatic geopolitical change, to include superpower détente, the end of the Cold War, and 9/11. Many longtime U.S. allies remained continually reliant on their partnership with the United States to shield them from current enemies, prospective threats, regional instability, and shocks to the geopolitical system.

#### Biden push solves.

Franklin D. Kramer et al. 20. Franklin D. Kramer is a distinguished fellow with the Scowcroft Center for Strategy and Security and a board director of the Atlantic Council Lauren M. Speranza is director of Transatlantic Defense and Security at the Center for European Policy Analysis (CEPA). Conor Rodihan is an assistant director in the Scowcroft Center for Strategy and Security’s Transatlantic Security Initiative. "NATO needs continuous responses in cyberspace". Atlantic Council. 12-9-2020. https://www.atlanticcouncil.org/blogs/new-atlanticist/nato-needs-continuous-responses-in-cyberspace/

President-Elect Joe Biden’s transition team has declared cyber threats as “one of the defining challenges of our time.” In its early days, the incoming US administration must take on cybersecurity threats as one of its key priorities. Nowhere will that effort be more important than with the United States’ closest Allies at NATO, a cornerstone for Western security. Today, NATO’s security is threatened by Russia’s and China’s continuous cyberattacks on the Alliance and its members. To accomplish its mission of deterrence and defense, NATO needs to implement a strategy of proactive, continuous responses to China and Russia in cyberspace, where great power competition is playing out in real time.

Russia and China challenge NATO and its members in cyberspace on a daily basis, as part of ongoing hybrid campaigns to undermine the transatlantic community. The Kremlin’s actions have involved intrusions into Allies’ critical infrastructures, manipulating Allies’ elections through hacks and disinformation, and even blocking GPS information critical to NATO activities. The Chinese government has engaged in cyber espionage against Allies’ military capabilities; intellectual property theft related to sensitive technologies, industries, and infrastructure; and disinformation against transatlantic countries, including around the coronavirus. These efforts to weaken NATO countries and Alliance cohesion represent a persistent threat to Allied security.

NATO has recognized the collective dangers of these hybrid attacks in cyberspace. Up to this point, however, the Alliance has taken a reactive approach, responding as if Russian and Chinese cyber attacks are each isolated incidents. But because Russian and Chinese cyber efforts are part of continuous campaigns directed at the overall capability of the Alliance, NATO’s response has been insufficient, failing to reduce or dissuade further attacks. To assure the security of its members going forward, NATO needs its own continuous response campaign to these threats.

President-elect Biden and his team have pledged to renew US leadership in cooperation with Allies and partners. That agenda should start at NATO, and a key focus should be on cybersecurity. In early NATO meetings, the Biden administration should champion a cybersecurity continuous-response campaign, built around three key actions.

### AT: Europe Solves---2AC

#### Local governments fail

CSE 20. Cyber Security Europe. "Elections vulnerable to cyber threats, say surveyed cyber pros". Cyber Security Europe. 7-13-2020. <https://www.cseurope.info/elections-vulnerable-to-cyber-threats-say-surveyed-cyber-pros/>

Europe’s democratic processes are exposed to interference and attack by cyber threats, a poll of IT security practitioners has warned. Seventy percent of those polled at the RSA Conference 2020 for a survey by machine identity protection specialist Venafi believe their local governments ‘cannot adequately defend election infrastructure against domestic and international cyber attacks’.

The survey also found that 75% of respondents believe that the spread of disinformation is now the ‘greater threat to election integrity’.

“IT security professionals are rightly concerned about cyber threats impacting the democratic process. The election ‘season’ is already in process, and the Coronavirus pandemic adds a new layer of security complications,” says Kevin Bocek, VP of Security Strategy & Threat Intelligence at Venafi. “Cyber attackers may take advantage of this period of uncertainty to further undermine public confidence by spreading disinformation. As a result, it is not surprising that many security experts are concerned that governments will not be able to safeguard election data.”

### XT---Solvency/Clarity Key---2AC

#### Clarity key to solvency.

Andrew Erskine 3/14/22. Parliamentary & legislative assistant to a Canadian Member of Parliament. He is also a research analyst at the NATO Association of Canada and a researcher for the Consortium of Indo-Pacific Researchers. He is a political analyst for The New Global Order, a think tank for young academics and professions based in Rome, Italy. Andrew is also an analyst director for the NATO Research Group, where he leads a case study on regional security in Southeast Asia. He holds a master’s degree from the University of Prince Edward Island. "The Western Flank: The Geosecurity Periphery NATO Forgot It Had". Air University (AU). 3-14-2022. https://www.airuniversity.af.edu/JIPA/Display/Article/2964827/the-western-flank-the-geosecurity-periphery-nato-forgot-it-had/

In the long-term, NATO needs to clarify and strengthen its stance on cyberattacks—formally enshrining what constitutes grounds for invoking Article V. In 2014, NATO declared that cyberattacks could invoke Article V, ambiguously directing such statements to Russia. However, it is worth pointing out that NATO members—in Europe and North America—have frequently been the targets of cyberattacks originating from Chinese proxies.62 Although similar occurrences of cyberattacks are still occurring, NATO has not moved forward on this vital geosecurity matter.

