Cybersecurity Affirmative - DUDL -

adapted from NAUDL core files

(includes answers to Russia DA)

CYBERSECURITY AFF

The goal of the affirmative is simple: Suggest a plan of action, show how it will work, and why it is a good idea. If the affirmative plan is a good idea at the end of the round, then you will win. The more you focus on the plan and why it is a bad idea, the more often you'll win debates.

Speech Time	(Minutes)
1st Affirmative Constructive (1AC)	8
2nd Negative Speaker Questions 1st Affirmative Speaker	3
1st Negative Constructive (1NC)	8
1st Affirmative Speaker Questions 1stNegative Speaker	3
2nd Affirmative Constructive (2AC)	8
1st Negative Speaker Questions 2nd Affirmative Speaker	3
2nd Negative Constructive (2NC)	8
2nd Affirmative Speaker Questions 2nd Negative Speaker	3
1st Negative Rebuttal (1NR)	5
1st Affirmative Rebuttal (1AR)	5
2nd Negative Rebuttal (Closing Statement) (2NR)	5
2nd Affirmative Rebuttal (Closing Statement) (2AR)	5

Speaking Roles on the Affirmative:

- **1st Affirmative Speaker:** Your job is to introduce the affirmative case in the 1AC, and to keep the affirmative case (plan, solvency and at least one advantage) alive during the 1AR.
- **2nd Affirmative Speaker:** Your job is to answer negative attacks in the 2AC, adding any evidence the affirmative might need, then to make a closing statement explaining why the affirmative team should win in the 2AR. This should focus on why the plan is a good idea and how the advantages are more important than the disadvantages.

Goals of each speech:

1. **1AC:** Build your case: Inherency, The Plan, Solvency, and the Advantages.
2. **2AC/1AR:** Respond to the negative's arguments and add new evidence if needed. You need to be winning at least Solvency and an Advantage after the 1AR to win the debate.
3. **2AR:** The second affirmative speaker should give a closing argument all about why the plan is a good idea. Answer the second negative rebuttal (2NR) and tell the judge why the affirmative team should win.

Each Affirmative Case will have four main parts. You'll have to win each piece in order to win a debate as the affirmative.

- **Inherency:** What is the problem, and why isn't it being fixed now? This usually identifies trends or specific barriers to the problem being fixed.
- **The Plan:** What is the affirmative going to do about it? This is a short description of action and should be written with care.
- **Solvency:** How will the plan work? Will it be too expensive? What paths are in place to allow this plan? Will it actually work?
- **Advantages:** What are the benefits of doing the plan, or the problems we can avoid by doing it? This is why we should care about the plan.

Your partner will have a chance to support your arguments and read more evidence in the second affirmative constructive (2AC).

Argument 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 algorithms, which would enable drastic progression in many fields.

Voter intimidation (noun)- Harassment at voting polls in an 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 movement 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 Technology

Topic Introduction

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. cybersecurity efforts or tried to join theirs. The United States is one of the strongest nations in the cyberspace 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.

Strategic Overview

The affirmative claims four advantages, although you are not required to try and read all of these advantages in the AFF. You can pick and choose which ones you like best or fit the debate better.

COVID-19 Advantage: The COVID-19 advantage argues that the impacts seen from the pandemic, i.e. travel restrictions and most of our lives being moved online, allows for hackers to more access and find more ways to attack individuals. Passing the AFF and improving our security in cyberspace will help mitigate those attacks.

Russia Advantage: Like what is explained in the majority of the AFF, Russia is constantly attacking the United States. For the US to help protect itself against any future Russian attacks that can cause more damage than what has already been done, we need to increase our cyber security.

Civic-Engagement Advantage: A lot of Americans do not trust the election process because of the known Russian attacks during some elections. POC communities are already disenfranchised from voting, even before the Russian attacks, and the distrust in American election process just makes those disparities worse.

Social Media Misinformation Advantage: Russia is planting fake news and stories on social media. This is bad for the American people because more than half of the population gets their news off social media, and they are consuming false information. Improving American cyber security would allow the government to better protect itself from news hacks.

When putting together your 2AC block, you'll want to follow the structure you learned during flowing:

They say →<Insert argument>

That's not true because →<Restate your argument or read a new card to answer their argument>

Prefer our argument because →<Explain why your argument is better>

Consider the following questions:

- Why is NATO the best option?
- Why can't the United States fortify their cyberspace on their own?
- What are the implications of working with NATO?
- If the United States chose not to work with NATO what would happen?
- Are there some policies that should not be done because the consequences are so bad?

The negative team will respond to your arguments, using "on case" responses. They'll also present some of their own. These "off case" arguments are dangerous and you'll need to respond in order to win the debate.

In the Novice Packet, there are three "off case" positions:

- **Russia Disadvantage:** The answers to this DA are broken up into three parts. Non-unique, which just states that Russia will not increase aggression with or without the AFF. Then we have No-impacts, this tells us that a Russian would not be detrimental for the U.S. and would not cause damage. Then finally No-Link which explains that if a conflict were to arise with Russia it is not because of the AFF.
- **China Disadvantage:** For the Non-unique these DA answers explain that NATO is already on the verge of collapse without the AFF. The No-impact says that even if NATO is stretched the AFF would stop a collapse and China is a threat in the way the NEG presents them to be. No-link is that the AFF does not trigger NEG impacts. It does not cause a strain and gives an **Alt-Cause.** Which is if anything is going to strain NATO it's their financing methods not the AFF.
- **Impact/Link Turn:** This is when you can turn these parts of your case back onto the other team. An Impact turn is turning the NEG's impacts back on them. Possibly stating that they make the impacts worse by not letting the AFF pass. A Link turn is saying that they link to the impacts better than the AFF. There is no Link turn in this particular case, but it is still just as valuable.
- **Alt-Cause:** This is called an alternative cause for why something is taking place, usually why the impacts could/are happening that is not the AFF. Even if the AFF causes the impacts there is a laundry list of other reasons that could also trigger those impacts and the blame cannot completely be put on the AFF. It just gives alternative reasons for why the impacts would happen.

PLAN TEXT

THE UNITED STATES FEDERAL GOVERNMENT SHOULD SUBSTANTIALLY INCREASE ITS SECURITY COOPERATION WITH THE NORTH ATLANTIC TREATY ORGANIZATION IN CYBER SECURITY.

INHERENCY

1) 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 DEFENSES TO FULFILL THE ALLIANCE'S CORE TASKS OF COLLECTIVE DEFENSE, 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 defense is part of NATO's core task of collective defense. NATO Allies have affirmed that international law applies in cyberspace. NATO's main focus in cyber defense 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 defenses, 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 defense, 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 defense 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.

2) The United States needs to increase cyber efforts with NATO to improve NATO's and their own cyber security

Luukas K. Ilves et al Timothy J. Evans, Frank J. Cilluffo, and Alec A. Nadeau, July 28, 2016, *Luukas Ilves is Counselor for Digital Affairs at the Permanent Representation of Estonia to the EU. Timothy Evans is Senior Advisor, Cyber Strategy and Policy, at Johns Hopkins University Applied Physics Laboratory in Arlington, Virginia. Frank Cilluffo is the Director of the George Washington University's Center for Cyber and Homeland Security. Alec Nadeau is a Presidential Administrative Fellow at the George Washington University's Center for Cyber and Homeland Security.* https://cco.ndu.edu/LinkClick.aspx?fileticket=HVJ82hUX7_s%3d&portalid=96

Developments in the cybersecurity operations of both NATO and the EU have paralleled the growth of cybersecurity as a major policy concern to the United States and other national governments. The digital revolution has also changed the basic environment in which governments operate, necessitating increasing levels of cross-border interdependence and connectivity. European countries have responded to the need to increase coordination and cooperation through new initiatives at the national level and under the auspices of NATO and the EU. Nevertheless, the relationship between national capabilities and sovereignty, and the authority of these two international organizations, remains unsettled. The efforts of NATO and the EU to mainstream cybersecurity into existing activities have thus far proven insufficient to fully address the growing cyber threat landscape. NATO's Development of Cross-border Cyber Defense Policy and Coordination NATO forecasted today's cyber threat environment in 2010: "Cyber attacks are becoming more frequent, more organized and more costly […]; they can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability."6 NATO faces a cyber threat landscape that abounds with hackers, hacktivists, nation-states, and criminals. NATO itself has been targeted directly by Russian hackers seeking information on its defensive posture against Russia.7 Furthermore, the recent attack by Russia on the Ukrainian power grid underscores the fact that Russian cyber attack capabilities are very real.8 NATO also faces the same types of cyber breaches that affect businesses in America on a daily basis, ranging from random criminal acts to infiltrate NATO's systems to those of a more sophisticated, targeted nature. Despite preventive measures, cyber criminals around the world continue to gain access to these networks, including those that are classified.9 In all, the current threat environment embodies much more significant risks than those first exemplified by the Russian cyber attacks on Estonia in 2007, which initially prompted NATO to address the dangers of cyber warfare.

