# Cyber Intel AFF Supplement – CNDI 2022

# AFF

## Uniqueness Extensions

### 2AC --- UQ Russia Cyber Attacks Now --- Ukraine Example

#### Russia cyber attacking Ukraine now – shows capabilities

Bannister 22 (Adam Bannister, In recent years Adam has written news, features, and white papers on intrusion detection, video surveillance, and physical-access control, with cybersecurity increasingly to the fore. The history graduate also covered entrepreneurship and, more recently, fire safety before joining *The Daily Swig*, ‘Russia behind cyber-attack on satellite internet network KA-SAT that disrupted Ukrainian infrastructure – EU’, The Daily Swig, 10 May 2022 at 12:52 UTC, https://portswigger.net/daily-swig/russia-behind-cyber-attack-on-satellite-internet-network-ka-sat-that-disrupted-ukrainian-infrastructure-eu)

**The EU has blamed Russia for a powerful cyber-attack that disrupted satellite broadband services in Ukraine** and “helped facilitate President Vladimir Putin’s invasion of the country”.Thousands of modems were knocked offline by the attack on the KA-SAT network, which took place one hour before Russia’s invasion of Ukraine commenced on February 24.**The incident caused communication outages and other disruptions for government websites and banks in Ukraine, and affected several EU Member States that also use the KA-SAT network.**The KA-SAT satellite and network is operated by US telecoms giant Viasat, which provides connectivity to military as well as commercial customers. **“This unacceptable** [**cyber-attack**](https://portswigger.net/daily-swig/cyber-attacks) **is yet another example of Russia’s continued pattern of irresponsible behaviour in cyberspace, which also formed an integral part of its illegal and unjustified invasion of Ukraine,”** reads a statement issued today (May 10) **by the Council of the EU.Cyber-attacks against** [**critical infrastructure**](https://portswigger.net/daily-swig/critical-infrastructure) “could spill over into other countries and cause systemic effects putting the security of Europe’s citizens at risk”, it warned.“The European Union, working closely with its partners, is considering further steps to prevent, discourage, deter and respond to such malicious behaviour in cyberspace. The European Union will continue to provide coordinated political, financial and material support to Ukraine to strengthen its cyber resilience.”Viasat revealed in a [statement](https://www.viasat.com/about/newsroom/blog/ka-sat-network-cyber-attack-overview/) issued on March 30 that a “targeted denial of service attack made it difficult for many modems to remain online”, and that an attacker had exploited a misconfiguration in a VPN appliance to gain remote access to the KA-SAT network.

### 2AC --- UQ --- Hacks

#### Risk of cyber-attacks high

Nichols 22(Shaun Nichols, with 15 years of experience as a reporter, Shaun Nichols has been covering the enterprise technology market since the days when the iPod had a hard drive and phones had actual buttons. He has written for international publications including VNUnet, V3, The Register and Lawrence Berkeley National Laboratory, covering everything from embedded controllers to supercomputers, ‘US warns of 'increased' threats from Russian hacking groups’, TechTarget, April 20, 2022, <https://www.techtarget.com/searchsecurity/news/252516169/US-warns-of-increased-threats-from-Russian-hacking-groups>)

**U.S. government agencies are warning the public of an expected increase in cyber-attacks from hackers affiliated with the Russian government.** The Cybersecurity and Infrastructure Security Agency joined with the National Security Agency and Department of Justice in [an advisory](https://media.defense.gov/2022/Apr/20/2002980529/-1/-1/1/JOINT_CSA_RUSSIAN_STATE-SPONSORED_AND_CRIMINAL_CYBER_THREATS_TO_CRITICAL_INFRASTRUCTURE_20220420.PDF) detailing the threats posed by Russian hacking groups -- both state-sponsored [advanced persistent threat](https://www.techtarget.com/searchsecurity/definition/advanced-persistent-threat-APT) groups and also private cybercrime gangs that support Russia's invasion of Ukraine. **The advisory warned that organizations within Ukraine as well as outside the region, including the U.S., could see "increased malicious cyber activity."** "This activity may occur as a response to the unprecedented economic costs imposed on Russia as well as materiel support provided by the United States and U.S. allies and partners," the advisory said. Also signing the joint advisory were the four other members of the Five Eyes intelligence network: the U.K., New Zealand, Australia and Canada. Most notably, the advisory for the first time addressed the issue of private cybercriminal hacking groups either working directly with the Kremlin or acting on its behalf in vigilante-style hacking campaigns, as Russia continues to work on disrupting communications in Ukraine. "Since Russia's invasion of Ukraine in February 2022, some cybercrime groups have independently publicly pledged support for the Russian government or the Russian people and/or threatened to conduct cyber operations to retaliate against perceived attacks against Russia or materiel support for Ukraine," the advisory read. "**These Russian-aligned cybercrime groups likely pose a threat to critical infrastructure organizations."**

### 2AC --- UQ --- Ambiguity

#### Ambiguity of cyber operations will lead to escalation

Lonergan and Milo 22 [Erica D. Lonergan is an Assistant Professor in the Army Cyber Institute at West Point and a Research Scholar at the Saltzman Institute of War and Peace Studies at Columbia University. Previously, she served as a Senior Director on the U.S. Cyberspace Solarium Commission. Keren Yarhi-Milo is a political scientist specializing in the study of interstate communication, crisis bargaining, reputation and credibility, and the psychology of leaders and decision makers. “CYBER SIGNALING AND NUCLEAR DETERRENCE: IMPLICATIONS FOR THE UKRAINE CRISIS”, War on the Rocks, 4-21-22, https://warontherocks.com/2022/04/cyber-signaling-and-nuclear-deterrence-implications-for-the-ukraine-crisis/] SL

Policymakers and academics are attuned to the cyber risks to nuclear command and control. The practitioner community has largely focused on U.S. vulnerabilities and how to mitigate them. Scholars, in turn, worry about how cyber operations could have unintended escalatory consequences. But less attention has been paid to another likely scenario: the use of cyber operations for signaling purposes (operations with visible effects that aim to convey a message to another state) in a nuclear context. The ambiguity of cyber operations can sometimes be useful for signaling — but the same ambiguity can be dangerous during a nuclear crisis. The problem is that civilian leaders in particular, distinct from the military, are inclined to see cyber attacks as effective signaling tools. Cyber operations could have nuclear implications, especially because modern nuclear command and control systems, like those in Russia and the United States, are becoming increasingly dependent on digital infrastructure. Nuclear command, control, and communications systems, which include early warning, information collection, and communications capabilities, alert decision-makers to impending nuclear strikes and also enable leaders to control decisions about nuclear use (or non-use). But their digital dependencies are creating opportunities for exploitation using cyber means. In a 2020 report, the Nuclear Threat Initiative found that “almost 9 out of 10 planned nuclear modernization programs involve at least some new digital components or upgrades.” Vulnerabilities inherent in the digital infrastructure that undergird modern nuclear systems provide opportunities for actors to engage in cyber espionage — gaining access to a network or system to steal information — or even conduct cyber attacks. Hypothetically, a cyber power like Russia could conduct a cyber attack against a U.S. early warning satellite to degrade its functionality. This has become an urgent concern for practitioners. U.S. Strategic Command, for instance, is currently working to “operationally harden NC3 systems against cyber threats.” Congress has also gotten involved, requiring the Defense Department to evaluate the cybersecurity of major weapon systems. And the Government Accountability Office has published multiple reports decrying the state of cybersecurity and scope of vulnerabilities of weapon systems, including elements of the nuclear triad.

### 2AC --- UQ --- Russia Undermines NATO

#### Russian cyberattacks target current NATO rifts

Shea 17 [Jamie Shea is NATO Deputy Assistant Secretary General for Emerging Security Challenges. He has been working with NATO since 1980. Positions included Director of Policy Planning in the Private Office of the Secretary General, Deputy Assistant Secretary General for External Relations, Public Diplomacy Division, Director of Information and Press, Spokesman of NATO and Deputy Director of Information and Press, Deputy Head and Senior Planning Officer in the Policy Planning and Multilateral Affairs Section of the Political Directorate as well as Assistant to the Secretary General of NATO for Special Projects. “How is NATO Meeting the Challenge of Cyberspace”, Prism National Defense University, 12-21-17, https://cco.ndu.edu/News/Article/1401835/how-is-nato-meeting-the-challenge-of-cyberspace/] SL

Yet it is not the much discussed theme of the economic damage inflicted by cyber crime in the past year that has dominated the debate. It is more the use of cyber as an instrument of state policy, political influence, and manipulation. From being a useful tool of espionage and intellectual property theft, cyber intrusions have evolved into a potent instrument of hybrid warfare and outright political vandalism. Ukraine, for example, has been the victim of an unprecedented and systematic campaign of cyber bullying. It has acknowledged up to 2,000 orchestrated cyberattacks since Russia occupied Crimea in March 2014. It has suffered disruption to its election voting system, train and airline on-line booking, ports, electricity grid, and most recently, the massive elimination of tax and financial accounting data through the NotPetya malware. Initially disguised as a ransomware attack similar to the previous WannaCry, a hack that affected more than 200,000 computer networks in 150 countries, it soon became clear that the data encrypted was being destroyed, and that the motive of the attack was not financial gain but rather economic and structural sabotage. Although companies in other countries were also affected by NotPetya, 80 percent of the impact was in Ukraine.1 Intelligence analysts now agree that NotPetya was a state-driven effort. All of these orchestrated cyber campaigns suggest that Ukraine is being used as a laboratory or proving ground to test a range of cyber weapons and assess their impact, with widespread collateral damage elsewhere accepted as a consequence of doing business; or even as a way to cover tracks.2 Given the difficulty of technical attribution and the inability of governments to deter or retaliate against cyberattacks in a manner that demands the attacker’s attention but avoids unwanted escalation, NATO has had to take a hard look at its preparedness, not only to fend off cyberattacks but also to preserve its political and military freedom of navigation in the cyber domain. The revelation in a recent Washington Post article of how the Obama Administration rejected nearly all proposed responses to Russian incursions into the communications of the Democratic National Committee because they were deemed to be ineffective, escalatory, or would compromise long-term U.S. intelligence gathering and prematurely expose U.S. offensive cyber capabilities, caught NATO’s attention.3 There is growing awareness that Russian operational activity built around groups such as APT28 is aimed at inflicting damage to the reputation and cohesiveness of organizations such as NATO.4 Consequently, reducing the strategic cyber threat to the functionality of governments and societies and making cyberspace more stable and transparent has become as important to international peace and order as nuclear arms control or the conventional balance of power.

