Russia DA

[Argument Glossarry 2](#_Toc106696484)

[Introduction 3](#_Toc106696485)

[Debating the Russia DA 4](#_Toc106696486)

[Topic Introduction Russia DA 5](#_Toc106696487)

[1NC Summaries 6](#_Toc106696488)

[1 NC Russia Disadvantage Shell 7](#_Toc106696489)

[1NC Impact Scenario: Economic Collapse 10](#_Toc106696490)

[2NC/1NR Link- AI Technology 12](#_Toc106696491)

[2NC/1NR Link- Cyber Security 13](#_Toc106696492)

[2NC/1NR Nuclear War Impact Extension 14](#_Toc106696493)

[2NC/1NR Answers to Russian Aggression 16](#_Toc106696494)

[2NC/1NR Answers to NATO Necessary 17](#_Toc106696495)

[2NC/1NR Answers to No Miscalculation 18](#_Toc106696496)

[2NC/1NR Answers to Diplomacy Reduces Russia Aggression 21](#_Toc106696497)

[2NC/1NR Answer to Non-Unique- Cybersecurity 23](#_Toc106696498)

[2NC/1NR Answers to No-Impact- Cybersecurity 24](#_Toc106696499)

[2NC/1NR Answers to No-Link- Cybersecurity 25](#_Toc106696500)

[2AC Answers to Russia DA 26](#_Toc106696501)

[AFF Extension- No Russian Aggression due to NATO Expansion 29](#_Toc106696502)

[AFF Extension- No Nuclear War Impact 30](#_Toc106696503)

[AFF Extension- No Economic Collapse Impact 31](#_Toc106696504)

## Argument Glossarry

**Nuclear Exchange (noun)** – Another term for nuclear warfare

**Tantamount** (noun) – equally as serious as

**The Cold War** (noun) – A proxy war, meaning an era of serious political tension and aggression, between the United States and the Soviet Union from 1947 to 1991

**Brinkmanship** (noun) – Brinkmanship is the practice of trying to achieve an advantageous outcome by pushing dangerous events to the brink of active conflict. The tactic occurs in international politics, foreign policy, labor relations, contemporary military strategy, and high-stakes litigation

**OECD** (noun) – Organization for Economic Cooperation and Development

## Introduction

Welcome to the Russia Disadvantage Evidence Set. In here, you’ll find all the research you’ll need to construct a winning disadvantage argument in the Novice Division and beyond on the negative for the novice affirmatives on this year’s topic: AI technology and cybersecurity.

We’ve organized this evidence into a few different categories:

•1NC: This section of the file includes the cards that should be read on the negative in the first negative constructive. These cards should be read in addition to other case arguments that you may already be more familiar with

•Negative Extensions: This section of the file includes arguments to bolster the claims you’ve made in the 1NC in later speeches in the debate, specifically the 2NC and 1NR.

•Affirmative Answers: This section includes the cards the affirmative team will need in order to answer the Russia DA.

How to use this file:

The file is organized by side and the components of a disadvantage. You will need to pick and choose which arguments you will make in a given round after the 1NC. You will not have time to make all of these arguments in any round.

1. Read the summaries of each argument available in the packet.

2. Check out the glossary to make sure you understand all of the words and terms.

3. Read and highlight the evidence, making sure you understand the argument being made and pulling out the key parts of each piece of evidence.

4. Pick the arguments you will use in the negative block and as the affirmative.

## Debating the Russia DA

The goal of the negative is simple: Prove that the plan presented by the affirmative team is a bad idea. The more you focus on the plan and why it is a bad idea, the more often you’ll win debates. The Russia DA is one way you can prove the affirmative is a bad idea. It argues that even if the plan has some good effects it starts a chain reaction that changes how Russia will react and that causes bad impacts.

Speaking Roles on the Negative:

•1st Negative Speaker: Your job is to introduce a range of negative arguments in the 1NC, and to definitively win at least one of those arguments in the 1NR.