To improve its resilience to cyberthreats from China and Russia, NATO needs to outline the types of cyberattacks that merit the invocation of Article V, along with advancing a counterinitiative to respond to hybrid forms of state-centric and proxy-centric cyber conflicts.63 A proclamation should also include the prohibition of cyberattacks on civilian digital infrastructure and grids, along with the capacity to threaten cyberattacks to coerce a NATO member into appeasing the demands of an antagonistic power such as China or Russia. As such, NATO should vehemently proclaim that “a coercive threat against one is a coercive threat against all.”64

#### NATO must clarify Article 5 for cyber.

Michael Klipstein and Tinatin Japaridze 2/24/22. Michael Klipstein, Associate Research Scholar, Arnold A. Saltzman Institute of War and Peace Studies, Columbia University. Tinatin Japaridze, Vice President of Business Development and Strategy, The Critical Mass. "Collective cyber defence and attack: NATO’s Article 5 after the Ukraine conflict". No Publication. 2-24-2022. https://www.europeanleadershipnetwork.org/commentary/collective-cyber-defence-and-attack-natos-article-5-after-the-ukraine-conflict/

Following the shortcomings of the 2015 United Nations Group of Governmental Experts report on information and telecommunications in the context of national security, a lack of consensus continues to exist on the severity of cyberspace operations targeting critical infrastructure requiring collective and even national responses. Individual nations constructed individual criteria and response actions, utilising diplomacy, information, military, or economic action. They largely did so alone or in combination with other states. NATO, however, did not formulate a coherent analogous response and as a result, lacks publicly acknowledged policy addressing cyberspace activities that would constitute a necessary collective response under Article 5. In order for NATO to maintain its relevance in the present moment and sustain it through the coming years, this paradigm must change.

NATO must adjust its thinking regarding methods of warfare as cyberspace operations—both destructive attacks and disinformation—continue to grow in complexity and in certain areas even replace traditional kinetic operations. To fulfill this role in kinetic as well as non-kinetic realms, NATO must be prepared for hybrid forms of warfare and present slated to join the alliance a cohesive and tailored response to transgressions. This is increasingly important as Russia continues to threaten potential future NATO members such as Finland and Sweden, who are slated to join the alliance in the coming months. Russia has overtly stated that the invasion of Ukraine was, in part, a response to NATO’s eastward expansion. Although Russia has deemed NATO expansion into former Soviet states to be problematic since the collapse of the USSR, recently, Moscow has also begun to denounce potential expansion beyond its perceived immediate sphere of influence. For example, on April 14, 2022, Russian Minister of Foreign Affairs Sergei Lavrov cautioned that the inclusion of Finland and Sweden into the military alliance would have dire consequences, including Russia reinforcing nuclear weapons in the Baltic Sea region.

Considering the increased emphasis and relevance of the transatlantic alliance leading up to and during Russia’s invasion of Ukraine, it is imperative for the organisation’s member states to identify and agree upon more pronounced “triggers” or “red lines” that determine what constitutes a sufficiently egregious action in cyberspace for Article 5 to be discussed, and if need be, potentially invoked. Furthermore, in enhancing its preparedness in cyberspace, specific policies must be crafted that delineate synchronised actions taken collectively by members to prevent Russian malign activities in the cyber domain under Article 5 to allow for a rapid and coordinated response. The dominance of the US, the UK, Australia, Canada, and New Zealand, known in government as the FVEY, or Five-Eyes, highlights the urgent need for the alliance to develop policy addressing the collective defence of NATO members. Effective policy for NATO should address collective and coordinated cyberspace operations, both offensive and defensive. Currently, NATO, as a military institution, lacks “rules of engagement” for cyberspace and individual member states lack a standardised threshold or response guidance. Therefore, NATO must define the activities, “red lines”, and threshold incurring response, as well as what a coordinated kinetic/cyber response would entail. The interconnectedness of European critical infrastructure, as illuminated by the Russian ViaSat communications attack impacting German wind power generation and distribution, highlights the requirement for NATO to address cyberspace as the critical domain it is. As a result, we recommend:

* In the event of adversarial cyberspace actions warranting Article 5 action, the NATO Commander becomes the commander and coordinator for all cyberspace activities, both defensive and offensive, by NATO nations within the area of hostilities.
* NATO identifies, establishes, prioritises, and continually refines critical infrastructure and key resources within member nations, as well as criteria for what constitutes necessary action for collective responses.
* NATO identifies limits of activity, or “red lines” resulting in Article 5 response discussions.
* NATO members present the NATO Commander intelligence identifying indications, warnings, and attribution of cyberspace attacks, both for response action and, where applicable, public consumption.
* NATO members present legal constraints and capabilities of nations to the NATO commander allowing maximisation of nations’ capacity and capability.

NATO must recognise cyberspace for what it is—an interlocutor of networks and devices from control systems for critical infrastructure to seemingly anonymous devices operating in the background of our lives. This interconnectedness by an invisible thread of information, however, is the critical vulnerability in the stability of societies. NATO must plan to protect the infrastructure and key resources of member states as a unified effort, not a piecemeal operation undertaken by a few nations. In order to do this, NATO must identify and prioritise infrastructure for protection, as well as criteria and policy for action. Russia’s recent invasion of Ukraine and the Kremlin’s increased aggression, not solely in kinetic but also in non-kinetic realms, is a stark reminder that the alternative to further delay of the inevitable recognition of cyberspace for what it is will, ultimately, prove to be all the more costly.