3) Cyber security attacks are becoming more and more dangerous

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

Malicious cyber activity has increased substantially over the past years, ranging from ransomware and espionage to politically motivated cyberattacks and sophisticated malware used in the war in Ukraine. NATO allies must remain on high alert. The changed nature of military conflict changes the defensive mission of NATO, which faces capable opponents in cyberspace and raises the question of how to create accountability when a hostile state fails to observe globally agreed norms. The set of actions for NATO for the next five years revolves around how to impose costs and how to deny benefits against malicious actors in cyberspace. 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 international 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. Cyber Challenge to 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.

HARMS

1) THE PAST ATTACKS ON US CYBER SPACE WILL CONTINUE TO HAPPEN WITHOUT STRONG CYBER SECURITY

Andy Purdy, July 30, 2021, Andy is CSO for Huawei Technologies USA, overseeing Huawei's US cyber assurance program.
https://www.forbes.com/sites/forbestechcouncil/2021/07/30/the-us-needs-a-stronger-commitment-to-cybersecurity/?sh=7a5b9db05daf

The Colonial Pipeline ransomware attack illustrated the vulnerability of America's critical infrastructure to a security breach. Fuel shortages and rising prices got people's attention. Data breaches have more than doubled over the past decade. RECENT CYBERATTACKS HAVE EXPLOITED THE "TRUSTED SUPPLIER" STATUS OF SOLARWINDS AND MICROSOFT EXCHANGE, AMONG OTHER COMPANIES, AND RAISED CONCERNS AT THE HIGHEST LEVELS OF GOVERNMENT AND THE PRIVATE SECTOR. The stakes are only getting higher as the internet of things makes everything more connected and we all become more dependent on 5G-enabled technologies. What's being done to prevent cyberattacks — and is it enough? Last month, President Joe Biden issued an executive order to begin developing mandatory baseline security requirements for government agencies and the companies that do business with them. The order states that the federal government must collaborate with the private sector and with the National Institute of Standards and Technology (NIST) to develop and implement a zero-trust model that "eliminates implicit trust in any one element, node, or service and instead requires continuous verification" from multiple sources.

2) 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.

3) 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.

SOLVENCY

1) 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 defenses, 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 defense is part of the Alliance's core task of collective defense, 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 defenses of national networks and infrastructures, as a matter of priority. Together with the continuous adaptation of NATO's cyber defense capabilities, this will reinforce the cyber defense 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 defense, crisis management and cooperative security, as well as its overall deterrence and defense 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 defense 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 defense 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 defense capability development, NATO also defines targets for Allied countries' implementation of national cyber defense capabilities via the NATO Defence Planning Process. NATO helps Allies to enhance their national cyber defenses by facilitating information-sharing, exchange of best practices and by conducting cyber defense exercises to develop national expertise .

2) WORKING WITH NATO WOULD IMPROVE THE U.S.' OWN SECURITY

is widely known. With its new strategy and continued investments, the Alliance seems to want to expand its cybersecurity capabilities and responsibilities dramatically. But NATO needs to avoid its Article 5 aspirations for cyberattacks and risks taking on too much cybersecurity accountability is widely known.

Myriam Dunn Cavelty, January 2012 Cavelty is a senior lecturer for security studies and deputy for research and teaching at the Center for Security Studies (CSS). She studied International Relations, History, and International Law at the University of Zurich. She was a visiting fellow at the Watson Institute for International Studies (Brown University) in 2007 and fellow at the stiftung neue verantwortung in Berlin, Germany 2010–2011. https://www.researchgate.net/publication/228199410_Cyber-Allies_Strengths_and_Weaknesses_of_NATO's_Cyberdefense_Posture

NATO has more of a history with cybersecurity than is widely known. With its new strategy and continued investments, the Alliance seems to want to expand its cybersecurity capabilities and responsibilities dramatically. But NATO needs to avoid its Article 5 aspirations for cyberattacks and risks taking on too much cybersecurity accountability NATO's New Tricks Looking back, 2010 seems to have been dominated by reports on one security issue in particular: cyber threats. The discovery of Stuxnet, the industry-sabotaging super worm that scared politicians all over the world; tales of (Chinese) cyberespionage in many variations; the growing sophistication of cybercriminals as evidenced by their impressive scams; as well as Wikileaks' release of US diplomatic cables and the subsequent actions of the hacker group Anonymous all catapulted the cyber topic from the realm of geeky experts and military strategists to a mainstream public fear. Whether the damage inflicted by cyberattacks is becoming more frequent, more organized, and more costly or if our perception has merely changed is unimportant. The outcome is clear: cyberattacks are considered one of the top security threats and have been anchored firmly in national strategy documents all over the world. Given this general mood, NATO's mention of cyberattacks as one of the primary future security concerns in its new Strategic Concept of November 2010 was widely applauded. But NATO was not just following the common strategic trend: this reference in its new roadmap marked the temporary culmination point of the Alliance's dealing with the threat.

3) PASSING THE AFF WOULD PROVIDE THE U.S. WITH TOOLS TO BETTER PROTECT THEIR CYBER SPACE

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

Despite a considerable arsenal of sophisticated offensive and defensive cyber capabilities, American political and military systems still struggle at times with inconsistent strategic communications and a dogged credibility gap. **The new deterrent framework in cyberspace must therefore focus more on communicating clear intent and building enduring credibility through redlines, deterrent language, and cross-domain options to impose further costs, deny added benefits, encourage greater restraints, and control more the narratives. Declaratory redlines make clear the unwanted risks, costs, and consequences of specific actions. They are an important way to influence an adversary's risk perception and rational calculus, lower the likelihood of misunderstanding, and encourage restraint. They also outline the conditions of and willingness to inflict unacceptable retaliatory damage or destruction.** U.S. policymakers should therefore "privately" reinforce to strategic competitors **(and potential adversaries) the deterrent public statements contained therein the 2018 National Cyber Strategy (NCS), 2021 Interim National Security Strategic Guidance (INSSG), 2022 National Defense Strategy (NDS), and (anticipated) forthcoming National Security Strategy (NSS).** U.S. law enforcement officials should likewise continue to "publicly" warn cyber criminals of egregious illicit cyber acts. In doing so, they should make it clear to both state and non-state threat actors that any cyber attack or cyber act that threatens U.S. national security interests, U.S. economic prosperity, and U.S. political stability is unacceptable and will be met with severe and disproportionate consequences for them. If they attack or act, they should not expect a proportionate response. They should expect prompt and devastating force that will cause retaliatory damages much greater than what they intended to inflict. This clear warning should have the effect of causing malicious cyber actors to think twice before acting and consider that the real costs may be much greater than any intended benefits.For cyber powers like China and Russia, it should be made unequivocally clear that any cyber attack on critical military space systems – missile warning, command and control of nuclear forces, and positioning, navigation, and timing – is an act of war and will be dealt with accordingly. **Doing so interlocks the 2020 National Space Policy with the 2018 NCS, both of which acknowledge the imperative of and calls for improvements to space cybersecurity. Like any other increasingly digitized and networked critical infrastructure, space-based and ground-based space systems and their communication links are vulnerable to cyber attacks.**

4) NATO'S CYBER-SECURITY IS CONSIDERABLY STRONGER THAN THE U.S.