## Internal Link Extensions

### 2AC --- Financial Collapse Internal Link

#### Cyber-attacks will cause the next financial crisis

Mee and Schuermann 18 [Paul Mee and Til Schuermann,a partner at consulting firm Oliver Wyman and leads its cyber risk practice, a partner in Oliver Wyman’s financial services practice and was a senior vice president at the Federal Reserve Bank of New York during the financial crisis, September 14, 2018, “How a Cyber Attack could Cause the Next Financial Crisis”, *Harvard Business Review*, https://hbr.org/2018/09/how-a-cyber-attack-could-cause-the-next-financial-crisis]-Hayer

But the next crisis might not come from a financial shock at all. The more likely culprit: a cyber attack that causes disruptions to financial services capabilities, especially payments systems, around the world. Criminals have always sought ways to infiltrate financial technology systems. Now, the financial system faces the added risk of becoming collateral damage in a wider attack on critical national infrastructure. Such an attack could shake confidence in the global financial services system, causing banks, businesses and consumers to be stymied, confused or panicked, which in turn could have a major negative impact on economic activity. Cybercrime alone costs nations more than $1 trillion globally, far more than the record $300 billion of damage due to natural disasters in 2017, according to a recent analysis our firm performed. We ranked cyber attacks as the biggest threat facing the business world today — ahead of terrorism, asset bubbles, and other risks. An attack on a computer processing or communications network could cause $50 billion to $120 billion of economic damage, a loss ranking somewhere between those of Hurricanes Sandy and Katrina, according to recent estimates. Yet a much broader and more debilitating attack isn’t farfetched. Just last month, the Federal Bureau of Investigation issued a warning to banks about a pending large scale attack known as an ATM “cash-out” strike, in which waves of synchronized fraudulent withdrawals drain bank accounts. In July, meanwhile, it was revealed that hackers working for Russia had easily penetrated the control rooms of US electric utilities and could have caused blackouts. How might a financial crisis triggered by a cyber attack unfold? A likely scenario would be an attack by a rogue nation or terrorist group on financial institutions or major infrastructure. Inside North Korea, for example, the Lazarus Group, also known as Hidden Cobra, routinely looks for ways to compromise banks and exploit crypto currencies. An attack on a bank, investment fund, custodian firm, ATM network, the interbank messaging network known as SWIFT, or the Federal Reserve itself would represent a direct hit on the financial services system. Another possibility would be if a so-called hacktivist or “script kiddy” amateur were to use malicious programs to launch a cyber attack without due consideration of the consequences. Such an attack could have a chain reaction, causing damage way beyond the original intent, because rules, battle norms, and principles that are conventional wisdom in most warfare situations but don’t exist in a meaningful way in the digital arena. For example, in 2016 a script kiddie sparked a broad denial-of-service attack impacting Twitter, Spotify, and other well-known internet services as amateurs joined in for mischief purposes. Whether a major cyber attack is deliberate or somewhat accidental, the damage could be substantial. Most of the ATM networks across North America could freeze. Credit card and other payment systems could fail across entire nations, as happened to the VISA network in the UK in June. Online banking could become inaccessible: no cash, no payments, no reliable information about bank accounts. Banks could lose the ability to transact with one another during a critical period of uncertainty. There could be widespread panic, albeit temporary. Such an outcome might not cause the sort of long-simmering financial crisis that sparked the Great Recession, because money would likely be restored to banks and payments providers once systems were back online. At the same time, it isn’t clear how a central bank, the traditional financial crisis firefighter, could respond to this type of crisis on short notice. After the problem is fixed and the crisis halted, a daunting task of recovery would loom. It would be even more difficult if data were corrupted, manipulated or rendered inaccessible.

### 2AC --- Grids Vulnerability

#### The US’ pipelines and electric grids are vulnerable to cyberattacks.

Plumer 21 [Brad, a reporter covering climate change, energy policy and other environmental issues for The New York Times. Previously, he was a senior editor at Vox.com and a reporter at the Washington Post. “Pipeline Hack Points to Growing Cybersecurity Risk for Energy System”, 08 June 2021, The New York Times, <https://www.nytimes.com/2021/05/13/climate/pipeline-ransomware-hack-energy-grid.html> ] -ALP

Despite years of warnings, America’s vast network of pipelines, electric grids and power plants remains **acutely vulnerable to cyberattacks** with the potential to disrupt energy supplies for millions of people. Dealing with those risks, analysts said, will pose a major challenge for the Biden administration as it seeks hundreds of billions of dollars to modernize the nation’s energy infrastructure and transition to cleaner sources of energy to address climate change. Regulators are increasingly poised to step in. On Monday, Richard Glick, the chairman of the Federal Energy Regulatory Commission, said it was **time to establish mandatory cybersecurity standards** for the nation’s nearly 3 million miles of oil and gas pipelines, similar to those currently found in the electricity sector. “Simply encouraging pipelines to voluntarily adopt best practices is an inadequate response to the ever-increasing number and sophistication of malevolent cyber actors,” Mr. Glick said in a statement. The risks to the nation’s energy systems are widespread and varied. Many oil and gas pipelines, for instance, rely on decades-old control systems that are not well defended against more sophisticated cyberattacks and can’t be easily updated. And it’s not just pipelines. As electric grid operators harness a growing array of digital technologies to help manage the flow of power and cut planet-warming emissions — such as smart thermostats, or far-flung yet interconnected networks of solar arrays — hackers may find new entry points to exploit. The shutdown on Friday of the Colonial Pipeline, which stretches 5,500 miles from Texas to New Jersey and transports 45 percent of the East Coast’s fuel supplies, illustrates how devastating such attacks can be. On Saturday, Colonial acknowledged that its corporate computer systems had been hit by a ransomware attack, in which criminal groups hold data hostage until the victim pays a ransom. The company said that it had shut down the pipeline as a precaution, apparently for fear that the hackers might have obtained information that would enable them to attack parts of the pipeline itself. Colonial said on Wednesday that it had started to resume pipeline operations, though it would take several days to restore full service. But throughout the Southeast, panicked Americans were racing to stock up on gasoline, causing thousands of gas stations to run out of fuel. While Colonial has yet to explain exactly what triggered the pipeline shutdown, experts said there were plenty of vulnerabilities lurking throughout America’s energy infrastructure. Last year, the Cybersecurity and Infrastructure Security Agency reported a ransomware attack on a natural gas compression facility that caused a shutdown of the facility for two days. In 2018, several natural gas pipeline operators reported that a system that processes customer transactions had been attacked, leading to service disruptions. But bigger risks lurk: In 2016, hackers knocked out large sections of the power grid in Ukraine, which was thought to be **the first intentional blackout triggered by a cyberattack**. At the time, the Obama administration warned that America’s electric utilities were not immune to similar attacks. In the past, energy companies typically kept the operational systems that run pipelines or power plants disconnected, or “air gapped,” from the broader internet, which meant that hackers could not easily gain access to the most critical infrastructure. But increasingly that’s no longer the case, as companies install more sophisticated monitoring and diagnostics software that help them operate these systems more efficiently. That potentially creates new cybersecurity risks. “Now these systems are all interconnected in ways that the companies themselves don’t always fully understand,” said Marty Edwards, vice president of operational technology for Tenable, a cybersecurity firm. “That provides an opportunity for attacks in one area to propagate elsewhere.” Many industrial control systems were installed decades ago and run on outdated software, which means that even finding programmers to upgrade the systems can be a challenge. And the operators of vital energy infrastructure — such as pipelines, refineries or power plants — are often reluctant to shut down the flow of fuel or power for extended periods of time to install frequent security patches. Making things harder still, analysts said, many companies do not always have a good sense of exactly when and where it’s worthwhile to spend money on costly new cybersecurity defenses, in part because of a lack of readily available data on which types of risks they are most likely to face. “Companies don’t always release a lot of information publicly” about the threats they’re seeing, said Padraic O’Reilly, a co-founder of CyberSaint Security, who works with pipelines and critical infrastructure on cybersecurity. “That can make it hard as an industry to know where to invest.” Analysts said that the nation’s electric utilities and grid operators were typically further ahead in preparing for cyberattacks than the oil and gas industry, in part because federal regulators have long required cybersecurity standards for the backbone of the nation’s power grid. Still, vulnerabilities remain. “Part of it is the sheer complexity of the grid,” said Reid Sawyer, managing director of the United States cyberconsulting practice at Marsh, an insurance firm. Not all levels of the grid face mandatory standards, for instance, and there are more than 3,000 utilities in the country with varying cybersecurity practices.

