## Topic Intro

The cyber security affirmative offers that we increase cooperation with the North Atlantic Treaty Organization (NATO) in cyber security. Currently the United States is a member of NATO, but has not made any efforts to include them in U.S. cyber security efforts or tried to join theirs. The United States is one of the strongest nations in the cyber space but is not the most protected. With the growing cyber-attacks from Russia, the U.S. needs to try to increase their security methods by cooperation with NATO. NATO is working on a new program for cyber protection and the U.S. should incorporate that in their own defenses.

The Biden Administration has made cyber security one of their top goals for the United States, and the AFF argues that working with NATO would fulfill that goal.

Video detailing the importance of cybersecurity:

<https://youtu.be/sdpxddDzXfE>

Interactive site with games and more information on cybersecurity:

<https://www.pbs.org/wgbh/nova/labs/lab/cyber/>

What is NATO: <https://www.youtube.com/watch?v=snXhtOpSXtI&ab_channel=NATO>

## Key Terms Glossary

**Cooperative security** (noun) - States working together to solve common problems

**NATO Industry Cyber Partnership** (noun)- A partnership between NATO alliance members to defend against cyber-attacks.

**The EU** (noun)- The European Union is a political and economic partnership between 27 countries, created after WWII. The EU promotes a common economic, social, and security leadership between its nations. Examples include a common currency between these nations, and the ability to travel within EU nations without needing to pass through customs again.

**Espionage** (noun)- Spying as a political or military strategy

**Traditional Military Deterrence** (noun)- A military strategy where one entity threatens the other with retaliation should they attack.

**International law** (noun)- International law consists of rules and principles governing the relations and dealings of nations with each other, as well as the relations between states and individuals, and relations between international organizations.

**NATO Strategic Concept document** (noun)- The Strategic Concept is a key document for the Alliance. It reaffirms NATO’s values and purpose, and provides a collective assessment of the security environment. It also drives NATO’s strategic adaptation and guides its future political and military development.

**Hypersonic Weapons** (noun)- Fast and low-flying missiles and projectiles which are too advanced to be detected by traditional missile defense systems.

**Quantum Computing** (noun)- An advanced emerging technology which would essentially make impossible problems solvable with data set algorithims, which would enable drastic progression in many fields.

**Voter intimidation** (noun)- Harassment at voting polls in attempt to scare individuals away from voting, usually towards POC or non-English speakers.

**Article 5** (noun)- This is what causes allyship between NATO members; when article 5 is invoked, if a member of NATO is victim of an, every other member will side with the victim and assist them.

**U.S. National Strategy for Global Supply Chain Security** (noun)- A strategy enacted by the Department of Homeland Security with the goals of efficient and secure moment of goods, and fostering a global supply chain system that is resilient against disruptions.

**Digital Colonialism** (noun)- Using technology for political, economic, or social domination of a targeted nation.

**CCDCOE** (noun)- The NATO Cooperative Cyber Defense Centre of Excellence is a research center meant to aid NATO alliance members in cyber defense, technology, operations, strategy, and law.

**ICT** (noun)- Information and Communications Techn

## Plan Text

The United States Federal Government should substantially increase its security cooperation with the North Atlantic Treaty Organization in cyber security.

### Contention 1: US/NATO Relations

**Scenario 1: Alliance**

**NATO and its allies depend heavily on a strong cyber defense**

#### North Atlantic Treaty Organization (NATO) March 23, 2022, <https://www.nato.int/cps/en/natohq/topics_78170.htm>

Cyber threats to the security of the Alliance are complex, destructive and coercive, and are becoming ever more frequent. NATO will continue to adapt to the evolving cyber threat landscape. NATO and its Allies rely on strong and resilient cyber defences to fulfil the Alliance’s core tasks of collective defence, crisis management and cooperative security. The Alliance needs to be prepared to defend its networks and operations against the growing sophistication of the cyber threats it faces. Cyber defence is part of NATO’s core task of collective defence. NATO Allies have affirmed that international law applies in cyberspace. NATO's main focus in cyber defence is to protect its own networks, operate in cyberspace (including through the Alliance’s operations and missions), help Allies to enhance their national resilience and provide a platform for political consultation and collective action. In July 2016, Allies reaffirmed NATO’s defensive mandate and recognised cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land and at sea. Allies also made a Cyber Defence Pledge in July 2016 to enhance their cyber defences, and have continued to bolster their national resilience as a matter of priority. NATO reinforces its cyber capabilities, including through education, training and exercises. Allies are committed to enhancing information-sharing and mutual assistance in preventing, mitigating and recovering from cyber attacks. NATO Cyber Rapid Reaction teams are on standby 24 hours a day to assist Allies, if requested and approved. At the 2018 NATO Summit in Brussels, Allies agreed to set up a Cyberspace Operations Centre as part of NATO’s strengthened Command Structure. They also agreed that NATO can draw on national cyber capabilities for operations and missions. In February 2019, Allies endorsed a NATO guide that sets out a number of tools to further strengthen NATO’s ability to respond to significant malicious cumulative cyber activities. NATO and the European Union (EU) are cooperating through a Technical Arrangement on Cyber Defence, which was signed in February 2016. In light of common challenges, NATO and the EU are strengthening their cooperation on cyber defence, notably in the areas of information exchange, training, research and exercises. NATO is intensifying its cooperation with industry through the NATO Industry Cyber Partnership. At the 2021 NATO Summit in Brussels, Allies endorsed a new Comprehensive Cyber Defence Policy, which supports NATO’s core tasks and overall deterrence and defence posture to enhance further the Alliance’s resilience. Allies are using NATO as a platform for political consultation, sharing concerns about malicious cyber activities and exchanging national approaches and responses, as well as considering possible collective responses. Allies are promoting a free, open, peaceful and secure cyberspace, and pursuing efforts to enhance stability and reduce the risk of conflict by supporting international law and voluntary norms of responsible state behaviour in cyberspace.

**U.S. cyber- security is currently weak against attacks**

Joseph Marks and Aaron Schaffer, June 6, 2022, Joseph Marks Education: Georgetown University, MS in Foreign Service; University of Wisconsin - Madison, BA in English, writes The Cybersecurity 202 newsletter focused on the policy and politics of cybersecurity. Before joining The Washington Post, Marks covered cybersecurity for Politico and Nextgov, a news site focused on government technology and security. He also covered patent and copyright trends for Bloomberg BNA and federal litigation for Law360. Aaron Schaffer is a technology and cybersecurity policy researcher Education: American University, MA in journalism and public affairs; University of Rochester, BA in international relations. Aaron Schaffer is a researcher for Technology 202 and Cybersecurity 202 <https://www.washingtonpost.com/people/aaron-schaffer/>

Our network of cyber experts have a less-than-rosy take on the United States' ability to fend off cyber attacks. Most of them said the U.S. is either just as vulnerable to cyberattacks or even more vulnerable today than it was five years ago. That assessment, from a group of experts polled by The Cybersecurity 202, reflects a half-decade during which government and industry have supercharged their efforts to defend against devastating hacks from foreign governments and criminals — but the bad guys have upped their game even more, most experts say. ‘[We’re] less vulnerable against the threats of five years ago. But I see no evidence that the threat has stood still, and in fact, it is likely that it has grown at a faster rate than our defenses,” said Herb Lin, senior research scholar for cyber policy and security at Stanford University. “We become evermore vulnerable with each passing day,” warned Lauren Zabierek, executive director of the Cyber Project at the Harvard Kennedy School’s Belfer Center. “I don't know where the bottom is.” The breakdown, About 43 percent of respondents to our Network experts poll said the United States is more vulnerable to cyberattacks now. About 38 percent said we’re just as vulnerable as we were five years ago. Just 19 percent of experts said the United States is less vulnerable in cyberspace than five years ago. The sobering results come as cyber executives and analysts are convening in San Francisco for the RSA Conference, the largest annual industry-focused cybersecurity gathering, which is being held in person for the first time since the start of the coronavirus pandemic. The cyber industry has fared extremely well during the past half-decade — nearly doubling in value, according to some estimates — but it has also struggled to keep up with the dizzying pace of attacks. More targets: One key problem, according to experts who said the United States is more vulnerable now: The nation has become more reliant on technology during the past five years — significantly increasing the targets that hackers can aim at. And that technology is often being built without security foremost in mind. “Cybersecurity is improving constantly, but the complexity of our digital society may be outpacing our efforts to keep up,” Mandiant Threat Intelligence chief John Hultquist said. Cyber and tech investor Niloofar Razi Howe: “We are more vulnerable because of the dizzying pace we are adopting technology, engaging in tech transformation, and adding devices without prioritizing security.”One particularly rich target has been a vast new array of Internet-connected devices, such as refrigerators, thermostats and cameras. These devices, commonly called the “Internet of things” or “IoT” are notorious for relying on weak or default passwords and being difficult to update with software patches — making them easy pickings for hackers.“Many of these technologies have shortchanged their cybersecurity expenditures, creating ever-increasing liabilities for everyone,” said Sascha Meinrath, founding director of X-Lab, a think tank at Penn State focusing on the intersection of technologies and public policy.“As the cyber-strategist Biggie Smalls would have said, ‘More IoT, More Problems,’ ” quipped Peter Singer, a fellow at the New America think tank. (Singer said the United States is equally vulnerable compared to five years ago). Many experts blamed the United States’ ongoing vulnerability to hacking on the increased brazenness of U.S. adversaries, especially Russia. Norma Krayem, a cyber policy expert at Van Scoyoc Associates: “Russia's use of cyber tools against Ukraine has clearly demonstrated to the world that it can fully disrupt key aspects of critical infrastructure.