Dr. Chris J. Dolan, June 8, 2022, Dr. Chris J. Dolan is Professor of Political Science and Director of the Master's of Science program in Intelligence and Security Studies at Lebanon Valley College in Pennsylvania. He is a two-time Fulbright U.S. Scholar in international security in North Macedonia (2022) and Kosovo (2020). Dolan is the author of Obama and the Emergence of a Multipolar World Order; In War We Trust; The Presidency and Economic Policy and Striking First. He is completing a book on NATO and research projects on geopolitics of the Western Balkans and hybrid warfare and the transatlantic alliance. In 2018, he received the Thomas Rhys Vickroy Distinguished Teaching Award and the Educator of the Year award in 2019. He writes a regular column on U.S. foreign policy and national security at The Hill. https://www.justsecurity.org/81839/natos-2022-strategic-concept-must-enhance-digital-access-and-capacities/

**Note: Since the date this article was made the 2022 Strategic Concept has been passed. Although this card is in future tense, in reality, it is happening currently.*

This month in Madrid, the North Atlantic Treaty Organization (NATO) will update its Strategic Concept, the principal document that guides the alliance's political-military strategy and collective defense operations. The war in Ukraine has put resilience in the face of Russian aggression front and center, especially in the cyber and information operation domains. Over the years, NATO has digitized and enhanced its security platforms, emphasizing interoperability of systems among its now 30 current member states. If NATO is to become more resilient against advanced persistent threats, hackers, and the maligned states that sponsor them, then the 2022 Strategic Concept must infuse multinational warfighting and deterrence against hybrid threats with methods that facilitate access to data and information sharing on its platforms and across multiple domains, namely in air, cyber, information, land, maritime, and space operations. The Strategic Concept is among NATO's most important documents as it informs alliance planning, resource allocation, and programming based on changes in the threat environment. But the document has not been updated since 2010. The 2010 Strategic Concept, entitled "Active engagement, Modern Defense," contained just one brief sentence about cyber attacks and did not even mention China. It also stated that "Today, the Euro-Atlantic area is at peace," even though Russia had invaded Georgia two years before and the threat of a return to great power competition loomed. To argue that a lot has happened between 2010 and 2022 would be an understatement. Russia's annexation of Crimea and intervention in the Donbas in 2014 and the invasion of Ukraine in 2022 shattered any illusions of a lasting peace with Russia. China's territorial ambitions, economic assertiveness, threats against Taiwan, and military modernization threaten the rules-based order. Emerging technologies – in the form of hypersonic weapons, artificial intelligence, quantum computing, and machine learning – have intensified great power competition. The 2022 Strategic Concept should highlight the essential role of technology in collective defense. To build greater digital capacity while also emphasizing resilience, NATO must adopt a new technological orientation on the military strategic level of command, especially within **the Allied Command Transformation** (ACT) in Norfolk, Virginia and the **Allied Command Operations** (ACO) in Mons, Belgium. ACT leverages advanced technologies for security and defense in capabilities, procedures, public-private partnerships, civil-military relations, and at NATO's Centers of Excellence. Led by the Supreme Allied Commander Europe, ACO is responsible for collective defense through direction, requirements, planning, and execution at the strategic level. However, the Strategic Concept 2022 should focus less on the emergence of new technologies and more on how NATO's military and civilian personnel use them. ACO and ACT must emphasize greater accessibility to information and data for its multinational warfighters, cyber operators, and civilian professionals. NATO must reach out to experts in the private sector, academia, and non-governmental organizations to harness ways to expand access and emphasize flexibility in multi-domain operations. NATO can do this by providing more grants to private sector partners and establish a new center of excellence on data and information sharing. ACO and ACT should also enable personnel and partners to readily access data and information in DIMEL domains: diplomatic, information/cyber, military, economic, and legal. This would expand the range of measures needed by ACT and ACO to connect and correlate deterrence with evolving hybrid threats. To deter hybrid threats across multiple domains, with enhanced access on different digital platforms, NATO members should develop smarter and lethal capabilities to confront threats from state and non-state actors. This would allow ACT and ACO to prepare for any contingency and respond to adversaries in battlefields and battlespaces.

ADVANTAGES

COVID-19

1) 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 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 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_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.4

Foundation for Defense of Democracies, 2021 (CHRIS NOLAN & ANNIE FIXLER "THE ECONOMIC COSTS OF CYBER RISK" https://www.fdd.org/analysis/2021/06/28/the-economic-costs-of-cyber-risk/)

While it could take months or even years to remove the compromised software and implement other remediation measures, and although the costs to the U.S. government alone could be in the hundreds of millions of dollars,[3] the breach was not as damaging as feared from an economic perspective, because its primary purpose appears to have been espionage. The breach did not cause large-scale business disruptions like those caused by Russia's NotPetya attack on Ukraine in 2017. That malware spread around the world, affecting tens of thousands of companies, costing some as much as hundreds of millions of dollars.[4]

The digital age has increased productivity and efficiency, but many firms are struggling to manage the downside risks that accompany it. Too many companies are prioritizing short-term growth and cost-cutting at the expense of cybersecurity. As the SolarWinds breach demonstrated, one company's cyber risk can have cascading economic and national security implications.

Twenty years ago, after a wave of corporate scandals undermined public confidence in the securities market, Congress passed the Sarbanes-Oxley Act, requiring greater corporate financial disclosures.[5] The law strengthened investor protections and confidence through better accounting standards, improved internal controls and disclosure by companies, and stronger external oversight. Poor cybersecurity is today's systemic risk, and the potential impact is even greater. Unlike the accounting malpractice and financial scandals of the 1990s and early 2000s that prompted congressional intervention, a single company with deficient cybersecurity could inflict substantial harm on the U.S. government, company shareholders (including retirees dependent on pensions), the public, and critical national infrastructure.

1) A STRONG CYBER SECURITY FRONT HELPS SECURE U.S. FROM FURTHER RUSSIAN ATTACKS

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

Another set of threats comes in the form of belligerent 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 undetected for months before the victims discovered vast amounts of their data had been stolen.5There 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 government has been hit by a series of cyberattacks that defaced government websites and wiped out the data on some government computers. In mid-January, 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 Transformation, whose e-governance portal gives the Ukrainian public digital access to dozens of government 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 international hacktivist collective Anonymous has declared "cyberwar" against Russia's government, claiming credit for several cyber incidents including distributed 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 sophisticated 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 infrastructure 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 WhisperGate, discovered in January by Microsoft, in Ukraine's networks that "provide critical executive branch or emergency response functions";

RUSSIAN ATTACKS COULD GO NUCLEAR

CNBC, April 29, 2022 Holly Ellyat is a correspondent with CNBC's international team in London – she cites multiple experts in this reporting: https://www.cnbc.com/2022/04/29/russia-ukraine-war-should-the-west-prepare-for-war-with-putin.html

Nonetheless, Ramani noted the threat posed by Russia could become more acute if it felt humiliated on the battlefield. In particular, military setbacks in Ukraine around May 9 could pose some danger. That's Russia's "Victory Day" — the anniversary of Nazi Germany's defeat by the Soviet Union in World War II.

"Putin has had a history of escalating unpredictability if he feels that Russia is being humiliated in some way ... and if there are major setbacks, especially on around the 9th [of May] then there's a risk of unbreakable action," he said. "But also there's a logic of mutually assured destruction that hopefully will rein everybody in."

Threatening nuclear attacks is part of Putin's "playbook," said William Alberque, director of strategy, technology and arms control at the International Institute for Strategic Studies think tank.

"Putin enjoys using risks and he thinks he has a much more appetite for risk than the West does," he told CNBC on Thursday. "He's trying to use the old playbook of 'if I terrify you enough, you'll back down'," he said.

"Ultimately, if he uses nuclear weapons, even a demonstration strike, this would turn Russia into a global pariah," Alberque said. He advised Western leaders, "We just need to be able to manage our risk and keep our nerve and not panic when he does something that we might not expect."

1) MANY AMERICANS LACK TRUST IN THEIR ELECTION PROCESS

Northwestern University December 23, 2020, https://news.northwestern.edu/stories/2020/12/38-of-americans-lack-confidence-in-election-fairness/

With the Georgia Senate runoff elections set for Jan. 5, 2021, a nationwide survey conducted post-election could provide insights about voter perceptions of fairness in the U.S. election and trust in democratic institutions. Researchers from a university consortium of Northwestern, Harvard, Northeastern and Rutgers surveyed more than 24,000 individuals across the nation between Nov. 3 and 30. The survey found that overall, 38% of Americans lack confidence in the fairness of the 2020 presidential election. That number is especially high among Republicans (64%) and Trump voters (69%) compared to Democrats (11%) and Biden voters (8%). "This level of distrust is not surprising, given political rhetoric, but it certainly is concerning. Elections are the foundation of our democracy and loss of faith in the process could undermine the new administration's legitimacy and ability to get things done," said James Druckman, the Payson S. Wild Professor of political science in the Weinberg College of Arts and Sciences at Northwestern and associate director of the University's Institute for Policy Research. The survey showed large partisan gaps of over 40 percentage points in public concern about mail-in fraud (85% of Republicans and 38% of Democrats), inaccurate or biased vote counts (84% of Republicans and 44% of Democrats) and illegal votes from non-citizens (81% of Republicans and 34% of Democrats). To better understand the reasons why some Americans distrust the election process, respondents were asked about their level of concern regarding voter suppression, intimidation, inaccurate or biased counts and interference. The problem most people found troubling was voter suppression (making it harder for certain groups to vote), with over two-thirds of respondents (67%) saying they were somewhat or very concerned about it. Voter intimidation was a concern for 62% of respondents, while inaccurate or biased vote counts concerned 60% of Americans. Foreign country interference was a concern for 59%, mail-in ballot fraud for 57% and illegal votes from non-citizens was a concern for 52%. "These numbers create a puzzle for the current Senate elections in Georgia," said Druckman. "For some, the concerns may de-mobilize but for others it may be a mobilizing factor to get your vote in, especially to combat concerns about suppression and intimidation." The three most polarizing election process issues with partisan gaps of over 40 percentage points had been heavily promoted by President Trump and received attention by right wing media. These included mail-in fraud (reported as somewhat or very concerning for 85% of Republicans but only 38% of Democrats), inaccurate or biased vote counting (a concern for 84% of Republicans and 44% of Democrats) and illegal votes from non-citizens (a concern for 81% of Republicans and 34% of Democrats). Partisan differences were lowest with regard to foreign interference in the election (60% Republicans and 63% Democrats), voter intimidation (60% Republicans and 67% Democrats) and voter suppression (63% or Republicans and 73% of Democrats). "The results make clear that we have a long way to go to restore faith in our electoral process," Druckman said.