### XT---Solvency/Deterrence---2AC

#### Plan solves---Article 5 causes Russia to back down.

Dr. Brian Mark Rigg 3/31/22. Military historian, former Marine officer and a financial planner. "Military Historian Talks Cybersecurity, Cyberattacks and Article 5 of NATO". EIN News. 3-31-2022. https://www.einnews.com/pr\_news/567021689/military-historian-talks-cybersecurity-cyberattacks-and-article-5-of-nato

DALLAS, TEXAS, UNITED STATES, March 31, 2022 /EINPresswire.com/ -- Should Russia’s attacks against us in the cyberwar space be considered an attack on NATO as a whole?

This is a complicated question to answer. However, in light of the damage cyber warfare can inflict on society, from shutting down computers at our nation’s medical centers, water treatment plants, transportation centers and banks, to disrupting the flow of capital from financial institutions for our national defense, one should consider a cyberattack a violation of the Geneva Convention, a Crime Against Peace, and an act that should trigger Article 5 of NATO’s treaty.

Article 5 of NATO’s founding treaty states that an attack on one is an attack on all. This article is meant to foster a spirit of solidarity with, and commitment to, all the members of this treaty, which now numbers 30 nations. The only time Article 5 has been enacted to date was after 9/11, when NATO collectively declared war against terrorism in general, and specifically against the terror groups located in Afghanistan under the command of Osama bin Laden.

Russia’s guilt is clear. We already know Russia meddled in America’s elections in 2016. We have evidence they continue to collect and interfere with our day-to-day operations in business and private life. Russia has large military outfits whose focus is strictly on attacking civilians of nations it deems hostile (like the United States). And the White House recently warned that the Putin government is searching out “options for potential cyberattacks” on critical American infrastructure in retaliation for Western sanctions following Russia’s invasion of Ukraine.

Cyberwarfare is a form of warfare with offensive and defensive capabilities. Going forward, NATO needs to send a strong message that if Russia presses a cyberattack on any NATO nation, it is an act of war—and NATO will respond strongly in kind.

Russia needs to be stopped from bullying the world. In light of Putin’s anger at how pathetic his military is performing in Ukraine, how isolated he must be feeling as the world cuts off the flow of trade to and from his nation, and how the hatred for Russia grows as its military kills innocent women and children (a clear violation of the Geneva Convention), Putin will likely resort to areas where he can inflict harm. He will especially do so in a realm where the world until now has not really held him accountable. After he meddled in the 2016 U.S. elections, shouldn’t the world have sanctioned him? That was a direct attack on a democracy. However, nothing was done. Isn’t it time to do something?

How might we counterattack a cyberattack? According to Article 5, it would be a full-on conventional attack across the board from NATO. If Article 5 is to be taken seriously, the 30 nations of NATO need to send a strong message to Putin and his Russian military goons that they cannot get away with causing death and chaos in the world like they have been doing for years. Yes, Putin has nuclear rockets and missiles—but will he try and nuke the entire NATO world? And what would that accomplish for him in return? It would mean the nuclear obliteration of his own nation.

Dictators throughout time have repeatedly shown that as their power increases, their reason decreases. With this in mind, Putin’s threats about using atomic warfare against the West needs to be taken seriously. However, if we want to remove Putin from power and prevent his legions from causing further chaos, we must stand up to him and show him and the Russian people that just because you are willing to use nuclear weapons does not mean that enemy nations are also not willing to use those same type of weapons against you. In this respect, using Article 5 in the broadest sense of its meaning should give Putin (or at least his military leadership) pause before they enact cyberwarfare, because they will understand the type of response it would elicit from NATO countries. Bullies usually stand down when the people they are picking on hit back—and hit back harder.

#### Cyber appeasement causes war---plan key

James Stavridis 2/26/22. Bloomberg Opinion columnist. He is a retired U.S. Navy admiral and former supreme allied commander of NATO, and dean emeritus of the Fletcher School of Law and Diplomacy at Tufts University. He is also chair of the board of the Rockefeller Foundation and vice chairman of Global Affairs at the Carlyle Group. "The West’s Cyber Appeasement Helped Give Putin a Green Light". Washington Post. 2-26-2022. https://www.washingtonpost.com/business/energy/the-wests-cyber-appeasement-helped-give-putin-a-green-light/2022/02/26/339f5a68-970d-11ec-bb31-74fc06c0a3a5\_story.html

There were many reasons Russian President Vladimir Putin finally decided to invade Ukraine, but one was the failure of an international alignment on the consequences of such aggression. Tacit indifference to Russia’s behavior from both sides of the Atlantic — regarding previous invasions of Georgia in 2008 and Ukraine in 2014, nerve-agent attacks on political opponents, support for a bloody war criminal in Syria — undoubtedly encouraged the Kremlin’s provocations.

But it’s not just indifference to Russia’s recent kinetic aggression that’s to blame. Insufficient response to its non-kinetic military operations helped equip the Kremlin with an effective virtual complement to the traditional invasion. The West in effect conducted a policy of digital appeasement in response to multiple cyberattacks. How did we get here, and what can we do going ahead?