This undermines alliance effectiveness for two reasons

**1—Unchecked attacks threaten alliance cohesion**

Kramer et al., Scowcroft Center Distinguished Fellow, ‘20

[Franklin D. Kramer, Distinguished Fellow, Scowcroft Center for Strategy and Security and Board Director, the Atlantic Council, Lauren Speranza, Director, Transatlantic Defense and Security, Center for European Policy Analysis, and Conor Rodihan, Assistant Director, Transatlantic Security Initiative, Scowcroft Center for Strategy and Security, “NATO Needs Continuous Responses in Cyberspace,” NEW ATLANTICIST, The Atlantic Council, 12—9—20, <https://www.atlanticcouncil.org/blogs/new-atlanticist/nato-needs-continuous-responses-in-cyberspace/>, accessed 5-23-22]

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.

**2—They also threaten NATO operations—facilitated by emerging vulnerabilities and the democratization of technology**

Bellasio & Silfversten, RAND analysts, ‘20

[Jacopo Bellasio, Senior Analyst, Defence, Security and Infrastructure, RAND Europe and Erik Silfversten, Co-Director, Centre for Futures and Foresight Studies, RAND Europe, “The Impact of New and Emerging Technologies on the Cyber Threat Landscape and Their Implications for NATO,” CYBER THREATS AND NATO 2030: HORIZON SCANNING AND ANALYSIS, ed. A.Ertan, K.Floyd, P.Pernik & T.Stevens, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), King’s College London, and William & Mary University, 2020, p. 99]

The technologies highlighted in this paper may contribute to the exacerbation of current trends in the cyber threat landscape and herald so-called grey swan scenarios.5 The increasing availability of powerful, easy-to-use and inexpensive technologies is likely to further stimulate the conduct of malicious activities by a wide array of state and non-state actors. The democratisation and ‘servitisation’6 of technology have enabled consumer access to a wide range of technologies that were previously accessible only by governments. This includes enabling technologies like additive manufacturing and largescale distributed computing, to more niche technological services such as ondemand development of bespoke software-defined radio applications that could be used for disrupting the electromagnetic environment. While most of these activities are likely to entail low-tech tactics, this trend could result in an even greater volume of malicious activities than currently witnessed.

The development of new, complex technological solutions and capabilities may also enable state-sponsored actors to conduct advanced, covert or persistent attacks and activities which could undermine or jeopardise NATO’s missions and day-to-day operations by, for example, exploiting unknown vulnerabilities in the NATO supply chain to gain access to sensitive information. Sophisticated and persistent attacks are likely to be less frequent, making these threats more challenging for NATO to identify, detect, prepare for and manage due to limited exposure to and knowledge of the tactics, techniques and procedures (TTP) employed. The proliferation of connected and embedded systems, particularly through a drive towards the Internet of Things (IoT) and the digitalisation of legacy infrastructure may also increase NATO’s attack surface and the likelihood of vulnerabilities that could be exploited by malicious actors.

**Infrastructure attacks are a unique terminal risk, threatening economic and societal collapse.**

Murphy 19 [Hannah, Tech Correspondent at Financial Times, 10-13-2019,   
“Companies urged to bolster infrastructure cyber defences,” Financial Times, <https://www.ft.com/content/797e1e5e-ca53-11e9-af46-b09e8bfe60c0>, accessed 07/04/22, GDI-JCR]

Hackers have traditionally focused their attention on computer software, resulting in a mushrooming of cyber security companies that promise protections for office-based clients. But there is another, less well-known hacking threat: cyber attacks on big corporate operations, such as **manufacturing facilities or power plants, as well as other vital infrastructure.** Such attacks are becoming more commonplace, fuelling concerns that companies should ramp up their efforts to guard against them. This is no small challenge. For companies with operational technology — the computerised systems used to control industrial operations — the risks of a breach are plentiful; disruptions to machinery processes could dent revenues or cause an accident. For those involved in “critical infrastructure” — the **dams, energy, oil and gas facilities** required for society to function smoothly — the risks are more dramatic and may attract nation state hackers, not just those seeking financial gain. “Our economy will disappear, society will collapse — and these things are possible,” says Sujeet Shenoi, professor of computer science at the University of Tulsa, who has been involved in multiple government-led critical infrastructure projects. “**There’s never been a war** in human history **where** the **critical infrastructure hasn’t been damaged**.” He notes that some 80 per cent of critical infrastructure in the US is privately run. “These companies are not prepared for [a cyber attack]. You need extremely well trained people,” he says, noting the many former government experts are moving into the sector. Historically, critical infrastructure and operational technology were kept separate from the computer networks typically used in corporate headquarters. However, those worlds are now converging as outdated analogue systems have become increasingly digitised. “Systems that have been developed over 30 or 40 years are having the internet introduced to them,” says Casey Ellis, founder and chief technology officer at Bugcrowd, a cyber security group. But **retrofitting systems** that were never intended to be on the internet **creates new opportunities for hackers**, he says. “The attack surface is expanding rapidly.” As with normal IT systems, ransomware and malware can be used to infect operational technology and critical infrastructure. The most high-profile worm was the 2010 Stuxnet malware, which targeted Iran’s nuclear facilities. Operations at the food company Mondelez and drugmaker Merck were disrupted by the ransomware dubbed NotPetya in 2017. Ukraine has suffered a spate of attacks on its power grid system recently, and earlier this year, Norwegian aluminium maker Norsk Hydro had to freeze operations earlier after it fell victim to ransomware. While the marketplace for cyber security companies offering support to such groups is smaller than the traditional IT security space, experts caution that companies should take action. Moves might include assessing company **systems to ensure staff know what devices are connected to the network,** testing and monitoring those systems, and devising a plan for worst-case scenarios. Above all, companies should isolate the most critical systems to ensure they can keep them operating no matter what, says Pedro Abreu, chief product and strategy officer at online security company Forescout, who dubs the process “containing the blast area”. “If a WannaCry [attack] happens, I want to [be able to] shut down that facility or country” while the rest of the network remains running, he says. Various sectors are equipped differently, experts say. Where deep-pocketed energy, and oil and gas groups have been able to pour investment into bolstering their protections, others, such as the water sector, are thought to be lagging. To their advantage, Michael Fabian, principal consultant at Synopsys, notes that operational technology systems are “very restrictive”, meaning that “some expertise is needed to hack [them]”. By comparison, “**people providing consumer services have a massive attack surface**,” he says, citing the likes of Citibank, Target or Amazon. Nevertheless, operational technology systems have their own nuances. First, testing them for vulnerabilities can be difficult because the systems are too sensitive or essential to pause. “There are things that are ultra critical that we can’t put at risk by testing them, but we are doing just that — putting them at risk — by not testing them,” says Charles Henderson, global head of IBM’s hacking unit X-Force Red. This means cyber security companies may have to test for vulnerabilities against a less reliable reproduction of an actual system. And if a problem is uncovered, it is harder to fix. “The life cycles of those systems in the field is extraordinarily long,” says Eric Cornelius, chief product officer at BlackBerry Cylance, a cyber security group. Moreover, even if cyber security companies offer solutions, it can be many years before a system can be updated. For example, many companies would opt to rebuild an offshore gas plant once it has finally stopped running, rather than upgrade at great cost, Mr Cornelius says.

**Economic downturn and fragmentation of world economy challenge LIO – and harms ability to deal with existential threats like climate change**

**Georgieva, IMF Managing Director, 2022**

[Kristalina “Facing Crisis Upon Crisis: How the World Can Respond” IMF, April 14, 2022 [https://www.imf.org/en/News/Articles/2022/04/14/sp041422-curtain-raiser-sm2022 accessed 7/7/22](https://www.imf.org/en/News/Articles/2022/04/14/sp041422-curtain-raiser-sm2022%20accessed%207/7/22) GDI -TM]

In economic terms, growth is down and inflation is up. In human terms, people’s incomes are down and hardship is up . These double crises—pandemic and war—and our ability to deal with them, are further complicated by another growing risk: fragmentation of the world economy into geopolitical blocs—with different trade and technology standards, payment systems, and reserve currencies. Such a tectonic shift would incur painful adjustment costs. Supply chains, R&D, and production networks would be broken and need to be rebuilt. Poor countries and poor people will bear the brunt of these dislocations. This fragmentation of global governance is perhaps the most serious challenge to the rules-based framework that has governed international and economic relations for more than 75 years, and helped deliver significant improvements in living standards across the globe. It is already impairing our capacity to work together on the two crises we face. And it could leave us wholly unable to meet other global challenges—such as the existential threat of climate change. It is a consequential moment for the international community. The actions we take now, together, will determine our future in fundamental ways. It reminds me of Bretton Woods in 1944 when, in the dark shadow of war, leaders came together to envision a brighter world. It was a moment of unprecedented courage and cooperation. We need that spirit today, as we face bigger challenges and more difficult choices.

#### **Strong relations are key to U.S. leadership and checking rising authoritarianism**

Nuland et al., Albright Stonebridge Group senior Counselor, ‘20

[Victoria Nuland, Senior Counselor, Albright Stonebridge Group, Non-Resident Senior Fellow, Brookings Institution, Christian Mölling, Director of Research of the German Council on Foreign Relations, and Sophia Becker, Research Fellow for U.S. Security and Defense Policy at the German Council on Foreign Relations, STRONGER TOGETHER: A STRATEGY TO REVIALIZE TRANSATLANTIC POWER, Belfer Center for Science and International Affairs, Harvard University and German Council on Foreign Relations (DGAP), 12—20, p. 27]

At its core, it is a resource question: Can the U.S. advance its global interests without Europe, or, more precisely, would a world without NATO and strong U.S.–EU relations be cheaper for the U.S. or for Europe? The answer is: no. One of the America’s greatest strategic advantages are its alliances and partnerships. From a European perspective, the most fundamental truth about NATO has not changed since 1949: Europe cannot yet guarantee its own security without the U.S., given the capability gaps in European armed forces. Nor can it address the myriad other security challenges it faces from China, to terrorism, to technological dependence to climate change without effective U.S.–EU cooperation. Finally, if the democratic world is going to mount a successful defense against authoritarian states’ efforts to rewrite global norms in their own favor, the family of NATO and EU nations must make up the core of that defense.