2) THE U.S. WEAK CYBER SECURITY AND CONSTANT ATTACKS FROM RUSSIA IS THE CAUSE FOR GROWING ELECTION DISTRUST

U.S. News, May 10, 2019,
https://www.usnews.com/news/the-report/articles/2019-05-10/after-russian-election-interference-americans-are-losing-faith-in-elections

As lawmakers, state elections officials and social media executives work to limit intervention in the 2020 elections by Russia and other foreign operatives, an unsettling truth is emerging. Vladimir Putin may already be succeeding. The troubling disclosures of Russian meddling in the 2016 campaign – "sweeping and systematic," special counsel Robert Mueller concluded in his report on the matter – have policymakers on guard for what intelligence officials say is a continuing campaign by Russia to influence American elections. But even if voting machines in all jurisdictions are secured against hacking and social media sites are scrubbed of fake stories posted by Russian bots, the damage may already have been done, experts warn, as Americans' faith in the credibility of the nation's elections falters."This is Vladimir Putin's game plan – sow distrust, discord, disillusionment and division," Sen. Richard Blumenthal, Democrat of Connecticut, says about the Russian leader. "It's his playbook for all Western democracies – not just us, but Europe and around the world. We're open societies, we're vulnerable to disinformation, and he regards himself as superior because he controls the press," adds Blumenthal, one of the authors of bipartisan legislation meant to improve election security. "There's a real danger to such distrust in the integrity of our election system that has lasting damage," he warns. Allegations of uncounted – or wrongly counted – ballots, voter suppression and other grievances tend to emerge in every election. Most famously in recent history, the 2000 presidential race was effectively determined by the Supreme Court. But the events of the past few years – including frequent comments by President Donald Trump questioning the integrity of a race he won – have aggravated the distrust, pollsters and analysts say. An NPR/Marist poll before last year's midterms found that nearly 2 in 4 voters do not believe elections are fair, and well over half said they did not think all votes would be counted in November 2018. That compared with a 2016 Gallup poll that found nearly two-thirds of Americans were confident in the vote count.Marist polling over decades shows that public faith in many institutions has plummeted, says Lee Miringoff, director of the Marist Institute for Public Opinion. For example, Miringoff says, in 1990, 62 percent of Americans said the media provided fair and accurate coverage of campaigns, with 37 percent disagreeing. Now, the numbers are virtually flipped, with an April Marist poll showing that 63 percent of Americans don't trust the media for fair and accurate campaign reporting, with 37 percent saying they do trust the media. The diminished trust in institutions is worrisome, Miringoff says, since it is those very institutions that inform the public of possible election meddling and handle the consequences of a disputed election.

3) POC VOTER TURNOUT IS ALREADY LOW, ELECTION FRAUD IS ANOTHER WAY TO STOP THEM FROM VOTING

American Bar Association, June 25, 2020
https://www.americanbar.org/groups/crsj/publications/human_rights_magazine_home/voting-in-2020/why-minority-voters-have-a-lower-voter-turnout/

With ethnic and racial minority populations in the United States rising, there is a growing population of voices that remain unaccounted for. Though current legislation has been implemented to ensure fair and impartial voting access, there is too much leeway given to state governments in the voting system's execution. As a result, restrictions in the election system have resulted in systematic discrimination toward minority populations, making them ineligible to vote. Voter ID laws have underlying racial biases and prevent minorities from engaging in active democratic participation. These requirements compel an individual to present his or her ID in order to cast a ballot on Election Day. Obtaining an ID can be costly and requires an individual's birth certificate, which may be burdensome. Proponents advocate for the law under the guise of preventing voter fraud and ensuring that only voter-eligible citizens partake in elections; however, individuals who lack government-issued identification are more likely to be younger, less educated, and impoverished, and—most notably—nonwhite. An example of the inherent discrimination of voter ID laws can be found in the implementation of Georgia's "exact match" system. This program requires an individual's voting status to be suspended if the name on their driver's license or Social Security records does not exactly match the name they inputted on their voter registration form. Of the 51,000 individuals that this law affected in 2018, 80 percent of them were African American. There is evidence that the "exact match" law played a role in the 2018 Georgia gubernatorial election, as African American candidate Stacey Abrams lost by approximately 55,000 votes. It is also far more difficult for members of minority communities to be able to locate polling places on Election Day. Only 5 percent of white survey respondents reported that they had trouble finding polling locations, compared to 15 percent of African American and 14 percent of Hispanic respondents. When deciding where to place a polling station, election officials are required to assign each precinct a designated station based on factors such as population, accessibility, and location recognizability; locations may be changed at the officials' discretion. Minorities have a lower voter turnout compared to whites and, in many cases, this has resulted in discriminatory polling place distributions. Disparities in polling places can also be the result of a change in the majority of election officials;

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 to Congress to pass the Freedom to Vote Act, 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.

1) Russia's cyber attacks have been planted false information in the media

Centre for International Governance Innovation, May 13, 2022,
https://www.cigionline.org/articles/nato-should-elevate-its-cyber-game-and-quickly/

Russia's propaganda and disinformation apparatus is extraordinarily complex. Some outlets are fully state-run, some are merely state-funded, and others are operated at arm's length by Putin-linked oligarchs. The system churns out conspiracy theories and whataboutism to aid Moscow's objectives. **From the start of the all-out invasion on February 24**, Russian disinformation has thumped on a series of narratives: that the North Atlantic Treaty Organization (NATO) posed a security risk to the Russian Federation; that Ukraine was run by neo-Nazis; that Ukraine is responsible for slaughtering civilians on its own territory. **Those narratives have, unfortunately, been somewhat effective in discouraging a unified response from NATO. They've influenced millions of Westerners and found purchase with far-right and Russophilic politicians the world over.** The most visible Western response to date has been the collective taking offline of Russia Today, or RT, the state-run television network. **Yet trying to ban Russian media is a mug's game. Any outlets forbidden by law or suspended by the social media giants would simply jump to the Russian-founded social media platform Telegram, which abhors regulation. Rather than playing whack-a-mole outlet by outlet, Ukraine's allies would be better off exposing how these disinformation networks work.** Many of these social media pages, self-styled think tanks, blogs and media outlets are designed to look fully independent and authentic. Efforts by Twitter, Alphabet and Meta to expose them as disinformation have been inconsistent. **Berlin-based, Moscow-run video aggregator Ruptly is "state-affiliated media," according to Twitter, but "state-controlled media" per Facebook; its"transparency" feature notes that the outlet's page administrators are in three EU countries, but doesn't name them.** Some smaller but perhaps more effective outlets **— such as the French-language Donbass Insider, which** has used manipulative practices to spread Kremlin disinformation on its Facebook page — carry no disclaimer at all.

1) 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 bonafide 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.

2) 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 news 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.