•2nd Negative Speaker: Your job is to expand upon one or two arguments made in the 1NC, then to choose the best argument made by the negative team and show why the negative should win the debate in the 2NR. You are in charge of choosing negative strategy, since you’ll have to explain it in the 2NR. \*NOTE: In the block decide who will take the DA and only address those arguments in the 2NC or the 1NR. The other speaker can take the case arguments. This is the best way to divide labor in the block.\*

## Topic Introduction Russia DA

The Russia disadvantage argues that NATO increasing their AI and cybersecurity technology is dangerous as it sends the wrong message to Russia. Russia is strongly opposed to the expansion of NATO, including their AI and cybersecurity developments, as they believe the organization poses a threat to their security. Therefore, if NATO increases cooperation within AI and cybersecurity, Russia will feel threatened and develop their own technology. As a result, NATO and Russia will enter an arms race which will create high tensions, increase the risk of miscalculation, and lead to nuclear war.

**Strategic Overview**:

To win the DA you will need to win that the risk of Russia developing their own AI and cybersecurity technology in response to the perceived threat of NATO expanding their AI and cybersecurity capabilities is more important than the impacts the affirmative claims. You will also need to win that the affirmative uniquely causes this change, and that it would not occur otherwise.

Debating the DA as the negative and affirmative:

When putting together your 1NC block, you’ll want to read the argument straight down. This will start a new flow sheet for the DA so you don’t need to worry about lining these arguments up with anything.

The 2AC will then number their responses straight down to set the order for the flow in the debate. For example:

1. Non-unique <insert card>

2. No link <insert card/analytic>

3. No link <insert card/analytic>

4. No internal link <insert card/analytic>

5. No impact <insert card/analytic>

6. Our impact outweighs <insert card/analytic>

\*Note: While some of these arguments can be analysis you will want a healthy mix of cards in the debate, particularly for claims that will need more expertise or proof.

The block then answers the 2AC. Either the 2NC or the 1NR will be responsible for winning the DA. They will answer those arguments using line by line and the “they say/we say” method:

“They say non-unique however, that’s not true because we say: <insert card/analytic>”

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:

•How does Russia perceive NATO?

•How would Russia react if they thought NATO was increasing their AI and cybersecurity capabilities?

•How likely is the risk of miscalculation if tensions are high between Russia and NATO?

•How should the judge evaluate the impacts of the aff and neg against each other?

## 1NC Summaries

1. Uniqueness:
   1. Tadjdeh, 2021: Russia is currently expanding its AI and cyber security technology by heavily investing within these sectors.
2. Link:
   1. Russia has a long history with NATO in which part of the reason for the organization’s establishment was to combat former Soviet Union aggression. As a result, Russia views NATO as a threat to their security therefore being aggressive at any sign of NATO expanding its capabilities, including AI and cyber security technology.
   2. The current AFF plan calls for further NATO cooperation within AI technology and cyber security which puts Russia on alert. Russia sees NATO’s increasing ventures into AI and cyber security as a threat to their development within the field. Russia is afraid that NATO and its allies may bolster their capabilities to an extent in which Russia cannot compete.
   3. Marijan, 2022: Consequently, Russia feels pressure to further engage in AI and cyber security advancements therefore creating an arms race in which both NATO countries and Russia are developing new AI technology. The issue with this new AI technology is that they are preliminary therefore at high risk for errors and miscalculation.
3. Impact:
   1. Fisher, 2022: If Russia perceives NATO expansion as a threat to their security, they are likely to use their emerging AI and cyber security technology which is a risk for miscalculation given the new nature and current conflict with Ukraine.
4. Impact Scenario-Economic Collapse:
   1. Bloomberg and Horobin, 2022: The global economy is extremely vulnerable right now given factors like COVID-19 and the Ukraine-Russia conflict. Therefore, any provocation from NATO that will make Russia more aggressive is dangerous as it has the potential to further disrupt the world’s economy.
   2. UNCTAD, 2022: A global economic collapse does not only affect the economy, but it has real human impacts. Given the current global climate, people in vulnerable countries risk facing food shortages, extreme debt, and blackouts if they are further burdened with a failing economy.