**A strong NATO is the cornerstone of global stability**

Burns, Harvard professor, ‘18

[Nicholas Burns, Barbara Goodman Family Professor of the Practice of Diplomacy and International Relations, Harvard Kennedy School, “Assessing the Value of the NATO Alliance,” Testimony before the Senate Foreign Relations Committee, 9—5—18, <https://www.belfercenter.org/publication/assessing-value-nato-alliance>, accessed 6-11-22]

Mr. Chairman and Mr. Menendez, you have asked for an assessment of NATO’s value to the United States. In my judgment, NATO continues to be of vital importance to American security interests in five principal ways. First, NATO is at the core of one of the most significant foreign policy accomplishments in American history—the creation of a long-term peace in Europe following the close of the Second World War. Because of NATO and the emergence of the European Union, Europe is united after centuries of division and war. NATO’s military strength has been a major reason for the absence of war with the Soviet Union and Russia since 1949. A recent Atlantic Council study reminds that America spent 14.1 percent of its GDP on defense during the First World War, 37.5 percent during the Second World War and 13.2 percent during the Korean Conflict. We spend nothing close to those levels now in large part due to the great power peace we have enjoyed for over seventy years. NATO has been a major factor in that peace. And due to the expansion of NATO and the European Union eastward after the fall of the Soviet Union, millions of East Europeans now live in free, democratic societies—a significant success for U.S. diplomacy. Second, NATO delivers additional benefits to U.S. military objectives and operations beyond our shores. NATO is at the heart of our defense of North America and Europe from nuclear and conventional threats. British and French nuclear weapons join ours in deterring aggression in the North Atlantic area. Since the late 1940s, every Administration has believed that the best way to defend our country is through American forces forward deployed in Europe with the NATO allies. This strategy remains right for today given Russia’s invasion of Georgia in 2008, of Crimea and Eastern Ukraine in 2014 and its current pressure on Estonia, Latvia, Lithuania and Poland. NATO remains our primary vehicle for deterring Putin in Eastern Europe. The NATO allies host a great number of critical bases for U.S. forces—Ramstein in Germany, Aviano in Italy, Rota in Spain, Souda Bay in Greece and Incirlik in Turkey—that serve as a platform for our presence in Europe, as well as for U.S. force projection against terrorist groups in North Africa and the Middle East and for our continued military operations in Afghanistan. Europe is a critical link in the development of our Ballistic Missile Defense network focused on the Middle East with Turkey, Romania, Poland, Germany, Spain, the Netherlands, Denmark, the UK and other allies all hosting elements of this system. NATO allies continue to participate in the U.S.-led coalition against the Islamic State in the Middle East. Many of the allies play lead roles in other counter terror operations such as French forces in Mali supported by the U.S. In Afghanistan, the NATO allies remain with us in combat operations and in training the Afghan military. Over 1000 soldiers from European and other partner nations have died there during the last seventeen years. NATO continues to maintain the hard-earned peace in Kosovo with European troops bearing the large share of the burden. An EU-led force has taken on all of the peacekeeping responsibility in Bosnia, freeing up the U.S. for other activities. Third, the NATO allies are among our closest and most supportive global partners as we confront the great transnational challenges that define this century—the fight against terrorism, the entire complex of cyber threats, climate change, the risk of pandemics, mass migration and others. The NATO allies and our partners in the European Union act together with us on these and other issues. This is of incalculable benefit to the U.S. Neither Russia nor China have treaty allies. NATO is a significant advantage for the United States when it acts as a force multiplier for American interests.

**Scenario 2 Russia**

**Simple U.S. deterrence does not work,**

Center for International Maritime Security May 11,2022 <https://cimsec.org/in-cyberspace-no-one-can-hear-you-bluff/>

General Paul Nakasone – Commander, U.S. Cyber Command (USCC) and Director, National Security Agency (NSA) – asserts that “traditional military deterrence is binary in regard to conflict and a deterrence model…does not comport to cyberspace where much of the nefarious cyber activity plays out non-stop in an ambiguous strategic gray zone.” While this article is in agreement with the “futility of totally deterring adversaries from operating in cyberspace and instead actively disrupting those activities before they can inflict damage,” it takes the position of respectfully disagreeing that traditional deterrence is binary and the rules of traditional deterrence do not hold in cyberspace. Deterrence centered around domain denial is neither desirable nor sustainable. Hindering access to cyberspace is not consistent with the enduring American values of individual liberty, free expression, and free markets. This encumbered access also runs counter to the U.S. national interest of protecting and promoting internet freedom to support the free flow of information that enhances international trade and commerce, fosters innovation, and strengthens both national and international security; and the universal right (global norm) of unfettered free access to and peaceful use of cyberspace for all. Restricting access to cyberspace is also not practical considering the cost to operate in cyberspace is modest, the barriers to entry low, and the ease of operating negligible. Deterrence, the “prevention of action by either the existence of a credible threat of unacceptable counteraction and/or belief that the costs of action outweigh the perceived benefits,” is more complicated and nuanced than a simple binary response of yes or no. Deterrence can create a delay or pause for transitory maneuvering space to mitigate the effects of the threat action, or better yet, take preemptive or preventive measures to disrupt (neutralize) the threat action. Deterrence, like warfighting (war), involves universal and immutable “human nature” that does not change over time or across nationality, demographic, culture, geography, and domain. Rational actors choose to act or not to act based on fundamental “fear, honor, and interest (Thucydides)” and are deterred to act or not to act by real or perceived “capability, intent, and credibility (deterrent triad).” Additionally, as Henry Kissinger once noted, “deterrence is a product of capability, intent, and credibility and not a sum…if any one of them is zero, deterrence fails.” Washington accordingly must do more and do better to ensure each factor succeeds as an aggregate deterrent triad for increased integrated deterrence, decreased strategic risk, greater strategic alignment, and lesser likelihood of conflict across all the interconnected and contested domains. Deterrence works best when it is clear, coherent, uniform, and complementary across the fluid competition continuum (steady state to crisis to conflict); expansive instruments of national power (diplomatic, information, military, economic, financial, intelligence, and law enforcement – DIMEFIL); and interconnected and contested domains (physical and nonphysical) for strategic consistency, operational agility, and tactical flexibility. Last year in an article titled “In Space, No One Can Hear You Bluff,” this author made the policy case for a more active space deterrence to better manage the growing threats to the vulnerable U.S. high-value space assets. This article makes the same policy case now for a more active cyber deterrence to better address the exigent factors of time, space, and force in cyberspace. An attack in cyberspace can come from anyone, occur anywhere, and happen anytime with no warning to react and no opportunity to respond – an increasing real risk as the ongoing Russian invasion of Ukraine persists and President Putin becomes more impatient and desperate for victory while becoming at risk of dangerously perceiving a shift in U.S. policy from conflict containment (vertical and horizontal) to conflict escalation, or worse, regime change.

**Russia is pursuing a hybrid warfare strategy to weaken the alliance and undermine the U.S.-led international order**

Speranza, Center for European Policy Analysis director, ‘20

[Lauren Speranza, Director, Trans-Atlantic Defense and Security, Center for European Policy Analysis, “A Strategic Concept for Countering Russian and Chinese Hybrid Threats,” Scowcroft Center for Strategy and Security, Atlantic Council, 7—20, p. 13-15]

For Russia, hybrid warfare is a set of means for it to roll back the post-Cold War settlement and undermine the predominantly US-led, rules-based international order to regain clout as a major player on the global stage. The Kremlin’s key objectives to that end include: dividing and weakening NATO and the EU, both of which the Kremlin sees as a threat; subverting pro-Western governments and institutions; promoting pro-Russia policies; expanding Russia’s sphere of influence (geographically, economically, politically, etc.); and establishing a “moral equivalence” between Russia and the West.3 Moreover, hybrid activities help the Kremlin pursue these goals in a more effective and realistic way. Its leaders recognize Russia cannot necessarily counter or outright compete with the West militarily, technologically, or economically. By employing hybrid methods as part of an overarching strategy of intimidation, however, the Kremlin can have significant influence over international affairs.4

Russia’s hybrid toolkit is multi-level and often country specific, which has made it highly effective and difficult to combat. In its most widely known example, Russia used below-threshold force to illegally invade eastern Ukraine and annex Crimea. The Kremlin has also used proxies and privately contracted forces to influence the outcome of conflicts abroad, from Syria to Libya. Other examples of Russia’s low-level uses of force include attempted assassinations of pro-Western leaders and the use of deadly chemical attacks to target political enemies on foreign soil. In terms of cyber and operational activities, Russia has conducted reckless and dangerous cyberattacks, infiltrated critical infrastructure in the United States, and manipulated gas pipelines, electric grids, and financial systems in Eastern Europe and beyond to increase its leverage abroad.

With respect to political subversion and economic coercion, Russia has interfered in elections in the United States and across Europe in attempts to divide transatlantic populations and influence the outcomes toward candidates the Kremlin views as favorable to Russia. Other tools and tactics include: bribing officials in foreign countries; financing anti-European parties in Central and Eastern Europe to promote pro-Russian narratives; and investing in strategic sectors in foreign countries to maximize dependency on Russia. On the information-warfare front, the Kremlin has orchestrated widespread disinformation campaigns and strategic hack-and-release efforts designed to sow doubt, create chaos, and sway public opinion in its favor on key policy issues.

While Russian hybrid activities can be traced much further back than these examples—including to the major cyberattacks in Estonia in 2007 and the Russo-Georgia conflict in 2008—they have been steadily increasing since the Kremlin’s illegal annexation of Crimea in 2014. Looking ahead, several elements could impact the future course of Russia’s hybrid actions. First are the constitutional changes that Russian President Vladimir Putin has pushed through national courts to reset presidential term limits.5 The reforms allow Putin to remain in power until 2036, or possibly for life, pending a final national referendum.6 With his grip on power soon to be cemented, Putin is likely to attempt more aggressive hybrid actions, knowing the domestic political risks for him are low.