3) More Americans are turning to social media for their news

Forbes, June 24, 2020,
https://www.forbes.com/sites/mikevorhaus/2020/06/24/people-increasingly-turn-to-social-media-for-news/?sh=37284ed13bcc

In these days of pandemic, protests, economic recession and angst among the world's population a recently issued report shows that consumers continue to shift away from traditional media sources for their news and are moving more towards social media and messaging services to find the news. Long gone are the days of people getting most of their news from a local TV station, their local newspaper or the national newscast from one of the networks. Over 15 years ago, we already saw the substantial decay of Americans using traditional news sources and instead the Internet becoming a major source of news, particularly for the 18 to 34 year old demographic. This data comes from a study done for Carnegie Corporation in 2005. A research group I led at the time was responsible for the study. Carnegie Corporation is a major U.S. charitable foundation with a significant interest in journalism and news. As newspapers have fallen dramatically in usage, and the national newscasts have dropped in ratings, the swing to new sources of information has accelerated considerably. Reuters Institute for the Study of Journalism at Oxford University has recently issued a report on the state of digital news around the world. One of the very notable facts coming out from the study is the heavy use of Instagram for news which could soon possibly overtake Twitter. Instagram news consumers were 11% of the social media population. Twitter was statistically tied at 12%. Just as we found in 2005 for Carnegie Corporation, the shift away from traditional news media sources is being led by the younger generation, in this case people under 25 years old. Two-thirds of that age cohort said they use Instagram for gathering news information. The same age group reported that they were two times more likely to look at news on social media apps. Facebook leads with 36% of social media consumers using the social media giant for consuming news. YouTube had 21% of social media users looking at news on the popular video site. WhatsApp had 16% of consumers in that group and 12% used Twitter. Facebook owns both Instagram and WhatsApp. In this time of political and social upheavals, it is interesting to note that the Reuters study (conducted by YouGov, a research agency) only found 14% of people in the US trusted news on social media compared to 22% in regard to news gathered from search engines. Also, as further evidence of the power of social media in driving news to consumers, social media as a news source, saw ongoing growth with news consumers, unlike platforms such as all online sources combined, TV, and print. When thinking about what we know about the news and where we get our news, I reflect back on Will Rogers' famous quote: "All I know is just what I read in the papers, and that's an alibi for my ignorance."

THE IMPACT IS AMERICAN FASCISM, WAR AND ECONOMIC COLLAPSE

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/)

But there's another political regime, a historical one, that may portend an even more dire future for the U.S.: the Weimar Republic. The situation in Germany in the 1920s and early 1930s was of course sui generis; in particular, the country had experienced staggering traumas – defeat in war, internal revolution and hyperinflation – while the country's commitment to liberal democracy was weakly rooted in its culture. But as I read a history of the doomed republic this past summer, I tallied no fewer than five unnerving parallels with the current U.S. situation. First, in both cases, a charismatic leader was able to unify right-wing extremists around a political program to seize the state. Second, a bald falsehood about how enemies inside the polity had betrayed the country – for the Nazis, the "stab in the back," and for Trumpists, the Big Lie – was a vital psychological tool for radicalizing and mobilizing followers. Third, conventional conservatives believed they could control and channel the charismatic leader and rising extremism but were ultimately routed by the forces they helped unleash. Fourth, ideological opponents of this rising extremism squabbled among themselves; they didn't take the threat seriously enough, even though it was growing in plain sight; and they focused on marginal issues that were too often red meat for the extremists. (Today, think toppling statues.)To my mind, though, the fifth parallel is the most disconcerting: the propagation of a "hardline security doctrine." Here I've been influenced by the research of Jonathan Leader Maynard, a young English scholar who is emerging as one of the world's most brilliant thinkers on the links between ideology, extremism and violence. In a forthcoming book, Ideology and Mass Killing, Dr. Leader Maynard argues that extremist right-wing ideologies generally don't arise from explicit efforts to forge an authoritarian society, but from the radicalization of a society's existing understandings of how it can stay safe and secure in the face of alleged threats.Hardline conceptions of security are "radicalized versions of familiar claims about threat, self-defense, punishment, war, and duty," he writes. They are the foundation on which regimes organize campaigns of violent persecution and terror. People he calls "hardliners" believe the world contains many "dangerous enemies that frequently operate in and through purported 'civilian' groups." Hardliners increasingly dominate Trumpist circles now.Dr. Leader Maynard then makes a complementary argument: Once a hardline doctrine is widely accepted within a political movement, it becomes an "infrastructure" of ideas and incentives that can pressure even those who don't really accept the doctrine into following its dictates. Fear of "true believers" shifts the behaviour of the movement's moderates toward extremism. Sure enough, the experts I recently consulted all spoke about how fear of crossing Mr. Trump's base – including fear for their families' physical safety – was forcing otherwise sensible Republicans to fall into line.The rapid propagation of hardline security doctrines through a society, Dr. Leader Maynard says, typically occurs in times of political and economic crisis. Even in the Weimar Republic, the vote for the National Socialists was closely correlated with the unemployment rate. The Nazis were in trouble (with their share of the vote falling and the party beset by internal disputes) as late as 1927, before the German economy started to contract. Then, of course, the Depression hit. The United States today is in the midst of crisis – caused by the pandemic, obviously – but it could experience far worse before long: perhaps a war with Russia, Iran or China, or a financial crisis when economic bubbles caused by excessive liquidity burst.

NON-UNIQUE

1) Russia will not increase aggression when AFF passed

Beth George, May 13, 2022 Beth served as the Acting General Counsel for the U.S. Department of Defense during the beginning of the Biden-Harris administration. Previously, Beth served as Deputy General Counsel to the U.S. Department of Defense (DoD), where she advised senior leadership on legislative, policy, and oversight matters. From 2011 to 2016, Beth served in various roles for the National Security Division of the U.S. Department of Justice (DOJ), including as Counsel to the Assistant Attorney General, Counsel to the Office of Law & Policy, and as an Honors Attorney and Attorney-Adviser in the Office of Intelligence. https://www.justsecurity.org/81519/russian-threats-and-cybersecurity-qa-with-beth-george/

Should we expect to see an increase in Russian cyber attacks against the United States and other countries providing support to Ukraine as the crisis draws on? If so, what kinds of attacks would you predict we'll see, and do you think potential targets – particularly private companies – are sufficiently prepared? Since the earliest days of the Russian invasion of Ukraine, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) has been issuing prominent warnings about the potential for an increase in Russian attacks against U.S. companies. They launched a campaign called "Shields Up" to provide warning and guidance to companies regarding potential Russian threats. Interestingly, in the private sector, what we noticed around the time of the Russian invasion was a decrease in attacks that cybersecurity professionals generally attributed to Russian state-sponsored and state-affiliated hacking organizations, particularly regarding ransomware. Last fall, ransomware attacks appeared to be at their highest, with attacks against private companies happening on a routine basis, although many of the attacks were not existential for the company involved or didn't compromise major systems. (Anecdotally, in October 2021, multiple forensic companies I work with reported that they were at capacity for ransomware attacks and were unable to take on additional clients.) But by the time of the invasion, ransomware attacks had significantly dropped off, and those of us who work in the private cybersecurity sector remarked quietly among ourselves that it was disconcertingly quiet. It is unclear – at least based on publicly available information – whether this is related to Russian state-sponsored and state-affiliated hackers focusing their efforts on the war in Ukraine or if there has been some other type of disruption in their operations, perhaps due to efforts by the U.S. government to address ransomware gangs.

2) A sweeping Russian cyber attack is unlikely

Rob Kuznia et al, March 16, 2022 Kuznia worked at The Torrance Daily Breeze where he won the 2015 Pulitzer Prize for local reporting alongside two colleagues for uncovering a web of corruption in a Los Angeles County school district. He also founded a class at the University of Southern California..https://www.cnn.com/2022/03/16/politics/russia-us-cyberattack-infrastructure-invs/index.html

To be sure, a ripple of smaller cyberattacks ricocheted through the websites of Ukrainian banks and government agencies just before the invasion, and larger attacks may still be in store for the besieged country of 43 million people. But the general consensus among the nearly 20 experts who spoke with CNN for this story is that while Russia is well positioned to launch catastrophic cyberattacks on the US, it is not likely to do so. "We do need to consider this possibility as a low probability but high-impact scenario," said Paul Prudhomme, the head of threat intelligence advisory at the cybersecurity firm IntSights. The prospects for a grand-scale cyberattack in America are low, experts say. For one, Putin understands that his country's cyber capabilities, though formidable, are outmatched by those of the United States, which is generally thought to be the most sophisticated player in the domain. The federal Cybersecurity and Infrastructure Security Agency told CNN it hasn't yet received any credible cyber threats resulting from the conflict in Ukraine, but it emphasized that the energy sector has been bolstering its defenses in recent years and is on high alert as it urgently prepares for any attempted breach. Experts say Russia's ability to conduct an impactful cyberattack in the US shouldn't be underestimated."