### 2AC --- Nuclear Stability

#### Russian Hacks Threatens Nuclear Stability

Schneider 22 [Jacquelyn Schneider is a Hoover Fellow at the Hoover Institution at Stanford University. “The Biggest Cyber Risk in Ukraine?” Foreign Affairs, March 7, 2022. <https://www.foreignaffairs.com/articles/ukraine/2022-03-07/biggest-cyber-risk-ukraine?check_logged_in=1&utm_medium=promo_email&utm_source=lo_flows&utm_campaign=registered_user_welcome&utm_term=email_1&utm_content=20220628>] - NAAh

Just as many military experts predicted that a Russian invasion of Ukraine would be quick and decisive, so many cyber-experts expected that Moscow would fortify its conventional onslaught with a devastating cyberattack. Ukrainian forces would be blinded, critical infrastructure broken, and Russian disinformation rampant. But just as the military experts have been surprised by Russia’s stalled invasion, so have the cyber-experts by the lack of major digital attacks. In the first few days of conflict, cyber-operations seem to be more fizzle than bang. Some Russian cyber-activity has been discovered, but it seems to have done little to invigorate the Russian military campaign or hinder the Ukrainian response. In the run-up to the invasion, Russia launched wiper malware attacks, which deleted data from computers at Ukrainian government agencies. Russia also appears to have conducted some distributed denial-of-service attacks, which bombarded websites with so much information they became paralyzed, and a series of cybernetwork exploitation attempts on Ukrainian government and military systems. But Ukrainian air defense and aircraft didn’t appear to be affected by cyber-disruptions, and there are no reports of critical infrastructure damage from cyberattacks. Even the Internet seems to be up and running in Ukraine. Why the apparent restraint? It is almost impossible to know exactly why (or if) the Russians have indeed held back. Perhaps cyber-operations have been attempted and failed; perhaps Russian President Vladimir Putin has held his cyber-capabilities in reserve, saving them for later. Or maybe cyber-operations have taken place, but their effect—which is often virtual and not clearly attributed—will take longer to materialize. What is known is that the conflict is far from over, and the next question becomes whether cyber-operations could play a larger role as the war turns more violent. It is likely that the next stage of conflict will more than ever be defined by planes, tanks, artillery, and soldiers. It seems unlikely, given the amount of indiscriminate damage currently being inflicted by Russia, that cyber-operations will escalate the violence of the campaign within Ukraine. That said, could cyber-operations lead to horizontal escalation, drawing NATO into the fight, for example? Or, given that the United States and Russia are the world’s largest nuclear powers, could cyber-operations escalate to the worst possible outcome—nuclear war? Recent wargaming research suggests that cyber-exploits into nuclear command and control may be enticing for states looking to neutralize a nuclear escalation threat in the midst of a conventional war, and that actors may underestimate the danger of these exploits and vulnerabilities to nuclear stability.

## Impact Extensions

### 2AC --- Impact UQ --- Biden Escalates

#### Biden would escalate a cyber conflict with Russia now.

Meyer 22 (Josh Meyer, Josh Meyer is a veteran correspondent focusing on domestic, national and global security issues, including terrorism, extremism, cybersecurity and transnational criminal organizations, ‘Biden says 'we are prepared to respond' if Russia launches cyberattack against US’ USA Today, 8:02 PM Feb. 18, 2022, <https://www.usatoday.com/story/news/politics/2022/02/18/biden-administration-goes-shields-up-protect-u-s-russian-cyber-attack/6853643001/>)

President Joe Biden warned Thursday that if **Russia launches cyberattacks on American companies and critical infrastructure as part of its hybrid war campaign against Ukraine, “we are prepared to respond.”** Biden didn’t elaborate on what the U.S. response might be in his televised address in response to Russia’s stunning invasion of its western neighbor. But U.S. cybersecurity experts say such **a response could include a range of options ranging from bolstering America’s cybersecurity safety net to launching top-secret offensive cyberweapons against Russian targets including its own critical infrastructure.** Some of those responses are already underway. On Thursday, administration officials stepped up their campaign to implement a “shields up” effort to **protect** [**key parts of U.S. critical infrastructure**](https://www.usatoday.com/story/news/politics/2022/02/08/local-government-cybersecurity-digital-threats/9208951002/) **– such as pipelines, banks, commercial aviation and hospitals – from potential Russian cyberattacks linked to its invasion of Ukraine**, top U.S. security officials say.

#### A major cyber attack would destabilize the country – makes nuclear response more likely

Sagan and Weiner, 21(Scott D. Sagan and Allen S. Weiner, Scott D. Sagan is the Caroline S.G. Monroe professor of political science and senior fellow at the Center for International Security and the Freeman Spogli Institute at Stanford University. Before joining the Stanford faculty, he served as special assistant to the Director of the Organization of the Joint Chiefs of Staff. Allen S. Weiner is senior lecturer in law and director of the program in international and comparative law at Stanford Law School. Before joining the Stanford faculty, he served as a career attorney in the U.S. State Department. ‘The U.S. says it can answer cyberattacks with nuclear weapons. That’s lunacy.’, New York Times, July 9, 2021 at 3:46 p.m. EDT, https://www.washingtonpost.com/outlook/2021/07/09/cyberattack-ransomware-nuclear-war/)

Over the July 4 weekend, the **Russian-based cybercriminal organization REvil** [claimed credit](https://www.washingtonpost.com/national-security/ransomware-biden-russia/2021/07/06/ff52a9de-de72-11eb-b507-697762d090dd_story.html?itid=lk_inline_manual_2) **for hacking into as many as 1,500 companies in what has been called the largest ransomware** attack to date. In May, another cybercriminal group, DarkSide, also apparently located mainly in Russia, [shut down](https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html) most of the operations of Colonial Pipeline, which supplies nearly half the diesel, gasoline and other fuels used on the East Coast — setting off a round of panic buying that ended only when the company handed over a ransom. These incidents were bad enough. But **imagine a much worse cyberattack, one that not only disabled pipelines but turned off the power at hundreds of U.S. hospitals, wreaked havoc on air-traffic-control systems and shut down the electrical grid in major cities in the dead of winter.** The grisly cost might be counted not just in lost dollars but in the deaths of many thousands of people. Under current U.S. nuclear doctrine, developed during the Trump administration**, the president would be given the military option to launch nuclear weapons at Russia, China or North Korea if that country was determined to be behind such an attack.** That’s because [in 2018](https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF), the Trump administration expanded the role of nuclear weapons by declaring for the first time that the United States would consider nuclear retaliation in the case of **“significant non-nuclear strategic attacks,”** including **“attacks on the U.S., allied, or partner civilian population or infrastructure.”** The same principle could also be used to justify a nuclear response to a devastating biological weapons strike.

### 2AC --- Impact --- CW = NW

#### Cyberwar escalates to Nuclear War

Gady 15 [Franz-Stefan Gady, Franz-Stefan Gady is a Research Fellow at the International Institute for Strategic Studies (IISS) focused on future conflict and the future of war, May 4, 2015, “Could Cyber Attacks Lead to Nuclear War?”, *The Diplomat*, https://thediplomat.com/2015/05/could-cyber-attacks-lead-to-nuclear-war/]-Hayer

“One-half of their [U.S. and Russian] strategic arsenals are continuously maintained on high alert. Hundreds of missiles carrying nearly 1,800 warheads are ready to fly at a moment’s notice,” a policy report compiled by a study group chaired by the retired U.S. general summarized. “At the brink of conflict, nuclear command and warning networks around the world may be besieged by electronic intruders whose onslaught degrades the coherence and rationality of nuclear decision-making,” the report further points out. Get briefed on the story of the week, and developing stories to watch across the Asia-Pacific. The War Games-like scenario could unfold in one of the following three ways: First, sophisticated attackers from cyberspace could spoof U.S. or Russian early warning networks into reporting that nuclear missiles have been launched, which would demand immediate retaliatory strikes according to both nations’ nuclear warfare doctrines. Second, online hackers could manipulate communication systems into issuing unauthorized launch orders to missile crews. Third and last, attackers could directly hack into missile command and control systems launching the weapon or dismantling it on site ( a highly unlikely scenario).

### 2AC --- Impact Extension --- Democratic Backsliding

#### Democratic backsliding undermines law

Wolkenstein 20[Fabio Wolkenstein is an Assistant Professor of "Transformations of Democracy" at the University of Vienna. I work on democratic theory, political parties, representation, ideologies, and the political theory of the EU. Previously I was Associate Professor of politics at Aarhus University and affiliated researcher in political theory, “Transnational Complicity in Democratic Backsliding”, Global Justice: Theory Practice Rhetoric, 12-2-20, https://www.theglobaljusticenetwork.org/index.php/gjn/article/view/206] SL

This leads to another question that must be clarified before moving on: why is democratic backsliding a form of wrongdoing? I have so far just postulated that democratic backsliding is a ‘wrong,’ and relied on readers’ intuitive agreement with this conjecture. But why exactly is it a wrong? The most straightforward answer, I suggest, is that Hungary and Poland violate their duty to obey EU law when they undermine democracy and the rule of law. That duty arises because both states have democratically ratified the EU treaties, thereby having accepted the treaties as (1) a framework for dealing with a specified range of issues and a source of normative demands on national institutional configurations.8 Of course, this is not the only answer that could be given to this question. It is probably possible to mount a more general case against democratic backsliding that shows that governments who undermine democracy and the rule of law engage in wrongdoing irrespective of which treaties they may have signed. This could be achieved by invoking a moral requirement that states ought to secure citizens’ public and private autonomy through well-functioning democratic and legal institutions.9 But though I am sympathetic to this line of reasoning, I simply lack the space to develop such an argument here. The more ‘legalistic’ (and possibly less controversial) argument from treaty-based obligations suffices for our purposes.