Another factor is the 2020 coronavirus pandemic, which has triggered a global recession and a drastic decline in demand for oil so critical to Russia’s energy-reliant economy. In early 2020, Russia and Saudi Arabia, the world’s biggest crude producers, failed to agree to mutual production cuts in response to the crisis, fueling a price war that further hurt Russia’s economy.7 Economic, public health, and social pressures inside Russia could push the Kremlin to temporarily scale back its ambitions in the short term. However, at the same time, uncertainty and anxiety around the pandemic could create more fertile conditions for Russia’s hybrid activities beyond its borders, especially as Euro-Atlantic governments take extraordinary domestic measures to respond.8 In the long term—even as the pandemic subsides, oil prices rebound, and the global economy begins to recover—conditions will remain difficult for Russia, whose economy has suffered from stagnation and sanctions from the West. These dynamics may lead Putin to be more assertive with hybrid strategies abroad with the aim of appealing to nationalist sentiments at home in order to quell domestic political tensions.

Further emboldening Putin is the lack of traditional US leadership and pushback that has helped to keep Russia in check. US President Donald Trump has instead tried to appeal to Putin, describing his own policy as “getting along with Russia” and reducing perceived or actual consequences of hybrid actions against the United States. Political allegations of the Trump campaign “colluding” with Russia to affect US elections9 have further divided the American public toward Russian aims, creating more fertile ground for the Kremlin’s malign influence.10 Compounding this is fraying transatlantic solidarity, whether the USGermany feud over defense spending or French President Macron’s comments that NATO is “braindead.”11 These divisions not only constrain the West’s response to Russia’s hybrid actions, but also expose cracks in the Alliance that Putin is all too eager to exploit.

Together, these factors indicate that as long as Putin remains in power, the Kremlin will likely continue escalating hybrid activities, short of an all-out war with NATO, to push boundaries and test what is acceptable going forward. In the relative near term, the transatlantic community must plan according to Russia’s current trajectory on hybrid issues, which demands a more proactive and widespread approach.

#### **The threat is large and growing—Ukraine proves the brink**

Maigre, 2022

[Merle, senior cybersecurity expert at e-Governance Academy in Estonia. In 2017–2018, she served as director of the NATO Cooperative Cyber Defence Center of Excellence (CCDCOE), “NATO IN A NEW ERA: GLOBAL SHIFTS, GLOBAL CHALLENGES NATO’s Role in Global Cyber Security” German Marshal Fund APRIL 06, 2022 <https://www.gmfus.org/news/natos-role-global-cyber-security> accessed jcp-TM 6/8]

Introduction

What the war in Ukraine says about cyber power is yet not entirely cleared from the fog of war. Many aspects remain uncertain, but given the unpredictability of the Putin regime, the risk of an escalation in hostile cyber exchanges between Russia and NATO states remains high. What is clear is that, as of February 24, 2022, we live in a different world in which the European and global security orders have been shattered. This brief first explores the challenge that cyber threats pose to NATO allies and how the rapidly evolving cyber-threat landscape can alter the inter- national security environment. Secondly, it looks at developments in cyber defense policy within NATO. Finally, the brief analyzes how NATO needs to adapt to address cyber challenges, studying how allies align their sovereign interests, capabilities, and cyber doctrines with NATO operational requirements and strategic ambitions. NATO is set to issue strategic documents in 2022 that will guide the next decade of its military planning. This will certainly require more transatlantic consultation on political-military matters with an emphasis on cyber security and cyber defense. The Cyber Challenge to the World and NATO Allies Malicious cyber activity has increased substantially over the past years while the world has kept turning amid the omnipresent pandemic and now war in Ukraine. States, non-state actors, and criminal groups compete and are increasingly weaponizing sensitive information and infiltrating other countries’ networks to steal data, seed misinformation, or disrupt critical infrastructure.

The coronavirus pandemic further complicated the cyber-threat landscape. In March 2020, attempts to mitigate the spread of the coronavirus led to social distancing measures, travel restrictions, and remote work. In a short span of time, IT security profes- sionals had to respond to the challenges of working from home, such as enterprise data movements when employees accessed cloud-based apps via their home internet, corporate software, videoconferencing, and file sharing.1 Even if hardware and software solutions were in place to secure the organization’s data, there were often no established policies to help employees wade through the jungle of threats and vulnerabilities they faced when moving their workplace out of the traditional office environment.2 According to the FireEye Mandiant Special Report: M-Trends 2021, the top five most targeted indus- tries in 2020 were business and professional services, retail and hospitality, finance, healthcare, and high technology. The main methods used were extortion, ransom demands, payment card theft, and illicit trans- fers. Direct financial gain was the likely motive for 36% of intrusions, and an additional 2% of intrusions were likely perpetrated to resell access. In 2021, data theft remained an important mission objective for threat actors; in 32% of intrusions, adversaries stole data.3 Currently, highly organized, technically proficient criminal syndicates comprise the most significant cyber threat to allies. These groups try to steal data or extort money through ransomware. In 2021, promi- nent ransomware attacks struck Colonial Pipeline, the operator of the largest fuel pipeline on the East Coast of the United States; JBS, the largest meat processing company in North America; and Coop, a major supermarket chain in Sweden. Healthcare was also targeted—in May of the same year, the entire health service system of Ireland was disrupted for weeks, and over the spring and summer, dozens of hospitals in Europe and the United States were locked out of life-critical systems by ransomware attacks.4 Another set of threats comes in the form of bellig- erent state actors that seek to steal sensitive data for espionage. In December 2020, Russian intelligence services infiltrated the digital systems run by US tech firm SolarWinds and inserted malware into its code. During the company’s next software update, the virus was inadvertently spread to about 18,000 clients, including large corporations, the Pentagon, the State Department, Homeland Security, the Treasury, and other US government agencies. The hack went unde- tected for months before the victims discovered vast amounts of their data had been stolen.5 There are also politically motivated cyberattacks mandated by states that interfere in democratic processes and political discourse. In September 2020, the internal email system of Norway’s parliament was hacked.6 Ine Eriksen Søreide, the Minister of Foreign Affairs of Norway, underlined the significance of the attack by calling it an important cyber incident that affected the “most important democratic institution” of the country.7 Norwegian authorities later identified Russia as the actor responsible for the attack, marking the first time that Norwegian authorities had made a political attribution to such an attack. Since the beginning of this year, Ukraine’s govern- ment has been hit by a series of cyberattacks that defaced government websites and wiped out the data on some government computers. In mid-Jan- uary, hackers defaced about 70 Ukrainian websites, including the Ministries of Foreign Affairs, Defense, Energy, Education, and Science, as well as the State Emergency Service and the Ministry of Digital Trans- formation, whose e-governance portal gives the Ukrainian public digital access to dozens of govern- ment services. The hackers replaced the home pages of about a dozen sites with a threatening message: “be afraid and expect worse.” After a couple of days,however, most of the sites were restored.8 The inter- national hacktivist collective Anonymous has declared “cyberwar” against Russia’s government, claiming credit for several cyber incidents including distrib- uted denial of service attacks that took down Russian government websites and Russia Today, the state- backed news service.9 Around the globe, aging critical infrastructure has long been vulnerable to attack. The most worrying type of cyberattack is sophis- ticated malware designed by states or state-backed actors that act as “time bombs” in the critical cyber networks of target countries, such as the energy, telecom, and transportation sectors. Around the globe, aging critical infrastructure has long been vulnerable to attack. In 2020, the UK’s National Cyber Security Centre issued a warning of Russian attacks on millions of routers, firewalls, and devices used by infrastruc- ture operators and government agencies.10 On the day of the Russian invasion, ViaSat, a provider of high-speed satellite broadband services, was hacked along with one of its satellites Ka-Sat, whose users included Ukraine’s armed forces, police, and intelligence service. Destructive wiper malware attacks by Russia against Ukraine included Whisper- Gate, discovered in January by Microsoft, in Ukraine’s networks that “provide critical executive branch or emergency response functions”;11 HermeticWizard and IsaacWiper,12 targeting multiple Ukrainian orga- nizations just hours before the Russian invasion began; and CaddyWiper, spotted by researchers at the Slovak internet security company ESET in mid-March.13 All of them were designed to wipe or overwrite critical files on infected systems and leave computer hard drives corrupted and unrecoverable. These incidents demonstrate that, in the words of cyber expert and Silverado Policy Accelerator think tank chairman Dmitri Alperovich, “Cyberattacks have become a theater for great-power conflict in which governments and militaries fight in the hybrid ‘gray zone,’ where the boundaries between peace and war are blurred.”14 The actors navigate a complex web of ambiguous and deeply interconnected challenges, where cyberattacks are not a separate front, but rather an extension of the conflict.

#### **Ukraine war increases risk of nuclear war and showcases fragility of deterrence strategies**

**Tannenwald,** a senior lecturer in political science at Brown University , **2022**

[Nina, “Is Using Nuclear Weapons Still Taboo? The world is starting to forget the realities of nuclear weapons” Foreign Policy JULY 1, 2022,<https://foreignpolicy.com/2022/07/01/nuclear-war-taboo-arms-control-russia-ukraine-deterrence/> accessed july 4 GDI-TM]

In March 1990, the New Yorker published a cartoon by Jack Ziegler that captured the optimism at the end of the Cold War. The cartoon shows an executive sitting at his desk as a worker enters the office carrying a large bomb with fins. “Bring that H-bomb over here, will you, Tom, and just slip it into my ‘out’ box,” the executive says. “Sure thing, boss!” the worker responds.

The image of putting nuclear bombs “in the outbox” was emblematic of the hope many had that a new era of cooperation between the United States and the former Soviet Union was emerging. The fear of a nuclear war breaking out between the world’s two superpowers receded, and many hoped that nuclear weapons, although they would still exist, would no longer be central to international politics. Mikhail Gorbachev, the Soviet Union’s last leader, declared in June 1991 that “the risk of a global nuclear war has practically disappeared.”