In 2015, Russia’s military intelligence directorate launched a cyberattack that knocked out power for over 200,000 Ukrainians two days before Christmas. This was followed in June 2017 when shadowy Russian actors compromised a popular tax accounting software called M.E. Doc, which was later distributed to hundreds of thousands of customers via a corrupted software update. Malware that was apparently intended for local effects propagated globally, resulting in billions of dollars in damages. It cost pharmaceutical company Merck & Co. an estimated $1.3 billion alone.

More recently in the U.S., we have seen ransom attacks by Russian cybergangs against various corporations and critical infrastructure, including the Colonial pipeline and parts of the food chain. The 2020 SolarWinds Corp. attack, which affected hundreds of the largest corporations in the U.S. and many government agencies, almost certainly originated in Moscow.

Thus it should have come as no surprise that in recent days Ukraine’s largest bank and defense agencies reported being hit with the biggest denial-of-service attack in the country’s history. This, and subsequent hacks, set the stage for the Thursday’s military thrust.

Cyberwarfare is a powerful asymmetric capability for any nation-state seeking to prepare the battlefield for an invasion; to support operations at sea, in the air or on land; and to achieve disruptive or destructive effects against digital or physical targets. Despite this military effectiveness, however, far too often the West has failed to respect cyberwarfare’s role as a strategic instrument of power projection.

Russia wields the power of cyber not necessarily to cause widespread damage, but to operate with precision below the perceived threshold of war, and thus beyond the reach of political consequences. Cyberattacks are at the heart of Putin’s so-called hybrid warfare, central to the current Kremlin playbook. And the Western allies have allowed Russia to act virtually unchallenged — even when it has involved meddling in U.S. and European elections — evoking legitimate comparisons of European appeasement of the Nazis in the lead-up to World War II.

### XT---Solvency/Democracy---2AC

#### The plan is key to prevent authoritarian cyber control---collapses democratic norms.

Jonathan Terra 21. Political scientist and former diplomat. "NATO Cannot Cede the New Art of Modern Warfare to Russia and China". Balkan Insight. https://balkaninsight.com/2021/08/04/nato-cannot-cede-the-new-art-of-modern-warfare-to-russia-and-china/

As cyberattacks start to resemble traditional acts of war in their destructive power, initiatives like the EU’s planned Joint Cyber Unit aimed at “coordinated detection and response” will prove inadequate for dealing with the problem. Only a bold doctrinal innovation of the mutual defence clause in Article 5 of the North Atlantic Treaty, based on a clear and proportional deterrent which updates the contemporary meaning of “an armed attack”, will prevent cyberwarfare from escalating and compelling the use of even more destructive means of waging war in the foreseeable future.

Point 32 of the Brussels Summit Communiqué of 14 June 2021 announcing NATO’s Comprehensive Cyber Defence Policy (CCDP) takes the first tentative step toward doing this. The statement asserts that: “the Alliance is determined to employ the full range of capabilities at all times to actively deter, defend against, and counter the full spectrum of cyber threats… in accordance with international law.” The CCDP also recognises that “significant malicious cumulative cyber activities might, in certain circumstances, be considered as amounting to an armed attack”, and it “reaffirm[s] that 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.”

Despite the tough words, the communiqué merely reaffirms a strategically muddled and dangerously ambiguous ad hoc policy of crisis management, damage control, and maybe retaliating – but only “in certain circumstances”. An effective CCDP would instead delineate clearly where inviolable national boundaries lie in cyberspace; formulate what a “proportionate response” could look like after a debilitating attack on any of the 16 critical infrastructure sectors; and incorporate these policies into an updated mutual defence doctrine based on a revised version of Article 5.

China’s increasingly aggressive approach to cyber warfare – which has recently evolved from an established pattern of technology theft to Russian-style disruption employing a wide range of highly-skilled domestic hackers who attack without restraint – gives further context to the urgency of effective cyber deterrence.

We have a clear choice: the transatlantic democratic alliance will either vigorously deter potentially costly aggression in any theatre of conflict, including cyberspace, and defend the values fought for in two world wars and numerous other bloody conflicts since 1945; or we will surrender to the current assault on liberal democratic norms from Russia, China and their opportunistic allies, and accept their vision of a post-liberal, post-democratic world as our inevitable collective future, as we cede the new art of modern warfare to them.

The stakes could not be higher.

### XT---Nationalism/Democracy/Secession IL---2AC

#### Russian cyber war pushes nationalism.

Brian E. Frydenborg 20. MS in Peace Operations from George Mason University's School of Public. BA from Washington and Lee University in Politics and History. Former intern in the United States Senate. "Nationalism: A National Security Threat from Without and Within and one of Putin’s Favorite Weapons". Real Context News (RCN). 9-10-2020. https://realcontextnews.com/nationalism-a-national-security-threat-from-without-and-within-and-one-of-putins-favorite-weapons/

Yet beyond use of military force, Russia would be even bolder with different approaches. The year 2014 saw Russian “active” hybrid measures support the 2014 Scottish secession campaign in the UK; 2016, the Brexit campaign, a failed coup attempt in Montenegro designed to thwart its entry into NATO, among other aims; the campaign to weaken and destabilize the U.S. by installing Donald Trump as the U.S. president in what I called back in December, 2016, the First Russo-American Cyberwar, which involved major efforts by Prigozhin in one of his other major capacities: helping to run Russia’s cyberwarfare (indeed, as I have written before, he is a real nexus of Russian international aggression). Since then, Russia has interfered with Catalonia’s secessionist campaign and German, French, Austrian, Italian, British, Dutch, Swedish, (North) Macedonian, Ukrainian, Bulgarian, Moldovan, and, even now in 2020, American votes. Also currently, Putin may be prepping for a military intervention in Belarus to crush a democratic uprising there, and we should not forget more general cyberattacks on Finland and the steady stream of cyberattacks against the Baltic states of Estonia, Latvia, and Lithuania.