#### Democratic Sliding means authoritarianism

Hudson 21 [Alexander Hudson, a Democracy Assessment Specialist in the Democracy Assessment Unit of International IDEA’s Global Programmes in Stockholm. As part of the team that produces the Global State of Democracy Indices and Global State of Democracy Report, Hudson contributes to our data collection, analysis and visualization work, December 16, 2022, “Democratic backsliding, Different causes, divergent trajectories”, *INTERNATIONAL IDEA*, https://www.idea.int/blog/democratic-backsliding-different-causes-divergent-trajectories]-Hayer

By democratic backsliding, political analysts generally mean that a democracy is slipping backwards in terms of its democratic performance, and that there are signs of rising authoritarianism. One succinct definition holds that democratic backsliding involves “state-led debilitation or elimination of any of the political institutions that sustain an existing democracy.” Democratic backsliding differs from more generalized democratic erosion in terms of both intent and focus. International IDEA’s research in this area has highlighted the linkage between democratic backsliding and actions that specifically damage both horizontal constraints (via attacks on the legislature and the courts) and accountability to the voting public (via interference with media integrity and civil liberties). In most cases of democratic backsliding, the ability to hold free and fair elections is not immediately impacted – though this may come later. Applying the implications of this research in a diagnostic way, International IDEA tracks the average value of its indicators for Checks on Government and Civil Liberties for every country, and where we see a decline compared to five years ago that is greater than the threshold we’ve defined, we classify that country as backsliding. That also means that each country is compared to itself, not to some abstract and universal standard.

### 2AC --- Impact Extension --- Populism

#### Populists use nuclear weapons irresponsibly

Meier and Vieluf 21 [Oliver Meier is a senior Researcher at the Institute for Peace Research and Security Policy. Prior to this, he was Deputy Head in the International Security Division of the German Institute for International and Security Affairs. Maren Vieluf is a researcher at Institute for Peace Research and Security Policy. December 16, 2021, "Upsetting the nuclear order: how the rise of nationalist populism increases nuclear dangers", The Nonproliferation Review, https://doi.org/10.1080/10736700.2020.1864932] SL

Nationalist populists, by contrast, often speak loosely about nuclear weapons, which complicates a “reading” of their statements.52 This concerns both style and substance, which coincide with their personalistic style of leadership53 and their desire to flout the rules of what they deride as “political correctness.”54 Donald Trump has again led the way—for example, through his excessive tweeting on nuclear-weapon issues.55 Other nationalist populists have also deviated from previous rhetorical styles by bragging about their nuclear weapons. In April 2019, shortly after an escalation of the Pulwama crisis between India and Pakistan had been averted, Indian Prime Minister Narendra Modi suggested that his country was ready to use nuclear weapons against Pakistan: “Every other day they used to say ‘we have nuclear button, we have nuclear button’. What do we have then? Have we kept it for Diwali?”56 President Recep Tayyip Erdogan’s October 2019 statement that it is unacceptable for Turkey not to have nuclear weapons because “[t]here is no developed nation in the world that doesn’t have them”57 is another typically populist statement, conflating strong views with half-truths or lies. Such loose talk may have several purposes. By emphasizing nuclear weapons, nationalist populists can set themselves apart from the established elite discourse. Donald Trump boasted of having gained knowledge of nuclear weapons not through a formal education but through his uncle, a professor of engineering at the Massachusetts Institute of Technology.58 Thus, the US president believed that he did not need to rely on the expertise and experience of the nuclear elite. This ignorance of nuclear lessons by virtue of not “being socialized to the dangers of nuclear weapons”59 derived from the past is a trademark of nationalist populists, but is also part and parcel of a general loss of expertise in executives and parliaments in nuclear-weapon states and nuclear-allied countries.60 Nationalist populists also like to make strong statements on nuclear issues because they may believe that this impresses their main target audience—that is, their domestic power base. Thus, Putin has several times used his regular direct encounters with the Russian public to highlight the importance of nuclear weapons for Moscow’s standing in the world. In March 2018, Putin, in his speech to the Federal Assembly of Parliamentarians, policy makers, religious leaders, public figures, and members of the media, boasted about Russia’s nuclear capabilities and in true populist fashion even invited “[t]hose interested in military equipment … to suggest a name for this new weaponry, this cutting-edge” nuclear-weapon system.

#### Populism accelerates climate change

Leigh 21 [Andrew Leigh, Member of Australian Parliament, November 5, 2021, “How Populism Imperils the Planet”, *THE MIT PRESS READER*, ttps://thereader.mitpress.mit.edu/how-populism-imperils-the-planet/]-Hayer

Yet focusing on catastrophic risk — in climate change and other areas — is hampered by the growth of populist politics. Not every populist is a climate denier, but virtually all climate deniers are populists. One analysis of the 21 largest right-wing populist parties in Europe found that one-third were outright climate deniers, while many others were hostile to climate action. Right-wing populists make up 15 percent of the European Parliament, but their votes account for around half of all those voting against climate and energy resolutions. A recent study in the United Kingdom identified voters who held populist beliefs about politics. These populist voters were significantly less likely to agree that global warming is caused by human action and less likely to support measures to protect the environment. Populism is on the rise. From 1990 to 2018, the number of countries with populist leaders increased from four to 20. The best known was President Donald Trump, who once claimed that climate change is a “hoax,” and asserted that “global warming was created by and for the Chinese in order to make U.S. manufacturing non-competitive.” In the current Congress, 52 percent of House Republicans and 60 percent of Senate Republicans are climate deniers. In Brazil, President Jair Bolsonaro has loosened controls over land clearing in the Amazon. This has led farmers to accelerate deforestation by logging and burning. In mid-2019, satellite analysis of major fires in the Amazon showed that an area the size of Yellowstone National Park had been burned. At this pace, this additional deforestation could push the Amazon rainforest toward a tipping point.

#### European populism will increase nuclear risk.

**Gevarter ’18** [David, an intern for European studies at the Council on Foreign Relations, “Could European Populism Go Nuclear on NATO?”, The Council for Foreign Affairs, 19 July 2018, <https://www.cfr.org/blog/could-european-populism-go-nuclear-nato> ] -ALP

As part of NATO’s shared nuclear deterrent, the United States currently deploys the B61 gravity bomb in five NATO countries: Belgium, Germany, Italy, the Netherlands, and Turkey. While nuclear weapons are not popular among the European public, technocrats in European governments have recognized that the NATO nuclear deterrent is an unpleasant but strategic imperative. However, the rise of populist and nationalist movements across Europe could damage this consensus and threaten the integrity of NATO’s nuclear mission. The Trump administration believes that the United States must deploy more tactical (non-strategic) weapons in Europe through NATO to signal to Russia that any use of tactical weapons would be met by an equivalent response. The 2018 U.S. Nuclear Posture Review claims that **Russia is more likely to use tactical nuclear weapons in a first strike to gain advantage because it believes the United States would not escalate with a strategic nuclear strike**. As such, the Trump administration has placed great importance on expanding the United States’ arsenal of tactical nuclear weapons—such as the B61—as a way of countering the perceived Russian advantage in this field. Yet, this strategy could encounter serious obstacles as populist governments gain a foothold on the continent, exacerbated by growing anti-American sentiment. As the wave of populist governments gains popularity in Europe, instead of upholding long-standing NATO commitments, these governments might cave to the will of the masses. They could order the withdrawal of NATO—namely, U.S.—nuclear weapons from their territory, disregarding strategic necessity. The surge of populism in Germany, the backbone of the European project, can do the most damage to the shared nuclear deterrent. The current German government has thus far maintained the nuclear status quo despite opposition, but Angela Merkel’s hold on power is not what it used to be. Recent figures show that 71 percent of Germans favor banning nuclear weapons, and a change in Germany’s executive government could put NATO interests at risk. In the 2017 federal election, **Merkel’s political alliance lost a significant percentage of its seats in the Bundestag, most notably to the populist, right-wing party Alternative for Deutschland (AfD).** In its platform, AfD explicitly calls for the withdrawal of all NATO troops and nuclear weapons from German territory. With the near collapse of the current German government over immigration, the possibility of a rise to power by AfD or a party with similar views is no longer far-fetched. Like in Germany, the specter of populism has become very real in Italy, with the anti-establishment coalition formed by the League and 5-Star parties taking power. This could spell trouble for the NATO shared deterrent, given the broad unpopularity of nuclear weapons in the country. According to a 2007 survey, 70 percent of Italian respondents indicated that the use of NATO nuclear weapons would never be justified, even in the context of war. Over half of respondents indicated that they believed NATO nuclear-sharing agreements violate the Nuclear Nonproliferation Treaty and that Italy should not be party to such agreements. Maintaining and expanding the U.S. nuclear arsenal in Italy will require significant cooperation from the Italian government, but Prime Minister Giuseppe Conte's government has shown little intention to acquiesce to President Trump's demands for NATO, such as increasing defense spending. It appears that the new, pro-Russia government in Italy is willing to do whatever it takes to appeal to public opinion, irrespective of the ramifications. Russia has always wanted the withdrawal of U.S. nuclear weapons from Europe and such a move could be part of **an Italian strategy of warming relations with the Kremlin**. The 2016 attempted military coup showed that Turkey is the most unstable NATO country, where the future of nuclear sharing is, at best, unsure. Since the attempted coup, President Recep Tayyip Erdogan’s populist government has further undermined Turkey’s relationship with the United States, NATO, and other Western countries as the country secures diplomatic and military rapprochement with Moscow. Erdogan has leveraged populist rhetoric to consolidate power, galvanizing support for his agenda and eroding checks and balances on his rule. Erdogan himself is no fan of nuclear weapons, and it is easy to imagine a scenario in which, as part of a pivot toward Moscow, Erdogan orders NATO nuclear weapons out of Turkey. Even if that is not the case, many experts argue that the United States should withdraw its nuclear weapons from Turkey, given the deteriorating political climate in the country. This, given the country’s proximity to Russia and other areas of interest in the Middle East, could jeopardize NATO’s ability to hold enemy targets at risk with its nuclear arsenal. The uncertainty throughout NATO countries prompts questions regarding the future of the shared nuclear deterrent. If U.S. tactical nuclear weapons are withdrawn from Turkey or elsewhere in Europe, where else could they go? Some have suggested Poland, given the country’s desire for an increased NATO presence, but this unprecedented expansion of the nuclear deterrent to Eastern Europe could—and likely would—spark a dramatic showdown with Russia, turning the Polish border with Kaliningrad into a hot zone. The worsening wave of populism in Europe could give impetus to European popular opposition to nuclear weapons, forcing their withdrawal from the continent. **If the Pentagon truly wants to adhere to its designs to expand its arsenal of tactical nuclear weapons deployed in Europe as part of the NATO shared nuclear deterrent, it needs to start coming up with contingency plans**. At the very least, President Trump should stop antagonizing NATO allies and try to preserve what little good will remains toward the U.S. agenda.