Today, more than 30 years later, nuclear bombs are back in the inbox. Fear of nuclear war between the United States and Russia has returned with a vengeance. As a result of Russia’s brutal invasion of Ukraine and Russian officials’ alarming nuclear threats, the world is closer to the use of nuclear weapons out of desperation—or by accident or miscalculation—than at any time since the early 1980s.

The Russia-Ukraine war serves as a harsh reminder of some old truths about nuclear weapons: There are limits to the protection nuclear deterrence provides. (Usable conventional weapons may get you more protection.) In a crisis, deterrence is vulnerable, not automatic and self-enforcing. There is always the chance that it could fail

#### **US Russia war massive and goes nuclear – prioritize this impact because cognitive bias underestimates it, and deterrence can’t solve it.**

Beebe 19 [George, VP and Director of Studies at the Center for the National Interest, a nonpartisan think tank, former head of Russia analysis at the CIA, “We’re More at Risk of Nuclear War With Russia Than We Think,” October 7, *Politico*, <https://www.politico.com/magazine/story/2019/10/07/were-more-at-risk-of-nuclear-war-with-russia-than-we-think-229436>, accessed 07/04/22, GDI-JCR]

Today, that old dread of disaster has all but disappeared, as have the systems that helped preclude it. But the actual threat of nuclear catastrophe is much greater than we realize. Diplomacy and a desire for global peace have given way to complacency and a false sense of security that nuclear escalation is outside the realm of possibility. That leaves us unprepared for—and highly vulnerable to—a nuclear attack from Russia. The most recent sign of American complacency was the death, a few weeks ago, of the Intermediate-Range Nuclear Forces Treaty—a pivotal 1987 agreement that introduced intrusive on-site inspection provisions, destroyed an entire class of dangerous weaponry, and convinced both Washington and Moscow that the other wanted strategic stability more than strategic advantage. The New START treaty, put in place during the Obama administration, appears headed for a similar fate in 2021. In fact, nearly all the key U.S.-Russian arms control and confidence-building provisions of the Cold War era are dead or on life support, with little effort underway to update or replace them. Meanwhile, U.S. officials from both parties are focused not on how we might avoid nuclear catastrophe but on showing how tough they can look against a revanchist Russia and its leader, Vladimir Putin. Summit meetings between White House and Kremlin leaders, once viewed as opportunities for peace, are now seen as dangerous temptations to indulge in Munich-style appeasement, the cardinal sin of statecraft. American policymakers worry more about “going wobbly,” as Margaret Thatcher once put it, than about a march of folly into inadvertent war. President Donald Trump’s suggestion that the United States and Russia might explore ways to manage their differences diplomatically has produced mostly head-scratching and condemnation. In my more than 25 years of government experience working on Russia matters, I’ve seen that three misguided assumptions underlie how the United States got to this point. The first is that American policymakers think that because neither side wants nuclear war, then such a war is very unlikely to occur. Russia would be foolish, we reason, to cross swords with the powerful U.S. military and risk its own self-destruction, and many Americans find it hard to imagine that modern cyber duels, proxy battles, information operations and economic warfare might somehow erupt into direct nuclear attacks. If the Cold War ended peacefully, the thinking goes, why should America worry that a new shadow war with a much less formidable Russia will end any differently? But wars do not always begin by design. Just as they did in 1914, a vicious circle of clashing geopolitical ambitions, distorted perceptions of each other’s intent, new and poorly understood technologies, and disappearing rules of the game could combine to produce a disaster that neither side wants nor expects. In fact, cyber technologies, artificial intelligence, advanced hypersonic weapons delivery systems and antisatellite weaponry are making the U.S.-Russian shadow war much more complex and dangerous than the old Cold War competition. They are blurring traditional lines between espionage and warfare, entangling nuclear and conventional weaponry, and erasing old distinctions between offensive and defensive operations. Whereas the development of nuclear weaponry in the Cold War produced the concept of mutually assured destruction and had a restraining effect, in the cyber arena, playing offense is increasingly seen as the best defense. And in a highly connected world in which financial networks, commercial operations, media platforms, and nuclear command and control systems are all linked in some way, escalation from the cyber world into the physical domain is a serious danger. Cyber technology is also magnifying fears of our adversaries’ strategic intentions while prompting questions about whether warning systems can detect incoming attacks and whether weapons will fire when buttons are pushed. This makes containing a crisis that might arise between U.S. and Russian forces over Ukraine, Iran or anything else much more difficult. It is not hard to imagine a crisis scenario in which Russia cyber operators gain access to a satellite system that controls both U.S. conventional and nuclear weapons systems, leaving the American side uncertain about whether the intrusion is meant to gather information about U.S. war preparations or to disable our ability to conduct nuclear strikes. This could cause the U.S. president to wonder whether he faces an urgent “use it or lose it” nuclear launch decision. It doesn’t help that the lines of communication between the United States and Russia necessary for managing such situations are all but severed.

### Contention 2: Liberal Order

**Scenario 1: Misinformation**

#### Hackers have broken into real news sites and planted stories

Andy Greenburg, July 29, 2020 Andy Greenberg is a senior writer for WIRED, covering security, privacy, and information freedom. He’s the author of the forthcoming book Tracers in the Dark: The Global Hunt for the Crime Lords of Cryptocurrency. His last book was Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers. The book and excerpts from it published in WIRED won a Gerald Loeb Award for International Reporting, a Sigma Delta Chi Award from the Society of Professional Journalists, two Deadline Club Awards from the New York Society of Professional Journalists, and the Cornelius Ryan Citation for Excellence from the Overseas Press Club. <https://www.wired.com/story/hackers-broke-into-real-news-sites-to-plant-fake-stories-anti-nato/>

OVER THE PAST few years, online disinformation has taken evolutionary leaps forward, with the Internet Research Agency pumping out artificial outrage on social media and hackers leaking documents—both real and fabricated—to suit their narrative. More recently, Eastern Europe has faced a broad campaign that takes fake news ops to yet another level: hacking legitimate news sites to plant fake stories, then hurriedly amplifying them on social media before they’re taken down. On Wednesday, security firm FireEye released a report on a disinformation-focused group it’s calling Ghostwriter. The propagandists have created and disseminated disinformation since at least March 2017, with a focus on undermining NATO and the US troops in Poland and the Baltics; they’ve posted fake content on everything from social media to pro-Russian news websites. In some cases, FireEye says, Ghostwriter has deployed a bolder tactic: hacking the content management systems of news websites to post their own stories. They then disseminate their literal fake news with spoofed emails, social media, and even op-eds the propagandists write on other sites that accept user-generated content. That hacking campaign, targeting media sites from Poland to Lithuania, has spread false stories about US military aggression, NATO soldiers spreading coronavirus, NATO planning a full-on invasion of Belarus, and more. “They’re spreading these stories that NATO is a danger, that they resent the locals, that they’re infected, that they’re car thieves,” says John Hultquist, director of intelligence at FireEye. “And they’re pushing these stories out with a variety of means, the most interesting of which is hacking local media websites and planting them. These fictional stories are suddenly bona fide by the sites that they’re on, and then they go in and spread the link to the story.”FireEye itself did not conduct incident response analyses on these incidents and concedes that it doesn't know exactly how the hackers are stealing credentials that give them access to the content management systems that allow posting and altering news stories. Nor does it know who is behind the string of website compromises, or for that matter the larger disinformation campaign that the fake stories are a part of.

#### **Fake news is driving a false wedge between countries**

Andy Greenburg, July 29, 2020 Andy Greenberg is a senior writer for WIRED, covering security, privacy, and information freedom. He’s the author of the forthcoming book Tracers in the Dark: The Global Hunt for the Crime Lords of Cryptocurrency. His last book was Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers. The book and excerpts from it published in WIRED won a Gerald Loeb Award for International Reporting, a Sigma Delta Chi Award from the Society of Professional Journalists, two Deadline Club Awards from the New York Society of Professional Journalists, and the Cornelius Ryan Citation for Excellence from the Overseas Press Club. <https://www.wired.com/story/hackers-broke-into-real-news-sites-to-plant-fake-stories-anti-nato/>