NO IMPACT

1) RUSSIA WILL NOT ATTACK BECAUSE OF CURRENT THREATS FROM THE U.S

Beth George, May 13, 2022 Beth served as the Acting General Counsel for the U.S. Department of Defense during the beginning of the Biden-Harris administration. Previously, Beth served as Deputy General Counsel to the U.S. Department of Defense (DoD), where she advised senior leadership on legislative, policy, and oversight matters. From 2011 to 2016, Beth served in various roles for the National Security Division of the U.S. Department of Justice (DOJ), including as Counsel to the Assistant Attorney General, Counsel to the Office of Law & Policy, and as an Honors Attorney and Attorney-Adviser in the Office of Intelligence. https://www.justsecurity.org/81519/russian-threats-and-cybersecurity-qa-with-beth-george/

How serious are the potential threats to critical infrastructure in the United States from hostile cyber operations, and do you anticipate Russia targeting U.S. critical infrastructure? There have been efforts across multiple administrations to raise awareness of cybersecurity threats to critical infrastructure, to share threat information with companies that own or operate critical infrastructure, and to improve private-public partnerships to further harden and protect these companies. Most recently, on March 15, 2022, the President signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (within the Consolidated Appropriations Act), which will require entities determined to be critical infrastructure to report substantial cyber incidents within 72 hours and ransomware payments within 24 hours to CISA. But it's unlikely that it will have an impact any time soon – the statute allows the CISA director until September 2025 to establish implementing regulations. And because passage of the bill was strongly criticized by the Department of Justice and the Federal Bureau of Investigation, there could be significant interagency fighting about the scope and content of the proposed rulemaking. Perhaps more importantly, in June 2021, after the Colonial Pipeline ransomware attacks, President Biden warned Putin that 16 critical infrastructure sectors should be off-limits from cyberattacks. Although it is not clear what the Biden administration has planned or specifically warned in the event of a critical infrastructure attack attributed to Russia, the presidential notice clearly raises the stakes for Russia: Putin must certainly expect that such attacks will have a significant response from the United States. In that warning, however, the administration took pains to differentiate between "destructive" hacks and "conventional digital espionage operations carried out by intelligence agencies worldwide." In March of this year, Deputy National Security Advisor Anne Neuberger issued a public warning that the U.S. government is observing "threat intelligence that the Russian government is exploring options for potential cyberattacks on critical infrastructure in the United States." One can imagine that what the U.S. is observing is Russia conducting the very espionage activities that the U.S. was careful to distinguish as not off limits, but whether the Kremlin decides to exploit any vulnerabilities it has found or accesses it has established is what matters. Regardless of President Biden's warning, Putin certainly understands that there is a big difference between hacking private email accounts of administration officials and dumping the emails for an embarrassment campaign, compared to an attack that impacts water, electricity, or communications systems in the United States. Russia will always want the option to disable the critical infrastructure in the United States – much the same way other countries proactively seek to understand weaknesses in their adversaries' defenses. But I would be surprised if Putin were to take action against U.S. critical infrastructure because of the potential for it to result in significant escalation, whether of the conflict in Ukraine or more generally. So despite the necessary focus on preparing for critical infrastructure cyber attacks, I would be more concerned about attacks on private companies or further disinformation campaigns.

2) A large scale cyber attack is the only way America would engage in conflict

Zachary Wolf, March 22, 2022, Zach Wolf writes the What Matters newsletter for CNN. He also serves as a senior writer for CNN Politics, where he writes political analysis. https://www.cnn.com/2022/03/22/politics/russian-cyberattacks-what-matters/index.html

When is a cyberattack an act of war? I called Tess Bridgeman, co-editor in chief of the website Just Security and a former attorney in the Obama White House who is an expert on war powers and international law. "If a cyberattack causes significant death, destruction or injury, of the same sort that you would see from a more traditional attack using kinetic means, like bullets or missiles, you know, then you would call it a 'use of force' in international law," she said. A cyberattack that targeted a dam or air traffic control towers might rise to this level, but the government would try very hard to avoid responding to a cyberattack with a military attack, she said. The attacks on the US to date have fallen short of the threshold to justify a military response. As the government seeks countermeasures to respond, Bridgeman said, there's a good chance they won't be publicly known."It may appear that the US is sitting by idly, but I would be highly doubtful that that's the case," she said, arguing that defensive actions might be more effective at de-escalating the standoff. "It's setting the example for what responsible state behavior looks like."The threat of a military response is always there for the worst cyberattacks, should they cost American lives. "Our policy, our declared policy is, if it's a big enough attack on us and it hurts us, we will use the conventional weapons response," Richard Clarke, who was a top adviser to President George W. Bush on cybersecurity, told CNN's Michael Smerconish shortly after the war in Ukraine began.

3) Russia will not attack the US over cyber security concerns

Zachary Wolf, March 22, 2022, Zach Wolf writes the What Matters newsletter for CNN. He also serves as a senior writer for CNN Politics, where he writes political analysis. https://www.cnn.com/2022/03/22/politics/russian-cyberattacks-what-matters/index.html

Most of these attacks are meant to be part of espionage campaigns or to be meddlesome rather than deadly. Clarke argued that Russian attacks on US industries could be more devastating than attacks on the government itself. He said the government doesn't really know what would happen if the Amazon, Google and Microsoft cloud systems went offline, for instance. "I can tell you if those clouds go down, the United States stops working, our economy stops working, the phones stop working -- we will find ourselves pretty soon in the dark ages if the internet goes down," said Clarke. It's not clear that Russia would want to provoke the US specifically in a such a devastating way, or how the US would respond. While its cyberattacks in Ukraine since the war began have been less severe than some expected, according to a report by Lyngass, Russia has targeted internet infrastructure in parts of the country. There has been concern that cyberattacks in Ukraine could spill over to nearby countries that are in NATO and could lead the organization to invoke Article 5 of its charter -- the principle that an attack on one member of NATO is an attack on all members. Could a cyberattack trigger Article 5? A cyberattack could absolutely trigger Article 5. NATO Secretary General Jens Stoltenberg made this clear in February just after Russia's invasion. "An attack on one will be regarded as an attack on all," Stoltenberg said at a news conference when asked about a potential Russian cyberattack. But he added that NATO would be very careful in assessing an attack and would make sure a cyberattack on Ukraine -- shutting off electricity, say -- that accidentally spilled over into Poland or Romania is not construed as an attack on those countries. He also said it's intentionally unclear what kind of cyberattack would rise to the level of invoking Article 5.

4) MISCALCULATIONS CAUSING CONFLICTS IN CYBER SECURITY IS EXTREMELY UNREALISTIC

Council on Foreign Relations, **May 20, 2015**, https://www.cfr.org/blog/preventing-conflict-cyberspace-triggered-miscalculation

To remedy the risk of conflict stemming from ambiguity in cyberspace, Brake recommends a series of preventive and mitigating policy recommendations, including: Congress should pass legislation that facilitates real-time information sharing within and between the private and public sectors. The White House should issue warnings to adversaries of the potential consequences of violating cyberspace norms, **such as "adjustments to network traffic, criminal sanctions, diplomatic condemnation, and U.S. Treasury actions."** Congress should create a Department of State Bureau of Internet and Cyberspace Affairs, **which would demonstrate that the United States gives as much weight to diplomatic policy options as it does military ones.** It should also make the National Security Agency director a Senate-confirmed position eligible for civilians. Missions other than intelligence should be shifted to other appropriate entities, including U.S. Cyber Command and the combatant commands. "When possible and appropriate, defense officials should highlight U.S. involvement in offensive cyber operations against states, terrorist groups, and other illicit actors to fortify the credibility of U.S. retaliatory capacity among potential adversaries."