### 2AC --- Impact Extension --- Cohesion

#### NATO cohesion allows for stability and advancement

Burns and Lute 19 [Ambassador Nicholas Burns is the Roy and Barbara Goodman Family Professor of the Practice of Diplomacy and International Relations at the Harvard Kennedy School. Ambassador Douglas Lute is the former United States Permanent Representative to the North Atlantic Council, NATO’s standing political body. “NATO at Seventy: An Alliance in Crisis”, Belfer Center for Science and International Affairs, 10-19-18, https://www.belfercenter.org/publication/nato-seventy-alliance-crisis] SL

NATO maintains a partnership with forty-one countries outside the Alliance from Mauritania in West Africa to Japan.16 Many states have been invaluable members of coalitions in Afghanistan, Iraq, the Balkans and in the fight against the Islamic State. Most important, NATO should strengthen its partnership with the European Union. Partnerships with the Gulf Coordination Council, the African Union and the Arab League could promote stability along NATO’s periphery. NATO faces yet another critical challenge in adapting quickly to a rapidly changing, global, military technology landscape. Its often-byzantine defense planning processes date to the Cold War, long before the extraordinary, current advances in military arms powered by artificial intelligence, cyber, robotics, quantum computing and biotechnology—perhaps the most decisive change in military technology since the start of the nuclear age. NATO allies, led by the United States, must now commit a far greater share of their military budgets to acquiring these new military technologies, lest China and Russia gain a decisive advantage in the decade ahead.

#### NATO cohesion is beneficial

Bazin and Kunertova 18 [Aaron Bazin and Dominika Kunertova, Lt. Col. Aaron Bazin, PsyD, is a transitioning U.S. Army officer, Functional Area 59 (strategist). He holds a doctorate in psychology, specializing in mediation and conflict resolution. He has over twenty years of experience including service with NATO and the U.S. Army Central Command, and operation deployments to Pakistan, Afghanistan, Iraq, Qatar, the United Arab Emirates, Bahrain, Kuwait, and Jordan. He previously published “Winning Trust under Fire” in the January-February 2015 issue of Military Review, Dominika Kunertova is a PhD candidate in the Department of Political Science at the Université de Montréal, Quebec, Canada. She holds a BA in political science from Comenius University, Bratislava, Slovakia, and an MA in international relations from Charles University, Prague, Czech Republic. Her research focuses on transatlantic security and defense cooperation, and she has published in the Journal of Transatlantic Studies and European Security, February 2018, “An Alliance Divided?”, *Military Review*, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/January-February-2018/An-Alliance-Divided-Five-Factors-That-Could-Fracture-NATO/]-Hayer

The next key term, alliance cohesion, reflects the degree to which the members are able to agree on goals, strategies, and tactics, and coordinate activity for attaining those goals.7 In addition to this behavioral component, cohesion represents the particular quality that makes its members operate as a whole during times of crisis. Literature from the psychology field defines cohesion as “bonds, either social or task based, that contribute to the synergistic functioning as a whole.”8 Other accounts claim “alliance cohesion is based upon the distance between individual member interests and the collective alliance interest.”9 In defining this term, it is key to note that cohesion is a very fluid idea, contextually based and highly subjective. Therefore, this research proceeded under the assumption that cohesion is largely qualitative in nature. Some assert that the best moment to understand cohesion is in time of crisis, such as when the Alliance faces a significant conflict. In case of wartime alliances, cohesion refers to the states’ ability to coordinate military strategy, agree on war aims, and avoid making a separate peace, together with “the degree of convergence among member states’ commitments to the alliance.”10 This is important, since conventional wisdom asserts the source of cohesion is usually the element (be it political, economic, military, or nonmaterial) that is targeted by adversary activities and likely results in the defeat of the attacked party. It then follows that by adhering to these definitions, one could consider Alliance cohesion to be at the level of a center of gravity, since it “exerts a certain centripetal force that tends to hold an entire … structure together.”

### 2AC --- AT: No Russia War --- Conflict Prone

#### Russia is likely to be in conflict - oil

Weeks and Colgan 2-27-22 [Jessica L.P. Weeks and Jeff D. Colgan, Jessica L.P. Weeks is professor of political science and H. Douglas Weaver chair in diplomacy and international relations at the University of Wisconsin at Madison and Jeff D. Colgan is the Richard Holbrooke associate professor of political science at Brown University, February 27, 2022, “There’s a reason Putin can be so aggressive: Oil”, *The Washington Post*, https://www.washingtonpost.com/politics/2022/02/27/theres-reason-putin-can-be-so-aggressive-oil/]-Hayer

Russia’s oil wealth intensifies the problem of personalist rule and aggressive foreign policy. One of us coined the term “petro-aggression,” indicating the link between oil and war. It turns out that major oil-exporting countries like Russia, known as petrostates, are about 50 percent more conflict prone than non-petrostates, on average, and oil has played a role in 25 to 50 percent of recent wars. Other petrostates with aggressive pasts include Iraq, Libya and Iran. Not every petrostate is conflict-prone, of course. Much depends on the leader’s preferences. When a leader is not interested in revising the status quo, there is nothing about oil that inherently leads to conflict. In the hands of an aggressive or revisionist leader like Putin, however, oil can further reduce domestic political constraints. Oil money allows an autocrat to buy off domestic opposition, build a military machine and create a war chest to ward off sanctions. In that sense, Putin is following in the footsteps of other petrostate dictators like Hussein and Moammar Gaddafi. Oil and energy also helped set the 2014 political context for Putin’s invasion of Crimea.

### 2AC --- Impact Extension --- Econ

#### US Economic Collapse has severe effects – utilities, unemployment, GDP

Amadeo 22 [Kimberley Amadeo, an expert on U.S. and world economies and investing, with over 20 years of experience in economic analysis and business strategy. She is the President of the economic website World Money Watch. As a writer for The Balance, Kimberly provides insight on the state of the present-day economy, as well as past events that have had a lasting impact, March 4, 2022, “US Economic Collapse: What Would Happen?”, *the balance*, https://www.thebalance.com/u-s-economy-collapse-what-will-happen-how-to-prepare-3305690]-Hayer

If the U.S. economy were to collapse, you would likely lose access to credit. Banks would close. Demand would outstrip supply of food, gas, and other necessities. If the collapse affected local governments and utilities, then water and electricity might no longer be available. A U.S. economic collapse would create global panic. Demand for the dollar and U.S. Treasurys would plummet. Interest rates would skyrocket. Investors would rush to other currencies, such as the yuan, euro, or even gold. It would create not just inflation, but hyperinflation, as the dollar would lose value to other currencies. If you want to understand what life would look like during an economic collapse, think back to the Great Depression. The stock market crashed on Black Thursday.3 By the following Tuesday, it was down 25%. Many investors lost their life savings that weekend. By 1932, one out of four Americans was unemployed.4 Wages for those who still had jobs fell precipitously—manufacturing wages dropped 32% from 1929 to 1932.5 U.S. gross domestic product was cut nearly in half. Thousands of farmers and other unemployed workers moved to California and elsewhere in search of work. Two-and-a-half million people left the Midwestern Dust Bowl states.6 The Dow Jones Industrial Average didn't rebound to its pre-Crash level until 1954.7

## Russia General – AFF

### 2AC --- Russia = Offensive

#### Russia is an offensive realist that acts irrationally through force

Dayspring 15 [Chief Warrant Officer 4 Stephen Dayspring is a Special Forces Warrant Officer with 17 years of operational experience in 10th Special Forces Group (Airborne). He is currently completing a Master of Science in Defense Analysis at the Naval Postgraduate School in Monterey, California, “TOWARD A THEORY OF HYBRID WARFARE: THE RUSSIAN CONDUCT OF WAR DURING PEACE”, Naval Postgraduate School, December 2015, https://www.hsdl.org/?view&did=790442] SL