But the company’s analysts have found that the news site compromises and the online accounts used to spread links to those fabricated stories, as well as the more traditional creation of fake news on social media, blogs, and websites with an anti-US and anti-NATO bent, all tie back to a distinct set of personas, indicating one unified disinformation effort. FireEye’s Hultquist points out that the campaign doesn’t seem financially motivated, indicating a political or state backer, and notes that the focus on driving a wedge between NATO and citizens of Eastern Europe hints at possible Russian involvement. Nor would it be the first time that Russian hackers planted fake news stories; in 2017, US intelligence agencies concluded that Russian hackers breached Qatar’s state news agency and planted a fake news story designed to embarrass the country’s leader and cause a rift with the US, though US intelligence never confirmed the Kremlin’s involvement."We can’t concretely tie it to Russia at this time, but it’s certainly in line with their interests," Hultquist says of the Ghostwriter campaign. "It wouldn’t be a surprise to me if this is where the evidence leads us." Much of the disinformation has focused on Lithuania, as DefenseOne reported late last year. In June 2018, for instance, the English-language, Baltic-focused news site the Baltic Course published a story claiming that a US Stryker armored vehicle had collided with a Lithuanian child on a bicycle, killing the child "on the spot." The same day, the Baltic Course posted a notice to the site that "hackers posted this news about the deceased child, which is FAKE!!! We thank our vigilant Lithuanian readers who reported on our Facebook page about fake new on site. We strengthened security measures."A few months later, the Lithuanian news site Kas Vyksta Kaune published a story stating that "NATO plans to invade Belarus," showing a map of how NATO forces in Polish and Baltic countries would enter the neighboring country. Kas Vyksta Kaune later acknowledged that the story was fake, and planted by hackers. Someone had used a former employee’s credentials to gain access to the CMS. Then in September of last year, another fake story was posted to the site about German NATO soldiers desecrating a Jewish cemetery, including what FireEye describes as a photoshopped image of a military vehicle with a German flag visible behind the cemetery. More recently, the fake stories have attempted to exploit fears of Covid-19. One story posted to both Kas Vyksta Kaune and the English-language Baltic Times in January claimed that the first Covid-19 case in Lithuania was a US soldier who was hospitalized in critical condition, but only after he "visited public places and participated in city events with child and youth participation," according to the Baltic Times version of the story. In April and May of this year, the focus turned toward Poland: A fake story was posted across several Polish news sites in which a US official disparaged local Polish forces as disorganized and incompetent. This time the campaign went even beyond news sites. A fake letter from a Polish military official was posted to the Polish Military Academy website, calling on the Polish military to cease military exercises with the US, decrying the US "occupation" of Poland, and calling the exercises an "obvious provocation" of Russia. The Polish government quickly called out the letter as fake. FireEye's finding that all of those operations to plant fake news were carried out by a single group comes on the heels of a report from The New York Times that Russia's military intelligence agency, the GRU, has been coordinating the publication of disinformation on sites like InfoRos, OneWorld.press, and GlobalResearch.ca. US intelligence officials speaking to the Times said that disinformation campaign, which included false reports that Covid-19 originated in the US, was specifically the work of the GRU's "psychological warfare unit," known as Unit 54777.Given the GRU's role in meddling in the 2016 presidential election, including its hack-and-leak operations against the Democratic National Committee and the Clinton Campaign, any GRU role in more recent disinformation raises fears that it may be targeting the 2020 election as well. While FireEye has made no such claims that the Ghostwriter news site compromises were the work of the GRU, Hultquist argues that the incidents in Poland and the Baltics should nonetheless serve as a warning. Even if false stories are spotted quickly and taken down, they could have a significant temporary effect on public opinion, he warns.

***Coronavirus impacts are made worse by weak cyber security efforts***

#### Merle Maigre, April 6, 2022 Merle Maigre is the senior cybersecurity expert at e-Governance Academy in Estonia. In 2017–2018, she served as director of the NATO Cooperative Cyber Defence Center of Excellence (CCDCOE)in Tallinn; in 2012–2017 as the security policy adviser to Estonian Presidents Kersti Kaljulaid and Thoomas Hendrik Ilves; and in 2010–2012 in the Policy Planning Unit of the Private Office of NATO Security General Anders Fogh Rasmussen. She is a member of the Executive Board of the Cyber Peace Institute in Geneva and the International Advisory Board of NATO CCDCOE. This brief is part of a project at the German Marshall Fund supported by the Norwegian Ministry of Foreign Affairs. <https://www.gmfus.org/news/natos-role-global-cyber-security>

The coronavirus pandemic further complicated the cyber-threat landscape. In March 2020, attempts to mitigate the spread of the coronavirus led to social distancing measures, travel restrictions, and remote work. In a short span of time, IT security professionals had to respond to the challenges of working from home, such as enterprise data movements when employees accessed cloud-based apps via their home internet, corporate software, videoconferencing, and file sharing.[1](https://www.gmfus.org/news/natos-role-global-cyber-security#footnote1_fhsuz62)  Even if hardware and software solutions were in place to secure the organization’s data, there were often no established policies to help employees wade through the jungle of threats and vulnerabilities they faced when moving their workplace out of the traditional office environment.[2](https://www.gmfus.org/news/natos-role-global-cyber-security#footnote2_j09lbjl) According to the FireEye Mandiant Special Report: M-Trends 2021, the top five most targeted industries in 2020 were business and professional services, retail and hospitality, finance, healthcare, and high technology. The main methods used were extortion, ransom demands, payment card theft, and illicit transfers. Direct financial gain was the likely motive for 36% of intrusions, and an additional 2% of intrusions were likely perpetrated to resell access. In 2021, data theft remained an important mission objective for threat actors; in 32% of intrusions, adversaries stole data.[3](https://www.gmfus.org/news/natos-role-global-cyber-security#footnote3_jbmz5mx)Currently, highly organized, technically proficient criminal syndicates comprise the most significant cyber threat to allies. These groups try to steal data or extort money through ransomware. In 2021, prominent ransomware attacks struck Colonial Pipeline, the operator of the largest fuel pipeline on the East Coast of the United StRates; JBS, the largest meat processing company in North America; and Coop, a major supermarket chain in Sweden. Healthcare was also targeted—in May of the same year, the entire health service system of Ireland was disrupted for weeks, and over the spring and summer, dozens of hospitals in Europe and the United States were locked out of life-critical systems by ransomware attacks.

#### **Misinformation is an existential threat—makes it impossible to solve the many challenges facing us**

Lin, CISC Senior Research Scholar, ’19

[Herbert Lin, Senior Research Scholar, Center for International Security and Cooperation and Fellow, Hoover Institution, Stanford University, “The Existential Threat from Cyber-Enabled Information Warfare,” BULLETIN OF THE ATOMIC SCIENTISTS v. 75 n. 4, 2019, p. 189-194]

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

On human cognition

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

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

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

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

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

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

Maintenance of an individual’s social identity is an important influence on his or her invocation of System 1 or System 2 thinking. Evidence suggests that individuals tend to adopt the views of the peer groups that are most salient to them, even if the “objective” or “factual” information available to them contradicts those views. (Asch 1951 performed the classic “conformity experiments” that demonstrated this phenomenon in the early 1950s.) Uncritical System 1 thinking is active in processing information that is consonant with the beliefs and attitudes of those peer groups. Critical and skeptical System 2 thinking is active in processing information that is dissonant to those groups’ beliefs. These effects (that individuals tend to accept salient group norms) are even more pronounced in an anonymous environment, such as that which characterizes much online interaction (Postmes et al. 2001). Lastly, there is evidence that emotion and motivation affect cognition. For example, people who are angry tend to rely more heavily on simple heuristic cues (suggestive of System 1 thinking) than those who are not angry (Bodenhausen, Sheppard, and Kramer 1994). Individuals are more likely to stereotype people (a form of System 1 thinking) when that stereotype is consistent with their desired impression of those people; conversely, when the stereotype is inconsistent with their desired impression, individuals tend to inhibit the use of this stereotype (Kunda and Sinclair 1999). Negative emotions (such as those induced by the receipt of information incongruent with a person’s prior beliefs) can improve the ability of a person to reason logically, thus enabling him or her to negate or discount that information (Goel and Vartanian 2011). In the new information environment, exploitation of human cognitive architecture and capabilities – which are largely unchanged from what existed millennia ago – provides the 21st century information warrior with cyber-enabled capabilities that Hitler, Stalin, Goebbels, and McCarthy could have only imagined. By exploiting cognitive limitations, the perpetrators of cyber-enabled information warfare have learned to exacerbate prejudices, biases, and ideological differences; to add heat but no light to political discourse; and to spread widely believed “alternative facts” in advancing their political positions. Russian interference in the 2016 US presidential election has dominated news headlines ever since. But interference by authoritarian countries in the elections of democratic states – as undesirable and threatening as it may be – is hardly the only negative consequence of cyber-enabled information warfare. The problems of nuclear war and climate change are hard enough to solve even when well-intentioned, well-informed parties on all sides share a basic understanding and knowledge of the relevant facts. Yes, they may have different values and different priorities, may act under different constraints, and be able to bring to bear different levels of resources to these problems. But without shared, fact-based understandings of the blast, thermal, and radiation effects of nuclear explosions, what hope is there for national leaders to reach agreements to reduce the threat of nuclear holocaust [war] or to make good decisions about nuclear weapons use in times of crisis? Without shared, fact-based understandings that rising atmospheric carbon dioxide concentrations caused by human beings result in corresponding increases in global temperature and climatic disruption, what hope is there for national leaders to reach agreements to begin serious efforts at decarbonizing their economies?

Climate change denialism Climate change denialism can be fairly characterized as cyber-enabled information warfare against the reality of large-scale anthropogenically-induced climate change. In the responses of people resistant to taking action to mitigate climate change, we see a number of psychological factors at work (Zaval and Cornwell 2016). For example, one key element of System 1 thinking is the availability heuristic, with which individuals tend to associate the likelihood of an event with the ease with which they can remember similar events in the past. But the long-term consequences of climate change are unprecedented in recorded human history and obviously people have no personal memories of unprecedented events. Moreover, climate change is a long-term process whose inexorable progression is easily masked by short-term fluctuations in local weather conditions. For example, public concerns about climate changes correlate with local weather conditions (Krosnick et al. 2006). Climate change deniers are also quick to flag for public attention days that are particularly cold as “evidence” that global warming is not occurring and thus, they claim, discrediting theories of climate change. This illustrates a bias known as attribute substitution, as Kahneman and Frederick (2002) describe, through which individuals substitute salient information (such as the cold temperature today) for information that is more relevant but harder to understand (such as information about global climate change).