There seem to be even still more countries that have been the target of Russian political interference and cyberwarfare.

With a large portion of these Russian campaigns, Putin has expertly manipulated what czars and comrades alike had often skillfully manipulated throughout Russian and Soviet history both within Russia and throughout is periphery: nationalism. And many of these campaigns are part, as I have noted before, of a larger Russian war against the West mean to destroy, NATO, European unity, and even Western democracy as we know it.

In his 1931 book Conversations with Oscar Wilde, A. H. Cooper-Prichard presented the following exchange with the book’s namesake: “’How is it,’ I once asked him, ‘that people who are not possessed of a single other virtue should come out at times as patriots?’ ‘Exaggerated patriotism,’ he answered, ‘is the most insincere form of self-conceit.’ And at another time he said, ‘Patriotism is the virtue of the vicious.’” And in his “Notes on Nationalism,” Orwell—who would use the term “nationalism” as Wilde used “patriotism,”—wrote that “nationalist thought” could be characterized primarily by “obsession,” “instability,” and “indifference to reality,” that one of the great dangers he saw for nationalism was that it “may work in a merely negative sense, against something or other and without the need for any positive object of loyalty.” Orwell here famously defined nationalism as

first of all the habit of assuming that human beings can be classified like insects and that whole blocks of millions or tens of millions of people can be confidently labelled ‘good’ or ‘bad’. But secondly – and this is much more important – I mean the habit of identifying oneself with a single nation or other unit, placing it beyond good and evil and recognizing no other duty than that of advancing its interests.

As Putin acts as a maestro conducting an orchestra of nationalism on a global scale to his ends in 2020 in ways most of us could have hardly imagined back in 2008, it is useful to look at how the Georgia war—this first great foreign campaign of Putin’s—can be a window into the world of nationalism, showing how banal and, sadly, normal ethno-nationalism can be. This is true globally, and I used excerpts from my 2009 graduate school paper that discussed nationalism in Georgian history to shed light—just weeks before his socking victory in the United States—on the rise of the similarly thoroughly unoriginal, bland, and boring nationalism of then-candidate Trump.

That exploration of my older 2009 work—which in important ways was especially enriched by Ronald Grigor Suny’s deconstruction of nationalism as a very much consciously constructed phenomenon with two main sides: inclusion and exclusion—in a 2016 context has only increased in relevance thanks to what President Trump and Trumpism have become: the largest force in American politics since George Wallace to be built so nakedly on inclusion and exclusion. The president does not even attempt to hide that white ethno-nationalism is what will be included in, and other identities excluded from, the top position in the national hierarchy. This white, exclusionary ethno-nationalism, which he fanned and flamed into the White House with substantial Russian support, has only gotten more extreme and more powerful since then and today has plenty of sensible people worried about the prospects of both civil war and the death of true American democracy.

### XT---Credibility IL---2AC

#### The plan solves NATO credibility---shows they can adapt.

Ethan Williamson 19. Security+ Certified Cyber Task Order Analyst with DoD Secret Clearance. "NATO’s Expanding Role in Cybersecurity". Charged Affairs. 5-13-2019. https://chargedaffairs.org/natos-expanding-role-in-cybersecurity/

As cyber attacks become more prevalent, NATO must address its shortcomings in responding to potential threats. If NATO clearly defines its role in cybersecurity and demonstrates that it can provide sound responses to attacks, NATO will not only be able to protect itself, but also expand its influence to new partners looking for security.

#### Asymmetric attacks collapse alliance credibility---comprehensive response strategy key

Brittany Beaulieu and David Salvo 18. Brittany Beaulieu is a fellow and program officer at the Alliance for Securing Democracy at The German Marshall Fund of the United States. David Salvo is deputy director of the Alliance for Securing Democracy at The German Marshall Fund of the United States. “NATO and Asymmetric Threats: A Blueprint for Defense and Deterrence”. German Marshall Fund of the United States. https://www.jstor.org/stable/pdf/resrep18856.pdf

Russia is increasingly turning its asymmetric arsenal on NATO allies to attack the credibility of the Alliance, undermine democratic institutions across member states, and disrupt NATO cohesion on a variety of policy and security issues. Despite falling below the threshold of conventional warfare, asymmetric threats are designed to weaken the security of the Alliance and individual allies, as well as destabilize allied governments and societies. NATO has taken some measures to address hybrid threats; however, NATO needs a more comprehensive strategy to counter the growing threat that asymmetric interference poses. The NATO Brussels Summit taking place July 11 and 12 presents an important opportunity on this front.