There are two traditions regarding the relationship between conflict and politics: realism and liberalism. “For the realist, the central problem of international politics is war and the use of force, and the central actors are states.”52 The realist is pragmatic in that he expects that others will try to take what he is unable to defend so he must demonstrate strength to ensure his sovereignty. By maximizing one’s own power, one minimizes the ability of other states to threaten one’s security.53 At a certain point however, the realist becomes strong enough that he begins considering what he might be able to take from a weaker neighbor. The “offensive realist” does not even think there is a choice; the only way he can better his odds of survival is to have more relative power than his potential enemies, a gulf he can widen by physically reducing his adversary’s strength.54 Realists see the contemporary international system as anarchic—there is no central or governing power- so the only things that enforce order are the individual states’ ability and willingness to fight to maintain the status quo. Neo-liberalism envisions “a global society that functions alongside the states and sets part of the context for the states.”56 Liberalism promotes the view not just of international governing bodies and legal restraint, but also that interdependent trade, monetary systems, and cross border communication have evolved into a transnational society where conflict is less likely. This is the essence of globalization, and is the preferred view of the world generally held in the West. Realists counter that there will always be a potential for a future state of war and one had better be ready to protect against it. Offensive realism is not a popular concept in the liberal-minded West because it tends to be at odds with our traditionally optimistic values.57 It is the difference in world view of relation power that explains why a country like Russia would suddenly seize Crimea, or why China would rapidly expand into its neighbors’ territorial waters. If a state views the world through the realist lens, specifically from the position of offensive realism, that state’s actions often appear irrational to liberal outsiders as those actions undermine the best interests of the international community. They appear much more pragmatic when they are seen to increase the relative power, and therefore the chances of survival, of the aggressor state. While this realist perspective might be depressing, “it behooves us to see the world as it is, not as we would like it to be.”

# NEG

## Russia General – NEG

### 1NC --- Russia = Defensive

#### Russia is not being aggressive towards NATO

Fernandes and Finney 16 (Benjamin J Fernandes and Nathan K Finney, Benjamin J Fernandes is a George Mason University PhD student, Council on Foreign Relations Term Member, and U.S. Army officer. His studies focus on security assistance, governance, principal-agent theory, and grand strategy. Nathan K Finney is an officer in the U.S. Army and a PhD candidate in history at the University of Kansas. He is also the founder of the online journal [The Bridge](http://thestrategybridge.com/), founder and [Managing Director of the Military Fellowship](http://www.wm.edu/offices/itpir/pips/people/index.php) at the [Project on International Peace & Security](http://www.wm.edu/offices/itpir/pips/index.php), ‘The Myth of Russian Aggression and NATO Expansion’, Strategy Bridge,  [December 16, 2016](https://thestrategybridge.org/the-bridge/2016/12/16/the-myth-of-russian-aggression-and-nato-expansion), https://thestrategybridge.org/the-bridge/2016/12/16/the-myth-of-russian-aggression-and-nato-expansion)

With the fall of the Soviet Union in the 1990s, many foreign policy experts such as [Kenneth Waltz](http://www.columbia.edu/itc/sipa/U6800/readings-sm/Waltz_Structural%20Realism.pdf), [Michael MccGwire](http://journals.cambridge.org/action/displayFulltext?type=1&pdftype=1&fid=33532&jid=RIS&volumeId=24&issueId=01&aid=33531), [Michael Brown](http://www.tandfonline.com.mutex.gmu.edu/doi/abs/10.1080/00396339508442775?journalCode=tsur20), and others warned against expanding the North Atlantic Treaty Organization (NATO) to former Soviet-aligned countries, arguing expansion would [unnecessarily provoke](http://journals.cambridge.org/action/displayFulltext?type=1&pdftype=1&fid=33532&jid=RIS&volumeId=24&issueId=01&aid=33531) the Russians to take steps inimical to America’s interests. The events of the post-Cold War era simply do not support this assertion. Rather, the historical evidence suggests Russian leaders act aggressively when the cost-benefit-risk of aggression weighs heavily in Russia’s favor—a threshold past NATO expansions have never crossed.

In the intervening 20 years, **Russia has protested NATO expansion but never acted aggressively in response to expansion**. Russia did respond militarily to events that threatened their interests, such as the revolution in Ukraine and improving Ukraine-European Union economic ties. In those cases, the benefits of military action dwarfed the costs from the perspective of Russian leaders. Recent Russian actions indicate U.S. and NATO will likely continue clashing with Russia, regardless of changes to U.S. administrations, due to the dramatically different values and assumptions held by Russian and NATO leaders. NATO’s defense reductions combined with perceptions the West has few [red lines](https://www.washingtonpost.com/news/post-politics/wp/2016/10/04/the-problem-with-obamas-account-of-the-syrian-red-line-incident/) have helped foster an environment where Russia likely believes the costs of aggression are low**. To counter this perception, the United States and NATO should continue and expand policies, like the** [European Reassurance Initiative](http://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2016/FY2016_ERI_J-Book.pdf)**, likely to increase the risks and costs associated with aggression from a Russian perspective.**

Russian aggression has resulted from a combination of many different factors that created a situation where the benefits of aggression significantly outweighed their costs. **While Russians certainly like using NATO expansion to justify aggression, this article describes facts suggesting Russia’s motives have little to do with fears over NATO expansion or military forces.** We will first explain U.S. and NATO efforts to strengthen and cooperate with Russia based on the assumption Russia could be a partner. This Western perception contributed to dramatic reductions in NATO’s combat power in Europe and prioritization of non-military spending.

#### The US and NATO are at fault for provoking Russia

**Carpenter 22** [Ted Galen Carpenter is senior fellow for defense and foreign policy studies at the Cato Institute. Carpenter served as Cato’s director of foreign policy studies from 1986 to 1995 and as vice president for defense and foreign policy studies from 1995 to 2011. “The U.S. and NATO Helped Trigger the Ukraine War. It’s Not ‘Siding With Putin’ to Admit It”, Cato Institute, 3-7-22, <https://www.cato.org/commentary/us-nato-helped-trigger-ukraine-war-its-not-siding-putin-admit-it>] SL

Moscow’s cruel overreaction deserves emphatic condemnation. However, the culpability of the United States and its NATO allies also is sizable. Moving an alliance that one great power dominates to the border of another major power is inherently destabilizing and provocative. Those people who are familiar with even the basics of international relations should grasp that point; it was inexcusable that so many U.S. and NATO leaders apparently did not do so. One can readily imagine how Americans would react if Russia, China, India, or another peer competitor admitted countries from Central America and the Caribbean to a security alliance that it led—and then sought to add Canada as an official or de facto military ally. It is highly probable that the United States would have responded by going to war years ago. Yet even though Ukraine has an importance to Russia comparable to Canada’s importance to the United States, our leaders expected Moscow to respond passively to the growing encroachment. They have been proven **disastrously wrong**, and thanks to their ineptitude, the world is now a far more dangerous place.

#### Russia is seemed as aggressive but is actually playing defense

ZollMann 21 [Florian ZollMann is an academic and author of media, Propaganda and the Politics of Interventions (Peter Lang, New York). “Russia is reacting to NATO’s policy of expansions”. Indybay, Monday Dec 27th 2021. <https://www.indybay.org/newsitems/2021/12/27/18846961.php#:~:text=%22Russia%20is%20being%20built%20as%20an%20enemy%20for,Florian%20Zollmann%20says%20in%20an%20interview%20with%20NachDenkSeiten>.] - NAAh

Russia is accused of calculating power and bellicose behavior. As far as the situation in Ukraine is concerned, however, the political facts speak a different language. Russia is being built as an enemy for peace. With its Ukraine policy, Russia is actually reacting to NATO's expansionist policy. Is Russia an aggressor in the Ukraine conflict? "The political facts speak a different language" Interview with journalism researcher Florian Zollmann [This interview published on 12/23/2021 is translated from the German on the Internet, <https://www.nachdenkseiten.de/?p=79327>.] "Russia is being built as an enemy for peace. With its Ukraine policy, Russia is actually reacting to NATO's policy of expansion." This is what journalism researcher Florian Zollmann says in an interview with NachDenkSeiten. Zollmann, who deals a lot with political propaganda in the media, says the media are "turning reality upside down" when it comes to classifying the tensions between Russia and Ukraine. "The Russian side, which perceives a progressive eastward expansion of NATO in disregard of agreements reached at the highest political level, is marginalized in the media," said Zollmann, who teaches at Newcastle University in England. By Marcus Klöckner. Mr Zollmann, the media is currently focusing again on Russia in connection with Ukraine. Recently, it was reported that Russia had gathered 175,000 troops on the border with Ukraine. What is happening right now. Representatives of leading NATO states are outraged because Russia has allegedly moved troops to the border with Ukraine. A look at the facts, however, shows that Russia is acting as any other state in a similar geopolitical situation would act. For a long time now, there has been no question in the "reporting" of major media: Russia is the aggressor! What does your analysis look like? Exactly. The media coverage gives the impression that Russia is an imperial power and that the West must protect itself and its allies from it. What does this view have to do with reality? Nothing. Reality is turned upside down. Because the historical context is hardly adequately illuminated in the media. The Russian side, which perceives a progressive eastward expansion of NATO in disregard of agreements reached at the highest political level, is marginalized in the media. Imagine the following hypothetical facts: Russia would have included Latin American states such as Guatemala, Nicaragua, Costa Rica, Panama and Honduras in its international military alliance Organization of the Collective Security Treaty (CSTO) and claimed to install nuclear weapons in these countries. Imagine, furthermore, that the CSTO launched military cooperation with Mexico and tried to include the country bordering the south of the USA in the CSTO. In this case, wouldn't it be expected that the US would move troops to the border of Mexico? And exactly this scenario is currently taking place, but on the border with Russia.