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

To close this (merely illustrative) exploration of biases relevant to climate change denialism, the optimism bias suggests that people consider themselves exceptions when considering the likelihood of a negative event occurring. That is, bad things may happen to other people, but they won’t happen to me, even though I and those other people are similar in important and relevant ways. In a climate context, the bad things may involve sea level rise or heat waves – and the misperception that “others may suffer from such problems but I won’t” diminishes the power of personal concern as a driver for rational decision making. Connecting the operation of these cognitive biases to the affordances of modern information technologies is not difficult. For example, Roxburgh et al. (2019) demonstrate how the characteristics of specific weather events (e.g. hurricanes or snowstorms) and “short-term socio-political context can play a critical role in determining the lenses through which climate change is viewed.” Note especially the importance of “short-term socio-political context” – precisely the context that social media shapes. Elsasser and Dunlap (2013) noted the influential role of a variety of newspaper columnists in advancing denialist arguments and thus amplifying these arguments to a broad segment of the American public. Fewer in number then, essentially all columnists today (of all political leanings) have a social media presence that they use to publicize their work, and in many instances their online presence is driven in significant part by social media and reach many more readers online than in print. Furthermore, subtleties and nuances in their extended written pieces are likely to be lost when they are represented in social media. Another important element of climate change denialism is the easy accessibility of seemingly-authoritative information that casts doubt on the well-established science of climate change. As reported by The Guardian, a variety of largely secret funding sources distributed $118 million to 102 denialist organizations (Goldenberg 2013). Oreskes and Conway (2011) provide the definitive work on deliberate information campaigns to obscure the scientific truth on a range of issues from smoking to climate change. These denialist organizations have generated a variety of products for public and policy consumption (but – unsurprisingly – not many peer-reviewed scientific articles) that are easily accessible to the public, mainstream media outlets, and policy makers. Their products are broadly disseminated through social media and easily found through customized search, and they are sought by reporters who seeking to cover “both sides” of a controversy that is intellectually equivalent to a “controversy” about whether the earth is round or flat. Nuclear conflict On the risks of nuclear conflict, theories and approaches to nuclear deterrence and strategic stability developed prior to the collapse of the Soviet Union in the late 1980’s and early 1990’s rest on the presumption of rationality in national decision makers. In particular, they assume that adversaries are deterred from attacking by a threat of retaliation that would impose costs on the adversary that would outweigh any conceivable benefits that it would gain from an attack (Morgan 2003). Central to this assumption is a rational adversary that can and does make a calculation of expected costs and benefits, compares them, and then acts accordingly. But the psychologically informed understanding of realworld decision making described above was not accepted widely in the scientific literature until approximately the same time as the collapse of the Soviet Union, and the seminal work in such understanding occurred only in the decade previous to that. What a psychologically-informed understanding of real-world decision making tells us is that the rationality assumption at the base of much traditional thinking on deterrence and strategic stability is untenable, given that humans have evolved to rely on intuitive, reflexive, heuristic System 1 thinking to make decisions, particularly when faced with time pressures, surprise and other obstacles to the deliberate calculation implied by System 2 thinking (Kahneman 2011). Psychology tells us that – more often than not – the fast, intuitive judgements of System 1 often take precedence over the slower, more analytical thinking of System 2. The challenges posed by reflexive reliance on System 1 thinking are greatly accentuated by characteristics of today’s information environment. Social media networks in particular are optimally designed to stimulate System 1 thinking – emotional, reflexive, immediate – and they rapidly transmit content among like-minded individuals, creating the ideal conditions for public polarization and divisiveness to occur (Pfeffer, Zorbach, and Carley 2014). Multiple narratives rapidly emerge around complex events; citizens splinter into their own informational universes and are unable to agree on an underlying reality. Political leaders themselves are subject to these conflicting narratives and may even be active and influential participants in one or another of them.

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

The coming information dystopia

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

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

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

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

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

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

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

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

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

Fearing the end of the enlightenment

The Enlightenment established reason and reality as the foundational pillars of civilized discourse. In such discourse, logic matters, and a logical contradiction between statement A and statement B means that at least one of those statements is false. The truth of a statement about the world is tested by its correspondence to objective reality rather than by how many people believe it; that is, empirical data are influential. Furthermore, statements known to be wrong or false do not affect conclusions or choices between alternative courses of action. Cyber-enabled information warfare provides the tactics, tools, and procedures – in short, the means – to replace the pillars of logic, truth, and reality with fantasy, rage, and fear. In a world of ubiquitous cyber-enabled information warfare, communication and information inflame passions rather than informing reason, play to the worst in people’s cognitive architectures rather than the best, and divide rather than unify. Deliberate corruption of the information ecosystem could be seen as an analog of poisoning water supplies that can be done remotely, inexpensively, and anonymously. All of this is just another way of saying that today it is possible to see glimmerings of an anti-Enlightenment that can possibly take root and that would indeed be the end of civilization as we know it.

US democracy could collapse in the next decade causing widespread instability and violence

Homer-Dixon 2022 (Thomas Homer-Dixon is the Executive Director of the Cascade Institute at Royal Roads University. He has a Ph.D in International Relations from the Massachusetts Institute of Technology and is an expert on threats to global security in the 21st Century. “The American Polity is Cracked and Might Collapse, Canada Must Prepare” in The Globe and Mail <https://www.theglobeandmail.com/opinion/article-the-american-polity-is-cracked-and-might-collapse-canada-must-prepare/>)

By 2025, American democracy could collapse, causing extreme domestic political instability, including widespread civil violence. By 2030, if not sooner, the country could be governed by a right-wing dictatorship. We mustn’t dismiss these possibilities just because they seem ludicrous or too horrible to imagine. In 2014, the suggestion that Donald Trump would become president would also have struck nearly everyone as absurd. But today we live in a world where the absurd regularly becomes real and the horrible commonplace. Leading American academics are now actively addressing the prospect of a fatal weakening of U.S. democracy. This past November, more than 150 professors of politics, government, political economy and international relations [appealed](https://can01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.axios.com%2Fmidnight-is-approaching-to-pass-voting-rights-protections-d3d8cb12-3b2c-4422-8eee-f60425265472.html&data=04%7C01%7CLJutras%40globeandmail.com%7C3f84cd1eaac546dd27bb08d9c59fa629%7C44376110425e46ab942e26c9518bfd03%7C1%7C0%7C637758112819131902%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C2000&sdata=u61H7OtYQWaGpivOnrfy8MUlJ6HL6cah1nyl8YxLHkU%3D&reserved=0) to Congress to pass the [Freedom to Vote Act](https://can01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.brennancenter.org%2Four-work%2Fresearch-reports%2Ffreedom-vote-act&data=04%7C01%7CLJutras%40globeandmail.com%7C3f84cd1eaac546dd27bb08d9c59fa629%7C44376110425e46ab942e26c9518bfd03%7C1%7C0%7C637758112819131902%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C2000&sdata=GvihVDwuaxEi2GG1s96iFS%2FTL1sC7MeApk6cIkHMCJI%3D&reserved=0), which would protect the integrity of US elections but is now stalled in the Senate. This is a moment of “great peril and risk,” they wrote. “Time is ticking away, and midnight is approaching.” I’m a scholar of violent conflict. For more than 40 years, I’ve studied and published on the causes of war, social breakdown, revolution, ethnic violence and genocide, and for nearly two decades I led a centre on peace and conflict studies at the University of Toronto. Today, as I watch the unfolding crisis in the United States, I see a political and social landscape flashing with warning signals.

#### **Democracy is key to solving a laundry list of impacts**

Chollet et al., German Marshal Fund of the United States Executive VP, ‘17

[Derek Chollet et al., Executive Vice President and Senior Advisor, Security and Defense Policy, German Marshall Fund of the United States, with 9 additional authors, BUILDING ‘SITUATIONS OF STRENGTH’: A NATIONAL SECURITY STRATEGY FOR THE UNITED STATES, Brookings Institution, 2—17, p. 3-4]

We believe that abandoning traditional U.S. support for the international order would be a serious strategic error that would leave the United States weaker and poorer, and the world more dangerous. It would encourage revisionist states to destabilize Europe, East Asia, and the Middle East. It would reduce global economic growth and leave us vulnerable to a new financial crisis. And it would damage efforts to tackle shared challenges like terrorism, nuclear proliferation, and climate change that have very real— and potentially very damaging—impacts here at home. The last time an unraveling of an existing international order occurred was in the 1930s, and the result was depression and world war. Indeed, much of the violence and disorder we see in the world today results from the weakening of the current order. Moreover, the existing order must be assessed relative to the plausible alternatives. The best case outcome in light of an American retreat from the international order is a spheres of influence system whereby China dominates much of East Asia, Russia dominates much of Eastern and Central Europe, and the United States is preeminent in its own hemisphere and possibly Western Europe. Spheres of influence approaches to international order are inherently unstable, largely because the lines of demarcation are contested. It is a configuration prone to great power conflict. And the process of transition from an open global order where small nations have rights to a more imperial model would be particularly fraught.

**Scenario 2 US Leadership**

#### **The United States should join forces with NATO to increase their own cyber security, they promised to**

North Atlantic Treaty Organization (NATO), March 23, 2022 <https://www.nato.int/cps/en/natohq/topics_78170.htm>?

To keep pace with the rapidly changing threat landscape and maintain robust cyber defences, NATO adopted an enhanced policy and action plan, which were endorsed by Allies at the 2014 NATO Summit in Wales. The 2014 policy established that cyber defence is part of the Alliance’s core task of collective defence, confirmed that international law applies in cyberspace, set out the further development of NATO’s and Allies’ capabilities, and intensified NATO’s cooperation with industry. At the 2016 NATO Summit in Warsaw, Allies reaffirmed NATO’s defensive mandate and recognised cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land and at sea. As most crises and conflicts today have a cyber dimension, treating cyberspace as a domain enables NATO to better protect and conduct its operations and missions. At the Warsaw Summit, Allies also pledged to strengthen and enhance the cyber defences of national networks and infrastructures, as a matter of priority. Together with the continuous adaptation of NATO’s cyber defence capabilities, this will reinforce the cyber defence and overall resilience of the Alliance. At the 2021 NATO Summit in Brussels, Allies endorsed a new Comprehensive Cyber Defence Policy, which supports NATO’s three core tasks of collective defence, crisis management and cooperative security, as well as its overall deterrence and defence posture. NATO’s defensive mandate was reaffirmed, and Allies committed to employing the full range of capabilities to actively deter, defend against and counter the full spectrum of cyber threats at all times. Responses need to be continuous and draw on elements of the entire NATO toolbox that include political, diplomatic and military tools. Allies also recognised that the impact of significant malicious cumulative cyber activities might, in certain circumstances, be considered as an armed attack. The nature of cyberspace requires a comprehensive approach through unity of effort at the political, military and technical levels. The 2021 policy and its corresponding action plan will drive forward activities across these three levels. Developing the NATO cyber defence capability The NATO Computer Incident Response Capability (NCIRC), based at SHAPE in Mons, Belgium, protects NATO’s own networks by providing centralised and round-the-clock cyber defence support. This capability evolves on a continual basis and maintains pace with the rapidly changing threat and technology environment. NATO has also established a Cyberspace Operations Centre in Mons, Belgium. The Centre supports military commanders with situational awareness to inform the Alliance’s operations and missions. It also coordinates NATO’s operational activity in cyberspace, ensuring freedom to act in this domain and making operations more resilient to cyber threats. To facilitate an Alliance-wide common approach to cyber defence capability development, NATO also defines targets for Allied countries’ implementation of national cyber defence capabilities via the NATO Defence Planning Process. NATO helps Allies to enhance their national cyber defences by facilitating information-sharing, exchange of best practices and by conducting cyber defence exercises to develop national expertise .