#### Sustained Russian attacks break Article 5---response is key

LéO-Paul Jacob 17. Junior Research Fellow at the NATO Association of Canada(NAOC), currently in his third year of B.A(Hons) in Political Science at Concordia University, "An Exploration into the Growth of Russian Cyber Warfare". NAOC. 3-25-2017. http://natoassociation.ca/russias-cyber-warfare/

More importantly, due to heightening tensions between NATO and Russia in the Baltic region, Russia may use cyber warfare against a Baltic state to test the strength and unity of the Alliance. If well-calibrated, and used along with other forms of hybrid warfare for a short period of time, such an attack could undermine the credibility of NATO’s article 5 if it is unanswered by the Alliance. This lack of solidarity, while damaging the credibility of the Alliance, would be an immense symbolic victory for Russia. Thus, to limit the probability of such an event occurring, NATO must boost its cyber defences and develop stronger offensive cyber warfare capabilities.

#### The plan solves credibility gaps---shows the US can meet any domain of defense.

Justin V. Anderson, Jeffrey A. Larsen, and Polly M. Holdorf 13. Justin V. Anderson is a Senior National Security Policy Analyst with SAIC in Arlington, . Dr. Anderson received his PhD in war studies from King’s College London. Jeffrey A. Larsen is a Senior Scientist with Science Applications International Corporation (SAIC) in Colorado Springs, CO. A retired Air Force Lt Colonel, Dr. Larsen earned his PhD in politics from Princeton University. Polly M. Holdorf (Annotated Bibliography) is a National Security Analyst with Toeroek Associates, Inc. at the US Air Force Academy . “Extended Deterrence and Allied Assurance: Key Concepts and Current Challenges for U.S. Policy”. https://www.usafa.edu/app/uploads/OCP69.pdf

In short, while the United States possesses offensive and defensive capabilities to address these challenges, it is possible that adversaries or allies would conclude there are significant gaps within the U.S. armor. Regardless of whether these perceptions are empirically true, they represent a challenge to the U.S. ability to deter and extend deterrence. With deterrence in the eye of the beholder, it is important for the United States to project an image of strength to both adversaries and allies, particularly in areas or operations that U.S. leaders have identified as important to U.S. and allied security. If the United States continues to struggle to address new space and cyber threats, and if potential adversaries continue to develop new, more sophisticated, and more diverse WMD and long-range strike capabilities, the United States may face increasingly persistent questions from foreign actors regarding whether it can continue to meet global defense obligations and carry out round-the-clock, cross-domain strategic operations.

## Case---Recutting/AT: Authors

### AT: Lonergan and Moller 22/Overcommitment---2AC

#### Clarifying ambiguity solves overcommitment

1NC Erica D. Lonergan and Sara B. Moller 4/27/22. Erica D. Lonergan is an assistant professor in the Army Cyber Institute and a research scholar at the Saltzman Institute of War and Peace Studies at Columbia University. Sara B. Moller is a former Eisenhower Fellow at the NATO Defense College and will be joining the Center for Security Studies at Georgetown University later this year. “Opinion | NATO’s Credibility Is on the Line with its Cyber Defense Pledge. That’s a Bad Idea.” Politico. 4-27-2022. https://www.politico.com/news/magazine/2022/04/27/nato-credibility-cyber-defense-pledge-russia-ukraine-00027829

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

### AT: Smeets 21/Divergence---2AC/1AR

#### The plan’s MoU solves.

Dr Max Smeets 21. Center for Security Studies, ETH Zürich (Switzerland) . "NATO allies’ offensive cyber policy: A growing divide?". 8-6-2021. https://hcss.nl/report/nato-allies-offensive-cyber-policy-a-growing-divide/

The divergence in cyber policy across NATO member states is problematic. Allies disagree on both the goals of cyber policy and the ways and means to achieve them. This can cause tension between allies, especially when it comes to the necessity and legitimacy of operating on each other’s national systems and networks.

Some may argue that these differences result from differences in maturity. Some states simply have not caught up with the latest developments, goes the argument. This assumes a single path to cyber maturity or that the dynamics of cyberspace pull all states in the same direction. It suggests that – even without major policy coordination – allies’ cyber policies will converge over time. But a more persuasive understanding of the current trend is that even though states can learn from each other’s institutional progress, differences do not merely stem from states “lagging behind.” These states are on a different policy path. This means it requires dedicated and sustained policy attention to, at a minimum, coordinating the different policies of states – and potentially bring them closer together.

---1NC CARD ENDS---

What can be done to ensure that this divergence in cyber policy does not cause further friction between allies?[11]

I have previously proposed a NATO Memorandum of Understanding (MoU) to reduce discord among the allies; the goal would be to enhance trust, transparency, and confidence between allies and to improve the effectiveness of disrupting and deterring adversaries’ operations in cyberspace.[12] The main purpose of the MoU would be to reach an agreement on the equities involved in permitting signatories to conduct cyber effect operations in each other’s networks—and the relative weight of those equities.