## AT: Uniqueness

### 1NC --- No NATO Credibility

#### NATO is not credible – Ukraine and Georgia

Hunter 22 [Robert E. Hunter, Robert E. Hunter served as U.S. ambassador to NATO (1993-98) and on the National Security Council staff throughout the Carter administration, first as Director of West European Affairs and then as Director of Middle East Affairs. In that role, he was the White House representative at the Autonomy Talks for the West Bank and Gaza and developer of the Carter Doctrine for the Persian Gulf. He was Senior Advisor to the RAND Corporation from 1998 to 2011, and Director of the Center for Transatlantic Security Studies at the National Defense University, 2011-2012. He served on the Pentagon’s Defense Policy Board and is a member of the American Academy of Diplomacy, March 24, 2022, “NATO has a serious credibility problem”, *RESPONSIBLE STATE CRAFT*, https://responsiblestatecraft.org/2022/03/24/natos-credibility-problem/]-Hayer

Damage to US and NATO credibility over the matter of Ukraine can trace its history at least as far back as the 2008 Bucharest summit, when President G.W. Bush proposed that Ukraine (and Georgia) be enrolled in Membership Action Plans (MAPs), the next-to-last step before becoming allies. This was a decisive move beyond the 1997 NATO-Ukraine Charter and consultative Council, which provided no security guarantees. Most allies resisted, including because they were not prepared to take the risk of pushing NATO right up to Russia and straddling the traditional invasion route into the heart of Europe – in both directions and with long memories. How would Russia respond to such a step? But the European allies also recognised that, although moving Ukraine and Georgia toward NATO membership had to be ruled out, the US president could not be sent home empty-handed. So the summit declared that both countries “will become members” of the alliance. Those words were designed to put off consideration of NATO membership for Ukraine and Georgia to the indefinite future (“never,” in the eyes of many European allies.) But in their haste, NATO’s leaders obviously did not understand the full import of that statement. It signaled that the two countries were geopolitically so important to the West that they would definitely be brought into the alliance, whatever Russia thought: in plain English, it was thus the actual moment of commitment. Soon thereafter, Georgia’s president, Mikheil Saakashvili, tested the proposition by using military force to try reclaiming occupied parts of South Ossetia, only to be defeated by Russian forces. Not a single NATO ally sent troops to defend Georgia. Finis, for any practical purposes, to “will become members” of NATO. Yet instead of putting the commitment into George Orwell’s Memory Hole, NATO has repeated the formulation at every summit and ministerial meeting, and, until just before Putin’s 2022 invasion, top leaders of the Biden administration were still harping on NATO’s “open door” to Ukraine’s membership, even though it is a fantasy. This last observation is based on two interrelated facts. First, NATO takes all decisions by consensus – a unit veto; and second, many allies have already made clear that would never be willing, in response to aggression against Ukraine (on Russia’s border), to invoke Article 5 of the NATO Treaty: that “…an armed attack against one or more [ally]….shall be considered an attack against them all…” Thus Ukraine will never be admitted to NATO.

#### Non-unique, NATO is not credible – Ukraine proves

Taylor 22 [Will Taylor, Journalist for LBC, March 13, 2022, “'Incredibly weak': Nato is using 'Chamberlain tactics' on Putin, ex-Ukraine PM warns”, *LBC*, https://www.lbc.co.uk/news/nato-weak-ukraine/]-Hayer

Oleksiy Hornachuk, who served as prime minister of Ukraine, told LBC's Swarbrick on Sunday that Russian invaders want to "destroy everything they can, kill everyone they can". He blasted the Western response to the invasion of his country as "incredibly weak" and compared it to Neville Chamberlain, the British prime minister most associated with appeasement of Adolf Hitler. The West has imposed severe economic sanctions and supplied weapons and equipment to Ukraine's military, but Kyiv has called for a no-fly zone to be imposed by Nato. Mr Hornachuk said: "What I see now, I see absolutely incredibly weak response from the West and from Nato. Incredibly weak.

## AT: Impacts

### 1NC --- AT: Democratic Backsliding

#### Democratic Leaders are more aggressive

Vasco 18 [American Journal of Political Science, July 18, 2018, “Democracies More Prone to Start Wars – Except When They’re Not”, *Caltech*, https://www.caltech.edu/about/news/democracies-more-prone-start-wars-except-when-theyre-not-82879]-Hayer

The difference boils down to public pressure, say the study's authors, Michael Gibilisco of Caltech and Casey Crisman-Cox of Texas A&M University. Because of pressure from voters to not back down and appear weak, democratic leaders tend to act more aggressively in international conflicts. An autocrat, on the other hand, is answerable to no one and can back down from a conflict without facing personal consequences. "If an elected leader makes a threat during a conflict with another country and the threat isn't followed through, they may face a decrease in approval ratings, or they may lose an election," says Gibilisco, assistant professor of political science. In democracies, he notes, voters can punish their leaders for appearing weak—these punishments or consequences are known as "audience costs" in political science parlance. To avoid those costs, leaders in representative governments become more aggressive during disputes. In their study, Gibilisco and Crisman-Cox, who is also an assistant professor of political science, first developed a mathematical model of dispute initiation between countries and then fit the model to data of actual conflicts that occurred among 125 countries between 1993–2007.

#### Democratic governments are disadvantaged

Hegre 14 [Håvard Hegre is the Dag Hammarskjöld Professor of Peace and Conflict Research, Uppsala University and Researcher, Peace Research Institute Oslo, “Democratization and Political Violence”, Our World-United Nations University, 5-15-14, https://ourworld.unu.edu/en/democratization-and-political-violence] SL

Democracies are at a disadvantage relative to non-democracies in two respects when it comes to countering political violence and insurgencies. First, they are accountable to a large citizenship. If terrorist activity succeeds in increasing the risk of death, it can create a widespread feeling of insecurity. Because democratic governments are expected to safeguard the lives and property of all of their citizens, they must respond in some way to this increased risk. At the same time, democracies are legitimate only to the extent that they protect individual freedoms and handle perpetrators through the legal system. Terrorism, then, may also undermine government support if authorities respond to threats too forcefully. Provoking such over-reactions may even be an aim of some terrorist groups. This means that democratic political systems provide more opportunities for the use of political violence than authoritarian systems. Indeed, comparative research shows that democratic governments experience more transnational terrorism than other governments. Rebel groups fighting democracies in civil wars target civilians more often than those fighting non-democracies, often using terrorism to complement guerilla warfare and other military challenges to government troops. Armed conflicts also tend to last longer in democracies than in non-democracies, possibly because counter-insurgency efforts are less brutal and hence less effective in restricting opportunities for violent political opposition.

### 1NC --- AT: Populism

#### Populists already have low public approval

Taylor 22 [Chloe is a news assistant at CNBC. “Populist politics lost support globally during the pandemic, research finds”, CNBC, 1-17-22, https://www.cnbc.com/2022/01/18/populist-politics-lost-support-during-the-pandemic-research-finds.html] SL

Opposition populist parties also lost support during the pandemic, while “mainstream” opposition parties gained supporters. Approval of the way governments handled the Covid crisis also showed rising skepticism toward populist leaders’ competence. In June 2020, public approval of how countries with populist leaders had handled the pandemic was an average 11 percentage points lower than approval of countries with centrist governments. By the end of 2020, the gap had widened to 16 points. Statements associated with populism, such as a dislike for “corrupt elites” and a desire for the “will of the people” to be obeyed, also saw a decline in support, the report found. The number of people saying they agreed with similar statements fell by around 10 percentage points in Italy, the U.K. and France between 2019 and 2021.

### 2NC/1NR --- No Impact Extension --- Cyber MAD

#### Russia isn’t causing major cyberattacks because of cyber MAD.

Maundrill 22 [Beth Maundrill began her career in business-to-business publishing in 2013 and has previously written about technology in the maritime industry, supply chain, defense and aerospace sectors. “Why Russia has refrained from a major cyber-attack against the West”, Cyber Security Hub, 6-15-22, https://www.cshub.com/attacks/articles/why-russia-has-refrained-from-a-cyber-attack-against-the-west] SL

Firstly, Charles Denyer, a national security and cyber security expert, told CS Hub that Russia does indeed have the capability to weaponize their cyber capabilities and could hit the West in a way which would have a similar impact to that of the Colonia Pipeline attack of 2021. One reason such an attack has not been perpetrated however, Denyer supposes, is the idea of mutually assured destruction (MAD). Reflecting on the MAD principle that provides the cornerstone of global nuclear policy, a significant cyber-attack committed by Russia against the West could see an equal level of retaliation which Moscow and Putin can ill-afford as they become bogged down in the campaign against Ukraine. “Russia is definitely among the top four or five cyber entities, with the US being number one,” Denyer said. “But from my understanding based on the intelligence apparatus of the US, they are clearly aware that if they hit the US with any type of meaningful cyber-attack that would really damage our CI to the point that American society would stop functioning, [Russia] knows what is going to happen. US Cyber Command would hit them back with an offensive counterpunch that could do damage of the likes the world has not seen.”