5) SUPPLY CHAIN SECURITY IS ALREADY IMPROVING TO STOP FUTURE ATTACKS

Ernie Hayden, **November 2018, Ernest N. Hayden (Ernie), CISSP, GICSP (Gold), PSP, is an industrial control systems cyber and physical security subject matter expert. Previously, he was a cybersecurity lead at the Canada-based BBA Inc.; an executive consultant with Alexandria, Va.-based Securicon; and before that, he was managing principal, critical infrastructure protection/cybersecurity with Verizon.**https://www.techtarget.com/searchsecurity/tip/How-supply-chain-security-has-evolved-over-two-decades

After a six-year wait, new emphasis on supply chain security arose first with the U.S. National Strategy for Global Supply Chain Security, a bill signed by then-President Barack Obama. This strategy emphasized that earlier efforts were still important, but that there needed to be a new focus on cybersecurity in the supply chain. Later work in 2012 and 2015 continued to expand on the concept of physical and cyber supply chain security. **Such guidance included "NIST IR 7622: Notional Supply Chain Risk Management Practices for Federal Information Systems," and "NIST SP 800-161: Supply Chain Risk Management Practices for Federal Information Systems and Organizations." NIST IR 7622 offers some suggested guidelines and "... repeatable and commercially reasonable supply chain assurance methods ... and visibility throughout the supply chain." NIST SP 800-161 covers the concepts from NIST IR 7622, but it includes more specific guidance for U.S. federal agencies to follow to identify, assess and mitigate information and communications technology (ICT) supply chain risks. In parallel with the release of NIST SP 800-161,** the Utilities Telecom Council published cybersecurity supply chain guidance specifically for electric utilities in its document "Cyber Supply Chain Risk Management for Utilities -- Roadmap for Implementation." This report offered ideas and approaches for electric utilities to organize and approach cyber suppliers and minimize cybersecurity risks. **This emphasis on supply chain cybersecurity is not unique to the U.S. The European Union Agency for Network and Information Security (ENISA) published its own overview of ICT supply chain risks in August 2015. ENISA's summary of the concern is well-stated:** Governments, corporations, organizations, and consumers are increasingly reliant on ICT products and services, and thus on the supply chains that deliver them. As a result of this reliance threats to supply chains have attracted more attention, including the threat of intentional tampering during development, **distribution or operations, or the threat of substitution with counterfeit (including cloned or overproduced) components before or during delivery, and attacks against the economy through the supply chain.**

NO LINK

1) RUSSIA DOES NOT CARE ABOUT US CYBER SECURITY, ONLY UKRAINE'S

Josephine Wolff March 2, 2022, Wolff is associate professor of cybersecurity policy at The Fletcher School at Tufts University, https://time.com/6153902/russia-major-cyber-attacks-invasion-ukraine/

In the relatively short and rapidly evolving history of cyber conflict, perhaps nothing has been established with greater certainty and more widely accepted than the idea that Russia has significant cyber capabilities and isn't afraid to use them—especially on Ukraine. In 2015, Russian government hackers breached the Ukrainian power grid, leading to widespread outages. In 2017, Russia deployed the notorious NotPetya malware via Ukrainian accounting software and the virus quickly spread across the globe costing businesses billions of dollars in damage and disruption. In the months that followed the NotPetya attacks, many people speculated that Ukraine served as a sort of "testing ground" for Russia's cyberwar capabilities and that those capabilities were only growing in their sophistication and reach. As tensions escalated between Russia and Ukraine, many people were expecting the conflict to have significant cyber components—the United States Department of Homeland Security even issued a warning to businesses to be on high alert for Russian cyberattacks, as did the U.K.'s National Cyber Security Centre. What is surprising is that—so far, at least—the devastating Russian cyberattacks everyone has been expecting have yet to materialize. There's no guarantee, of course, that a large-scale cyberattack on Ukraine's electrical grid or global banks or anything else isn't just around the corner. Russia has proven time and again that it has few compunctions about targeting critical infrastructure and causing considerable collateral damage through acts of cyber aggression. But as the invasion continues with few signs of any sophisticated cyber conflict, it seems less and less likely that Russia has significant cyber capabilities in reserve, ready to deploy if needed. Instead, it begins to look like Russia's much vaunted cyber capabilities have been neglected in recent years, in favor of developing less expensive, less effective cyber weapons that cause less widespread damage and are considerably easier to contain and defend against.

2AC Answers to Russia DA

Russia's invasion of Ukraine is not in response to NATO expansion. NATO has expanded in previous years, yet Russia did not react.

Popova & Shevel, 2022, (Maria is a Jean Monnet Chair and Associate Professor of Political Science at McGill University, Oxana is an Associate Professor in the Department of Political Science at Tufts University's School of Arts and Sciences), "Russia's Invasion of Ukraine Is Essentially Not About NATO". Just Security. 02/24. https://www.justsecurity.org/80343/russias-new-assault-on-ukraine-is-not-entirely-maybe-not-even-largely-about-nato/

In his Feb. 15 Just Security article "Ukraine: Unleashing the Rhetorical Dogs of War," Barry Posen argued that NATO and Ukraine should have cut a deal with Russia because the Ukrainian military would surely be defeated by Russia without direct U.S./Western military participation and U.S. offers of equipment were only encouraging a potential Ukrainian insurgency against Russian occupation that would be as bloody as it would be futile. The prescription depends entirely on Posen's assumption that to satisfy Russia, all Ukraine would have had to do would be "to swallow the bitter pill of accepting armed neutrality between NATO and Russia, rather than NATO membership." This assumption contradicts events of recent months and the historical record. While Vladimir Putin has claimed that his goal is keeping Ukraine out of NATO, he also insisted that he was just conducting military exercises. Instead, he is invading Ukraine again. He likewise insisted in 2014 that he wasn't capturing Crimea, despite the presence of his unidentified "Little Green Men" and his subsequent annexation of the peninsula, or that he was not fighting in Ukraine's Donbas area in the east all these years, despite all evidence to the contrary. There is no reason to take Putin at his word. His Feb. 21 diatribe conferring Russian recognition of independence for the two eastern Ukrainian regions of Donetsk and Luhansk and his order for Russian troops to move in as ostensible "peacekeepers" shows clearly his disdain for diplomatic resolutions. Moreover, this is not even primarily about NATO. NATO's eastward expansion may have played a role in straining the relationship between Russia and the West, but mainly because, for Russia, seeing former satellites eagerly abandon it for the greener pastures of Euro-Atlantic integration stung. However, Putin's rhetoric and actions over almost two decades reveal that his goals extend beyond imposing neutrality on Ukraine or even staving off further NATO expansion. The larger objective is to re-establish Russian political and cultural dominance over a nation that Putin sees as one with Russia, and then follow up by undoing the European rules-based order and security architecture established in the aftermath of World War II. Given these goals, Ukrainian neutrality is a woefully insufficient concession for Putin. If Russia's main concern had been NATO enlargement, it would have reacted with rhetoric and/or hostile actions in its neighborhood after each step in the NATO expansion process. The largest wave of NATO's eastward expansion took place in March 2004, when seven Eastern European countries joined, including the formerly Soviet Baltic states. Russia "grumbled," as the New York Times put it then, by adopting a Duma resolution criticizing the expansion, but no hostile and sustained rhetoric followed about NATO enlargement as a Western plot against Russian interests.

RUSSIA IS TOO FAR BEHIND TECHNOLOGICALLY TO REACH US ADVANCEMENTS IN AI AND CYBERSECURITY INNOVATION.

Chernenko and Markotkin, 2020, (Elena is a journalist with Kommersant newspaper.and Nikolai is an expert with the Russian International Affairs Council), "Developing Artificial Intelligence in Russia: Objectives and Reality". Carnegie Endowment for International Peace. 05/08. https://carnegiemoscow.org/commentary/82422

The Russian government finances industry-specific projects—quite generously by Russian standards—which testifies to the high priority assigned to this field. The application of AI in the military industry, in which Russia's position is traditionally strong, is the subject of particular attention. Nevertheless, it is unlikely that Russia will become a leader in the development of AI as set forth in the national strategy because of its current lag behind the leading technological powers, as well as some other factors, such as a small venture capital investment market. Unlike China and the United States, Russia isn't a global leader in AI technologies. Although the strategy states that "the Russian Federation possesses significant potential to become one of the international leaders in the development and use of artificial intelligence technologies," it's unlikely the country will be able to achieve this goal in the short and medium term. Nevertheless, certain areas of AI development and application do exist; Russia enjoys strong positions there and can succeed in the future. Russia's ranking in the AI technology race is hard to establish, since current international ratings use different methodologies. Many of them don't list Russia at all, which is unsurprising, since the country lacked an official AI development strategy until November 2019.

In terms of individual AI-related technology indicators, Russia has only three supercomputers ranked among the 500 most powerful computers in the world, for example, while China has 228, the United States has 117, and Japan has 29. The number of AI start-ups in a given country is also a key indicator of its progress in this field. According to TRAXCN statistics, Russia currently has 168 AI start-ups, compared with 6,903 in the United States and 1,013 in China. These estimates appear to be somewhat exaggerated, since the list includes twenty- and thirty-year-old "start-ups," but still, they make it possible to assess the bigger picture of the state of venture capital investment markets with respect to AI. In part, the small number of Russian AI start-ups can be explained by the domination of established companies in this sphere. This is what distinguishes Russia from most other developed technological powers. According to Russia's proposed Artificial Intelligence road map, the country has a total of 400 companies working on developing AI.