### AT: Patrick 18/Attribution---2AC

#### Patrick concedes clarity solves war.

1NC Stewart M. Patrick 18. James H. Binger Senior Fellow in Global Governance and Director of the International Institutions and Global Governance Program. "NATO's Deterrence Problem: An Analog Strategy for a Digital Age". Council on Foreign Relations. https://www.cfr.org/blog/natos-deterrence-problem-analog-strategy-digital-age

Given these stakes, NATO has an obvious incentive to strengthen its capacity to deter and punish cyberattacks, including through conventional retaliation. A U.S. Department of Defense memorandum published in early 2017 stated that at least for the next decade, offensive cyber capabilities are likely to outpace cyber defense, making deterrence the most viable option. Both the United States and NATO also recognize that a devastating cyberattack could quickly escalate to violent conflict by triggering a conventional response. Unfortunately, the alliance’s policy of strategic ambiguity falls short. By failing to define the rules of engagement for retaliation, the alliance leaves open the potential for chaos in determining an appropriate response to cyberattacks. In doing so, it invites adversaries to test the waters.

---1NC CARDS STARTS---

Cyber deterrence is inherently more challenging than nuclear or conventional deterrence because such attacks are difficult to definitively attribute to a particular actor. For example, it is easier to mask the source of a cyberattack on a power grid than it would have been for the Warsaw Pact to conceal a massive incursion into West Germany. This attribution problem could complicate NATO’s capacity to conclusively determine the source of a cyberattack and justify and conduct a timely conventional response, particularly if member states diverge in their perceptions. This dilemma could strain the foundations of collective defense and undermine any unified front against cyberattacks.

For NATO to commit to military action, all of its members would need certainty, beyond a reasonable doubt, about the identity of the perpetrator. This is particularly true in the case of Russia—a known sponsor of cyberattacks. Without conclusive proof, it might be a challenge to convince a distant country like Portugal or a dangerously close one like Estonia to join in a counterattack. Complicating matters, such post-attack decisions would need to be made quickly, given Russia’s precedent of using cyberwarfare as a precursor to kinetic invasion. The need for speed leaves little room for philosophical debates over what constitutes an act of war.

---1NC CARD ENDS---

To be sure, NATO’s strategic ambiguity is not without its benefits. Uncertainty about the threshold for a military response could persuade an adversary not to push the envelope with an audacious attack. But that same ambiguity could lead an adversary to miscalculate. Moreover, the doctrine also leaves open the possibility of discord in the ranks of NATO member states regarding how to deal with any such attack.

NATO’s policy of strategic ambiguity served it well during the long Cold War nuclear confrontation. But it may be less appropriate to the era of cyberwarfare, particularly given the problem of attribution and the potential for inter-allied disagreement on the appropriate response to any particular incident. NATO policymakers need to resolve this dilemma by formulating a more explicit cyberwarfare doctrine to which all of its member states can adhere. This should include updating their mutual understanding of what constitutes an act of aggression under NATO’s collective defense provisions, making explicit to potential adversaries just what its red lines are, and establishing clear procedures and channels for robust allied response to cyberattacks. Unless NATO clarifies current ambiguities, Russian aggression in the cyber realm could go unchecked.

## AT: Topicality---“Cybersecurity”

### CI---Cybersecurity---2AC

#### Counter-interpretation---cybersecurity includes deterrence and response.

Reeshad S. Dalal et al. 22. Department of Psychology, George Mason University David J. Howard, Department of Psychology and Muma College of Business, University of South Florida. Rebecca J. Bennett, Department of Management, College of Business, University of Central Florida. Clay Posey, Department of Management, College of Business, University of Central Florida & Cybersecurity and Privacy Cluster, University of Central Florida. Stephen J. Zaccaro, Department of Psychology, George Mason University. AND Bradley J. Brummel, Department of Psychology, The University of Tulsa. “Organizational science and cybersecurity: abundant opportunities for research at the interface”. J Bus Psychol. 2022; 37(1): 1–29. Published online 2021 Feb 4. doi: 10.1007/s10869-021-09732-9

\*\*NOTE---This is from Table 1, accessible @ https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7861585/table/Tab1/?report=objectonly

|  |  |
| --- | --- |
| Cybersecurity | “Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompass[ing] the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure” (NICCS, 2018). See also “organizational cybersecurity.” |

### XT---CI---Cybersecurity---1AR

#### Cybersecurity includes incident response.

Chris Jaikaran et al. 18. Coordinator, Analyst in Cybersecurity Policy. John W. Rollins, Specialist in Terrorism and National Security. Rachel F. Fefer, Analyst in International Trade and Finance. Rita Tehan, Senior Research Librarian. Kristin Finklea, Acting Section Research Manager. Catherine A. Theohary, Specialist in National Security Policy, Cyber and Information Operations. Eric A. Fischer, Senior Specialist in Science and Technology. Baird Webel, Specialist in Financial Economics. “Cybersecurity: Selected Issues for the 115th Congress”. https://sgp.fas.org/crs/misc/R45127.pdf

This report provides an overview of cybersecurity concepts, the role of selected federal agencies in addressing cybersecurity threats, and a discussion of cybersecurity issues that may be of interest to Congress, including:

 protecting critical infrastructure;

 data breaches and data security;

 education and training;

 encryption;

 information sharing;

 insurance;

 international issues;

 the Internet of Things;

 oversight of federal agency information technology; and

 incident response.

This is a coordinated report with multiple authors, who are listed with their contact information in footnotes at the beginning of the section(s) they authored as well as at the end of the report.