### 1NC --- AT: Deterrence

#### 10 reasons why Nuclear Deterrence doesn’t work

Krieger 11 [David Krieger, Krieger is President Emeritus of the Nuclear Age Peace Foundation. He is the author and editor of many books on peace and nuclear weapons abolition, including "Speaking of Peace: Quotations to Inspire Action.", February 7, 2011, “TEN SERIOUS FLAWS IN NUCLEA DETERRENCE THEORY", *NUCLEAR AGE PEACE FOUNDATION*, https://www.wagingpeace.org/ten-serious-flaws-in-nuclear-deterrence-theory/]-Hayer

As volcanoes often give off strong warning signals that they may erupt, so we have witnessed such signals regarding nuclear arsenals and the failure of nuclear deterrence theory over the course of the Nuclear Age. Nuclear arsenals could erupt with volcano-like force, totally overwhelming the relatively flimsy veneer of “protection” provided by nuclear deterrence theory. In the face of such dangers, we must not be complacent. Nor should we continue to be soothed by the “experts” who assure us not to worry because the weapons will keep us safe. There is, in fact, much to worry about, much more than the nuclear policy makers and theorists in each of the nuclear weapon states have led us to believe. I will examine below what I believe are ten serious flaws in nuclear deterrence theory, flaws that lead to the conclusion that the theory is unstable, unreliable and invalid. 1. It is only a theory. It is not proven and cannot be proven. A theory may posit a causal relationship, for example, if one party does something, certain results will follow. In the case of nuclear deterrence theory, it is posited that if one party threatens to retaliate with nuclear weapons, the other side will not attack. That an attack has not occurred, however, does not prove that it was prevented by nuclear deterrence. That is, in logic, a false assumption of causality. In logic, one cannot prove a negative, that is, that doing something causes something else not to happen. That a nuclear attack has not happened may be a result of any number of other factors, or simply of exceptional good fortune. To attribute the absence of nuclear war to nuclear deterrence is to register a false positive, which imbues nuclear deterrence with a false sense of efficacy. 2. It requires a commitment to mass murder. Nuclear deterrence leads to policy debates about how many threatened deaths with nuclear weapons are enough to deter an adversary? Are one million deaths sufficient to deter adversary A? Is it a different number for adversary B? How many deaths are sufficient? One million? Ten million? One hundred million? More? There will always be a tendency to err on the side of more deaths, and thus the creation of more elaborate nuclear killing systems. Such calculations, in turn, drive arms races, requiring huge allocations of resources to weapons systems that must never be used. Leaders must convince their own populations that the threat of mass murder and the expenditure of resources to support this threat make them secure and is preferable to other allocations of scientific and financial resources. The result is not only a misallocation of resources, but also a diversion of effort away from cooperative solutions to global problems. 3. It requires effective communications. In effect, nuclear deterrence is a communications theory. Side A must communicate its capability and willingness to use its nuclear arsenal in retaliation for an attack by adversary B, thereby preventing adversary B from attacking. The threat to retaliate and commit mass murder must be believable to a potential attacker. Communications take place verbally in speeches by leaders and parliamentary statements, as well as news reports and even by rumors. Communications also take place non-verbally in the form of alliance formations and nuclear weapons and missile tests. In relation to nuclear deterrence, virtually everything that each side does is a deliberate or inadvertent form of communication to a potential adversary. There is much room for error and misunderstanding. 4. It requires rational decision makers. Nuclear deterrence will not be effective against a decision maker who is irrational. For example, side A may threaten nuclear retaliation for an attack by adversary B, but the leader of side B may irrationally conclude that the leader of side A will not do what he says. Or, the leader of side B may irrationally attack side A because he does not care if one million or ten million of his countrymen die as a result of side A’s nuclear retaliation. I believe two very important questions to consider are these: Do all leaders of all states behave rationally at all times, particularly under conditions of extreme stress when tensions are very high? Can we be assured that all leaders of all states will behave rationally at all times in the future? Most people believe the answer to these questions is an unqualified No. 5. It instills a false sense of confidence. Nuclear deterrence is frequently confused with nuclear “defense,” leading to the conclusion that nuclear weapons provide some form of physical protection against attack. This conclusion is simply wrong. The weapons and the threat of their use provide no physical protection. The only protection provided is psychological and once the weapons start flying it will become clear that psychological protection is not physical protection. One can believe the weapons make him safer, but this is not the same as actually being safer. Because nuclear deterrence theory provides a false sense of confidence, it could lead a possessor of the weapons to take risks that would be avoided without nuclear threats in place. Such risks could be counterproductive and actually lead to nuclear war. 6. It does not work against an accidental use. Nuclear deterrence is useful, if at all, only against the possibility of an intentional, premeditated nuclear attack. Its purpose is to make the leader who contemplates the intentional use of a nuclear weapon decide against doing so. But nuclear deterrence cannot prevent an accidental use of a nuclear weapon, such as an accidental launch. This point was made in the movie Dr. Strangelove, in which a US nuclear attack was accidentally set in motion against the Soviet Union. In the movie, bomber crews passed their “failsafe” point in a training exercise and couldn’t be recalled. The president of the United States had to get on the phone with his Soviet counterpart and try to explain that the attack on Moscow that had been set in motion was just an accident. The Americans were helpless to stop the accident from occurring, and so were the Soviets. Accidents happen! There is no such thing as a “foolproof” system, and when nuclear weapons are involved it is extremely dangerous to think there is. 7. It doesn’t work against terrorist organizations. Nuclear deterrence is based upon the threat of retaliation. Since it is not possible to retaliate against a foe that you cannot locate, the threat of retaliation is not credible under these circumstances. Further, terrorists are often suicidal (e.g., “suicide bombers”), and are willing to die to inflict death and suffering on an adversary. For these reasons, nuclear deterrence will be ineffective in preventing nuclear terrorism. The only way to prevent nuclear terrorism is to prevent the weapons themselves from falling into the hands of terrorist organizations. This will become increasingly difficult if nuclear weapons and the nuclear materials to build them proliferate to more and more countries. 8. It encourages nuclear proliferation. To the extent that the theory of nuclear deterrence is accepted as valid and its flaws overlooked or ignored, it will make nuclear weapons seem to be valuable instruments for the protection of a country. Thus, the uncritical acceptance of nuclear deterrence theory provides an incentive for nuclear proliferation. If it is believed that nuclear weapons can keep a country safe, there will be commensurate pressure to develop such weapons. 9. It is not believable. In the final analysis, it is likely that even the policy makers who promote nuclear deterrence do not truly believe in it. If policy makers did truly believe that nuclear deterrence works as they claim, they would not need to develop missile defenses. The United States alone has spent over $100 billion on developing missile defenses over the past three decades, and is continuing to spend some $10 billion annually on missile defense systems. Such attempts at physical protection against nuclear attacks are unlikely to ever be fully successful, but they demonstrate the underlying understanding of policy makers that nuclear deterrence alone is insufficient to provide protection to a country. If policy makers understand that nuclear deterrence is far from foolproof, then who is being fooled by nuclear deterrence theory? In all likelihood, the only people being fooled by the promised effectiveness of nuclear deterrence theory are the ordinary people who place their faith in their leaders, the same people who are the targets of nuclear weapons and will suffer the consequences should nuclear deterrence fail. Their political and military leaders have made them the “fools” in what is far from a “foolproof” system. 10. Its failure would be catastrophic. Nuclear deterrence theory requires the development and deployment of nuclear weapons for the threat of retaliation. These weapons can, of course, be used for initiating attacks as well as for seeking to prevent attacks by means of threatened retaliation. Should deterrence theory fail, such failure could result in consequences beyond our greatest fears. For example, scientists have found in simulations of the use of 100 Hiroshima-size nuclear weapons in an exchange between India and Pakistan, the deaths could reach one billion individuals due to blast, fire, radiation, climate change, crop failures and resulting starvation. A larger nuclear war between the US and Russia could destroy civilization as we know it.

### 1NC --- AT: Nuclear Extinction

#### Nuclear war doesn’t mean extinction

Ladish 20 [Jeffrey Ladish, an Information Security and Biosecurity Consultant at Gordian Research, November 6, 2020, “Nuclear war is unlikely to cause human extinction”, *Lesswrong*, https://www.lesswrong.com/posts/sT6NxFxso6Z9xjS7o/nuclear-war-is-unlikely-to-cause-human-extinction]-Hayer

There simply aren't enough nuclear warheads to kill everyone directly with kinetic force, and there likely never will be. There are ~14,000 nuclear weapons in the world, and let’s suppose they have an average yield of something like 1 megaton. This is a conservative guess, the actual average is probably closer to 100 kilotons. With a 1 megaton warhead, you can create a fireball covering 3 km², and a moderate pressure wave that knocks down most residential houses covering 155 km². The former kills nearly everyone and the latter kills a decent percentage of people but not everyone. Let's be conservative and assume the pressure wave kills everyone in its radius. 14,000 \* 155 = 2.17 million km². The New York Metro area is 8,683 km². So all the nuclear weapons in the world could destroy about 250 New York Metro areas. This is a lot! But not near enough, even if someone intentionally tried to hit all the populations at once. Total land surface of earth is: 510.1 million km². Urban area, by one estimate, is about 2%, or 10.2 million km.² Since the total possible area destroyed from nuclear weapons is ~2.17 million km² is considerably less than a lower bound on the area of human habitation, 10.2 million km², there should be basically no risk of human extinction from kinetic destruction.