#### **A strong NATO bolsters the U.S.’s military capabilities—important to our global leadership**

Lute & Burns, Harvard researchers, ‘19

[Ambassador Douglas Lute, Senior Fellow, Belfer Center and President, Cambridge Global Advisors and Ambassador Nicholas Burns, Professor, Diplomacy and International Politics, Harvard Kennedy School, “NATO at Seventy: An Alliance in Crisis,” Project on Europe and the Transatlantic Relationship, Belfer Center for Science and International Affairs, Harvard Kennedy School, 2—19, p. 41-42]

As a military alliance, NATO’s most important contribution to American interests is security. Above all, NATO has helped keep the peace in Europe after centuries of division and war. NATO has invested for decades in the ability of its members to operate together—so-called “interoperability”— based on practiced procedures, common standards and NATO’s historically unique integrated military command structure. Many of NATO’s partners also share in this interoperability. This military potential means that when America faces security challenges anywhere, it has ready teammates based on NATO, either with the Alliance as a collective whole or with select allies to form a purpose-built military coalition. Further, NATO allies provide America basing and access rights across Europe; bringing U.S. forces a continent closer to trouble spots in the Middle East, Africa and beyond, and providing improved response times and sustainability. Bases like Lakenheath in the U.K., Ramstein in Germany, Aviano in Italy, Rota in Spain, Souda Bay in Greece and İncirlik in Turkey are strategic assets. NATO allies employ tens of thousands of intelligence personnel, extending the reach of the United States’ eyes and ears.125 In short, NATO reinforces America’s national military strength with increased scale, diversity and geographic position.

NATO is not perfect. This report addresses the array of significant challenges the Alliance must face. At heart, however, Americans must remember that a Europe “whole, free and at peace” is fundamentally in the U.S. interest and NATO is America’s primary bridge across the Atlantic.126 In fact, most Americans continue to support NATO overwhelmingly.127 America by itself enjoys great human capital, vast resources and favorable geographic position. Together with its allies, both in NATO and in East Asia, America holds an unmatched geo-strategic advantage over any potential competitor, today and for the foreseeable future. America’s main strategic competitors, China and Russia, do not compare. Sustaining this strategic advantage by nurturing and investing in alliances, beginning with NATO, is therefore in America’s vital national interest. Allies are the ultimate guarantee of American security and prosperity.

#### **Resiliency, active cybersecurity, sustained interventions to reduce China and Russia cyber capabilities should be focus of NATO cyber shift – US leadership necessary**

**Ahlawat, 2021**

[Urjasvi, Jindal School of International Affairs and Research Intern at the Centre for Security Studies, “NATO: CYBERSECURITY AND CYBER COALITION“CSS ISSUE BRIEF, January 2021, https://jgu.s3.ap-south-1.amazonaws.com/jsia/Urjasvi+-+NATO+Cybersecurity.pdf accessed jcp-tm 6/9]

THE UNITED STATES ASPECT

Being the influential and dominant member, the United States did not consider NATO or cybersecurity to be of great importance, however, the dynamics are likely to change post- 2020 Presidential elections. Joe Biden, the President-elect, declared cyber threats as “one of the defining challenges of our time.” He believes that in today’s time, Russia and China impose a threat to NATO’s security by continuously attacking the Alliance and its members. To equip with protection from the aforementioned threats, Biden under the US believes that NATO has to adopt a policy of constructive, ongoing responses to China and Russia in cyberspace to achieve its mission of deterrence and security, where great power rivalry is taking place in real-time. NATO’s central focus should be on cybersecurity, for which the following three key actions are to be followed.

First, NATO should mandate that resilient cybersecurity architectures, the powers of its members and its main essential infrastructures be built and enforced by itself. Primary elements of a robust infrastructure could include the use of cloud technologies in the private sector; zero confidence architecture for successful access management; creation of stable hardware capabilities; and cyber defences increased by deep learning and artificial intelligence. To achieve this, the architecture framework suggested needs to be flexible to adapt to the rapidly developing and emerging technologies. However, the barrier arises as it is a challenge for NATO to itself build the suggested architecture. Using the NATO Defence Planning Process (NDPP), procurement processes, requirements and goals, and Allied Command Transition strategy to promote a robust research and development initiative, it should stress their necessity and require its members to do so.

NATO must agree that one size would not fit all when determining specifications for these resilient architectures. Not only will requirements differ among military, government, and critical infrastructures operators, but, as has been shown in the development of autonomous vehicles and space capabilities, there are a variety of different approaches that may prove effective.10

Second, **NATO should conduct active cybersecurity in cooperation with its nations**. Due to technological loopholes or human error, even the best exclusionary technologies in a cybersecurity resilient design may fail. As a result, even after an attacker has abused cybersecurity, the alliance requires "active cyber defences'' that will create durability. These features impact only certain networks where they have been built by providers and owners and are not for offensive purposes. In its Active Cyber Defence11, the US National Security Agency illustrates how the key elements of active defence capacities include “real-time communication, sense-making analytics to understand the current state and automated decision-making to decide how to react to current state information.’’[10]

NATO must be capable of searching for potential enemies within electronic networks vital to security as a core aspect of successful cyber defence. By removing malware and closing redundant **ports, the Alliance could build highly competent specialist hunting teams to review device operations, identify irregularities, and combat intruders**. NATO Standing Cybersecurity Hunt Teams should also be working with the cooperation and active collaboration of national governments and operators of infrastructure networks. These hunting teams will perform in- depth technological assessments of live networks to detect unnoticed risks, according to the US Department of Homeland Security. Standing Cybersecurity Hunt Teams will broaden the capacities of NATO's existing Cyber Rapid Response teams, which are small in size and work reactively, with an emphasis on aggressive protection.

Third, NATO should strategize a sustained intervention policy aimed at reducing Russian and Chinese interventions to undercut the cyberspace alliance. US Cyber Command developed the idea of sustained commitment, but the reasoning still extends to NATO, arising from the need to tackle the current cyber attack campaigns emanating from Russia and China. Persistent engagement includes monitoring enemies, recognising their objectives, evaluating the instruments used for attacks, and taking steps to degrade their ability to blunt current attacks or stop potential attacks. As a core aspect of its deterrence and security, the Alliance wants a sustained commitment cyber policy.

NATO should exploit its intelligence and defence preparation resources to build a framework for allies to actively control cyberattacks from Russia and China to ensure sustained participation successfully in the Alliance. NATO can collect information through its Intelligence and Security Branch, attacking allied vital assets, strategic capabilities, or democratic structures. Using this material, the Cyberspace Operations Center (CYOC) of NATO could outline ways to decrease the capacity of Russia and China to carry out such attacks. The CYOC should share its analyses with pre-designated Allies who would work with targeted countries and employ their cyber effects against the identified threats12. In support of NATO operations, nine NATO nations have already pledged to make those results possible. The aforementioned cyber-capable allies will be responsible, based on NATO guidelines, for persistently undermining the cyber operations of adversaries. This model will make the CYOC of NATO a strategy platform with an approach to persistent interaction around the Alliance. It will allow NATO to encourage its members to take individual or multilateral measures against hybrid cyberspace operations by adversaries.

#### **The plan is key propagating liberal cyber norms**

Pernik & Jermalavičius, International Centre for Defence & Security analysts, ‘16

[Piret Pernik and Tomas Jermalavičius, Research Fellows, International Centre for Defense and Security “Resilience as Part of NATO’s Strategy: Deterrence by Denial and Cyber Defense,” FORWARD RESILIENCE: PROTECTING SOCIETY IN AN INTERCONNECTED WORLD, 2016, p. 106-107]

Due to interdependencies of communication and information systems, and critical infrastructures, resilience can only be developed through an integrated approach.Disruptions of host nation and coalition partner networks and critical infrastructure upon which NATO depends can degrade NATO’s ability to conduct operations. Secondly, projecting cyber defense beyond NATO’sterritory would help to define global cybersecurity norms and behaviors around liberal democratic values. In recognising this indivisibility of security, the NATO-EU Joint Declaration,signed in Warsaw, stresses the need to “foster the resilience of our partners” through individually tailored projects. 13 Indeed, NATO should project its soft side of cyber power in its neighborhood and globally with an aim to expand secure, open and free cyberspace and advocating democratic liberal values in cyberspace.

NATO has a wide range of cooperation formats with more than 40 partners. These partnerships can be leveraged and further expanded according to cyber defense needs of individual partners. 14 For example, in the existing framework of the Partnership for Peace Planning and Review Process, Georgia, Moldova, Iraq, Jordan have included cyber defense aspects into their capacity-building packages. 15 Non-NATO nations also participate in Smart Defense projects such as Multinational Cyber Defense Capability Development (MNCD2), which focuses on sharing technical information, situational awareness and creating a cyber security assessmentteam. 16They have participated at NATO cyber defense and crisis management exercises, and at technical exercises run by the NATO Cooperative Cyber Defense of Excellence.It is possible to include cyber defense issues in their consultations with NATO bodies (28+ meetings) and through staff-to-staff talks. Lastly, NATO educational bodies provide training courses on strategic, operational and technical levels to partners with requisite security clearances.