### AT: Only Deterrence by Denial---2AC

#### Both punishment and denial are cybersecurity strategies.

Chris Jaikaran 1/18/22. Analyst in Cybersecurity Policy. CRS. “Cybersecurity: Deterrence Policy”. https://crsreports.congress.gov/product/pdf/R/R47011

Denial and deterrence cybersecurity strategies are different approaches to achieve the same goal: a safer digital environment. These strategies are not mutually exclusive. As seen by the Commission’s recommendations, particular activities can serve both strategies, and combining activities can have a multiplier effect on the actions.

Generally, for cybersecurity, denial strategies seek to improve technology, processes, and practices over something in one’s own control so that despite an adversary’s efforts, their success rate is low. Deterrence strategies seek to affect the behavior of other individuals or entities— stopping them from engaging in an unwanted activity. The DOD developed descriptions of “denial” and “deterrence,” which are used in this report in the context of cybersecurity to categorize activities and provide a framework for discussing policy options.

Glossary

Denial A denial measure is an action to hinder or deny the enemy the use of territory, personnel, or facilities. It may include destruction, removal, contamination, or erection of obstructions. 11

Deterrence Deterrence prevents adversary action through the presentation of a credible threat of unacceptable counteraction and belief that the cost of the action outweighs the perceived benefits.12

### XT---Includes Offensive---1AR

#### Offensive usage is cybersecurity!

Haleema Zia 21. Director Communications, ADAL Foundation Islamabad. “The Evolution of Artificial Intelligence: Implications for Cybersecurity and Hybrid Warfare”. Pakistan Jounral Of Terrorism. https://nacta.gov.pk/wp-content/uploads/2019/12/Pakistan-Jounral-Of-Terrorism-2021-web-version.pdf

Cybersecurity includes a broad range of tools, applications, and concepts which are closely related to informational and operational defence. It involves the offensive usage of information technology for attacking adversaries. According to technology practitioners the term cybersecurity should only be used for security purposes that involve information or operational technology systems51. Cybersecurity is defined as the development, management, governance and use of operations security, information security, and Information Technology security techniques and tools in order to defend assets, compromise the assets of adversaries, and achieve regulatory compliance52. Cyber defence is a computer-based network defence mechanism that provides responses to certain actions and protection to precarious infrastructure and information assurance for government entities, organizations and other related networks. Cyber defence is very important in order to prevent sensitive data and information and to safeguard assets. It involves prevention, detection, and provision of timely responses to threats or attacks. It provides assurance to work and run different processes and activities without worrying about threats or attacks53.

### AT: Mahoney---1AR

#### Offensive is a subset of cybersecurity.

Dr. Charles W. Mahoney 21. Associate professor in the Department of Political Science at California State University, Long Beach. He holds a PhD from UCLA. His research on international security, foreign policy, and defense outsourcing has been published in numerous scholarly journals. “Corporate Hackers: Outsourcing US Cyber Capabilities.” Strategic Studies Quarterly. https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-15\_Issue-1/SSQSpring2021.pdf?ver=St5HSe-vLIhxcbMF13qh-w%3D%3D&timestamp=1614258916947

Cyber operations are an emerging field in which the DOD and the intelligence community are highly integrated with the private sector and where contractors perform mission critical functions. In 2017, the United States government authorized $19.8 billion in unclassified spending for all cyber related activities performed by defense contractors, an increase of 120 percent over 2012 levels.8 Scholars have advanced several typologies to classify varying types of cyber operations. While academic debate in this area is likely to persist, there is emerging consensus that distinct differences exist among cybersecurity—which includes defensive cyber operations,9 offensive cyber operations, and data analytics.10 What follows is an analysis of outsourcing in these three strategically important cyber markets.

### Predictability---2AC

#### Predictability---it’s the most comprehensive definition for governmental policies.

USOSTP 09. United States. Office of Science and Technology Policy. Date: 2009?. “ Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure [open pdf - 710KB]” https://www.hsdl.org/?abstract&did=740047

"The President directed a 60-day, comprehensive, 'clean-slate' review to assess U.S. policies and structures for cybersecurity. Cybersecurity policy includes strategy, policy, and standards regarding the security of and operations in cyberspace, and encompasses the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure. The scope does not include other information and communications policy unrelated to national security or securing the infrastructure. The review team of government cybersecurity experts engaged and received input from a broad cross-section of industry, academia, the civil liberties and privacy communities, State governments, international partners, and the Legislative and Executive Branches. This paper summarizes the review team's conclusions and outlines the beginning of the way forward towards a reliable, resilient, trustworthy digital infrastructure for the future."

### CI---Security---2AC/1AR

#### “Security” in “cyber” includes deterrence.

NIST 21. National Institute of Standards and Technology. “Developing Cyber-Resilient Systems: A Systems Security Engineering Approach”. NIST Special Publication 800-160, Volume 2 Revision 1 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf

|  |  |
| --- | --- |
| security  [SP 800-160 v1] | Freedom from those conditions that can cause loss of assets with unacceptable consequences. |
| [ISO 15288] | Protection against intentional subversion or forced failure. A composite of four attributes – confidentiality, integrity, availability, and accountability – plus aspects of a fifth, usability, all of which have the related issue of their assurance. |
| [CNSSI 4009]  [SP 800-37] | A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise’s risk management approach. |

# 