In November 2019, the RDIF reported that it had raised $2 billion in domestic and international investments in Russian companies that use AI. The RDIF will also undertake to bring these companies to international markets. According to some media publications, the fund will invest some of its money in creating an Artificial Intelligence Institute at Moscow State University. Such investment volumes are unique for Russian science. But how significant are they on a global scale? It is certainly far less than the leaders of the tech race spend on AI. China annually invests tens of billions of dollars in AI, including at a regional level. Beijing alone is planning to invest $2.1 billion in an AI industrial park, while Tianjin is considering the creation of a $16 billion AI development fund. In turn, the U.S. government allocated $4.9 billion for AI research in 2020. Venture investors have contributed even more, investing over $8 billion in AI start-ups in 2018 alone. As of today, Russia cannot be described as a leader in the AI race. Even if AI development becomes Russia's highest priority, Moscow essentially has no chance of catching up with Washington and Beijing in this field.

THE CURRENT GLOBAL ECONOMY IS STRONG AND RAPIDLY RECOVERING FOLLOWING COVID-19.

Conference Board, 2021, (Conference Board is a member-driven think tank that delivers trusted insights for what's ahead), "Global Economy Enters 2022 in Strong Health after Surprisingly Swift Pandemic Recovery—But New and Pre-Existing Conditions Cloud the Long-Term Prognosis". Conference Board. 11/03.
https://www.conference-board.org/topics/global-economic-outlook/press/global-economic-outlook-2022

The global economy is set for another year of above-potential recovery growth in 2022, after expanding by a robust 5.1% in 2021. Global Economic Outlook 2022: From Pandemic Downturn to Growth Revival, our suite of forecasts for the decade ahead, tracks the future of this historically rapid resurgence with detailed analyses for the US, Europe, China, and the Gulf region.

"Despite the depth of the recession in the first half of 2020—and the unexpected setbacks of the Delta variant in 2021—the global economy has recovered rapidly from the pandemic shock compared to past recessions," said Dana M Peterson, Chief Economist of The Conference Board. "Massive fiscal and monetary stimulus in major economies around the world—which built a bridge to economic reopening enabled by the rapid development of effective vaccines—likely prevented the recession from devolving into a long period of lackluster economic growth."

Indeed, global GDP—which contracted by an unprecedented 3.3% in 2020—is calculated to have recovered all of its losses by Q1 2021. By the end of 2022, 66 out of 77 key economies, representing 96% of global GDP, should be at or above pre-pandemic output levels, though labor market and income recovery will lag somewhat.

Putin is not concerned about NATO expansion given statements about Sweden and Finland seeking membership.

Bove, 2022, (Tristan is a graduate of DePaul University with degrees in International Studies and Chinese), "Putin says Sweden and Finland joining NATO and breaking with decades of neutrality is fine after all. 'No problems'". Fortune. 05/16. https://fortune.com/2022/05/16/sweden-finland-join-nato-putin-no-threat-russia/

But three months into a Ukraine invasion that's not going according to plan, and after two other countries close to Russia announced that they are joining NATO, Putin appears to be softening his tone, and resigning himself to the fact that NATO's eastward expansion is happening anyway.

On Sunday, Finland—which shares an 800-mile border with Russia and was part of the Russian Empire for over a century—said it had applied to join NATO to ensure that its own national security would not be threatened by Russia in the future. On Monday, Sweden followed suit after a meeting amongst ruling party officials over the weekend, who voted to end the country's 200-year neutrality policy. Minister Magdalena Andersson said on Sunday. "We're facing a fundamentally changed security environment in Europe."

For months, Russian officials have warned against the two countries taking this decisive step, but now that it has actually happened, Putin appears to be doing his best to diminish the significance of the act. "As for the expansion of NATO, including through new members of the alliance which are Finland, Sweden — Russia has no problems with these states," Putin said Monday at a summit of the Collective Security Treaty Organization, a military alliance composed of several post-Soviet states.

For months, Russian officials have been saying that should Finland and Sweden join NATO, Russia would receive it as a threat, and respond by building up its military capabilities in the Baltic Sea. Former Russian president Dmitry Medvedev even suggested in April that nuclear weapons and hypersonic missiles could be deployed. Just last week, Putin warned that Finland joining NATO would be a "mistake," and suggested that Russia would interpret it as an act of aggression. But Putin signaled on Monday that Finland and Sweden's decision to join NATO is one of relative unimportance, and does not constitute a danger to Russia. "Expansion at the expense of these countries does not pose a direct threat to Russia," he said.

Russia's current fight to lead AI and cybersecurity innovation futile due to their focus on Ukraine.

Whyte, 2022, (Christopher is an assistant professor in the homeland security and emergency preparedness program in the Wilder School of Government and Public Affairs at Virginia Commonwealth University), "Russia's AI setbacks will likely heighten its cyber aggression". CSO. 04/14. https://www.csoonline.com/article/3656957/russias-ai-setbacks-will-likely-heighten-its-cyber-aggression.html#:~:text=With%20the%20weight%20of%20Western,AI

The consequences of the war waged against Ukraine on Russia's wealth, workforce and access to sophisticated imported products such as microprocessors used to operate everything from mobile devices to automobiles are immense. Without capital, talent and a line on critical commodities and technologies, Russia will struggle to be competitive in everything from medical technology development to national security practice. This likely result of increasing isolation seems doubly assured with AI. Russia's relatively weak fundamentals and strong competition from both China and the West virtually guarantee vast opportunity costs to Russia in years to come. This outcome might be seen as a positive development that will cede techno-strategic advantages to defense communities in North America, Europe and East Asia--those most concerned about Russia's military capabilities and intentions.

Despite Putin's statements, Russia's AI efforts have lagged behind most initiatives in other countries. In 2014, barely two years after a breakthrough innovation of deep neural networks by a multinational group of researchers energized AI development, Russia's buildout of new machine learning applications and other AI tools was already slowing significantly. Collaborations with cutting-edge projects in the West, China, India and elsewhere began to drop away following Putin's annexation of Crimea and decision to embroil Eastern Ukraine in ongoing conflict. State-sponsored companies and military-intelligence institutions in the Russian Federation have consistently been a leading source of novel AI technologies aimed at bolstering national security and strengthening mechanisms of population control. However, a slow leak of human capital and a complicated relationship with parts of the global economy that dominate critical high technology resources, such as graphics processing units (GPUs), have become a substantial obstacle for the country's AI ambitions. Even if Moscow matched China's or the United States' levels of domestic AI investment, its fundamentals of innovation for the field simply haven't been concrete for some time.

One major blow to Moscow's AI ambitions is the dramatic acceleration of the brain drain that has plagued Russian high technology and scientific communities for years. Enticing researchers out of private industry and academia is perennially difficult for governments, but Russia has been even less capable in this regard than most, likely due to the unappealing culture and benefits of Putin's military and paramilitary communities. Now, up to 70,000 tech workers that were otherwise minimal flight risks have fled the country. Many have ended up in former Soviet states and South Asia, and no small number have left positions tied to the Russian state's focus on building out facial recognition, autonomous vehicles and surveillance capabilities. Sanctions worsen the impact of this brain drain by cutting across the research and business relationships that Moscow has heavily supported in recent years.

THE GLOBAL ECONOMY IS IN RECOVERY WITH POSITIVE OUTLOOK AHEAD.

OECD, 2021, (OECD is a global policy forum that promotes policies to preserve individual liberty and improve the economic and social well-being of people around the world), "Global economic recovery continues but remains uneven, says OECD". OECD. 09/21. https://www.oecd.org/newsroom/global-economic-recovery-continues-but-remains-uneven-says-oecd.htm

The global economy is growing far more strongly than anticipated a year ago, but the recovery remains uneven, exposing both advanced and emerging markets to a range of risks, according to the OECD's latest Interim Economic Outlook. The OECD says extraordinary support from governments and central banks helped avoid the worst once the COVID-19 pandemic hit. With the vaccine roll-out continuing and a gradual resumption of economic activity underway, the OECD projects strong global growth of 5.7% this year and 4.5% in 2022, little changed from its May 2021 Outlook of 5.8% and 4.4% respectively. Countries are emerging from the crisis with different challenges, often reflecting their pre-COVID 19 strengths and weaknesses, and their policy approaches during the pandemic. Even in the countries where output or employment have recovered to their pre-pandemic levels, the recovery is incomplete, with jobs and incomes still short of the levels expected before the pandemic. Presenting the Interim Economic Outlook alongside Chief Economist Laurence Boone, OECD Secretary-General Mathias Cormann said: "The world is experiencing a strong recovery thanks to decisive action taken by governments and central banks at the height of the crisis. But as we have seen with vaccine distribution, progress is uneven. Ensuring the recovery is sustained and widespread requires action on a number of fronts – from effective vaccination programmes across all countries to concerted public investment strategies to build for the future."