## 1 NC Russia Disadvantage Shell

#### Uniqueness: Russia is increasing AI and cyber security innovation.

Tadjdeh, 2021, (Yasmin, N/A) “Algorithmic Warfare: Russia Expanding Fleet of AI-Enabled Weapons”. National Defense. 07/20. https://www.nationaldefensemagazine.org/articles/2021/7/20/russia-expanding-fleet-of-ai-enabled-weapons

Russia — which has made no secret of its artificial intelligence ambitions — is building a cadre of AI-enabled, autonomous weapon systems that could one day threaten the United States. “The Russian military seeks to be a leader in weaponizing AI technology,” Lt. Gen. Michael Groen, director of the Pentagon’s Joint Artificial Intelligence Center, told National Defense.

The JAIC — which has been working to facilitate AI adoption across the Defense Department since 2018 — recently commissioned a report by CNA, a research organization based in Arlington, Virginia, to examine Russia’s developments. The report — titled “Artificial Intelligence and Autonomy in Russia” — identified more than 150 AI-enabled military systems in various stages of development, Groen said in an email in June. Key areas of interest include autonomous air, underwater, surface and ground platforms. The nation wants to use AI for electronic warfare, intelligence, surveillance, reconnaissance and strategic decision-making processes as leaders pursue information dominance on the battlefield, Groen said.

While Russia is not a leader in commercial and academic AI research — as the United States and China are — it would be a grave mistake for the Pentagon to take its eyes off the threat, he said. “Russia was not a major leader in the development of the internet or computer networking, but Russia has become a leader in weaponizing those technologies for advanced cyberattacks and cybercrime capabilities,” he noted. The Russian military has taken significant steps to reform and improve the organization of its research and development enterprise, he noted. This was done in part because Moscow believed its previous structures were stifling innovation in technology areas such as AI.

The scale of these reforms — such as creating a new advanced R&D organization modeled on the Pentagon’s Defense Advanced Research Projects Agency — demonstrates the nation’s seriousness about fielding an AI-enabled fighting force, he said. Vice Chairman of the Joint Chiefs of Staff Gen. John Hyten noted that Russia has invested enormous resources into the development of artificial intelligence, big data and software technologies. The country is moving quickly across many areas, including nuclear weapons, space and cyber, he said during remarks at the Defense Department’s AI Symposium in June. Embedded in each of those elements is new software, processing and artificial intelligence systems.

“Russia is a significant threat, especially in the near term,” he said. “It is a challenge to not just keep up with them but stay ahead of them.” Like the United States, Russia is working to digitize its military. Its Ministry of Defense recently announced it intends to create a specialized department to develop AI, according to the CNA report. It is even working on developing a military information sharing structure that resembles the Pentagon’s joint all-domain command and control, or JADC2, effort.

#### Link: If Russia perceives NATO as a huge threat, they are likely to engage in risky AI technology which is at high risk for errors leading to miscalculation.

Marijan, 2022, (Branka, Senior Researcher at Project Ploughshares), “Beyond Ukraine: AI and the Next US-Russia Confrontation”. Centre for International Governance Innovation. 02/14. <https://www.cigionline.org/articles/beyond-ukraine-ai-and-the-next-us-russia-confrontation/>

Two titans from the Cold War era seem set to go another round, this time over the prospect of Ukraine’s membership in the North Atlantic Treaty Organization (NATO), which the United States calls a sovereign Ukrainian decision and Russia opposes vehemently. Whatever the outcome of the current standoff, another confrontation between the United States and Russia that merits closer attention is brewing — one that may fundamentally reshape the US-Russia security relationship in the not-so-distant future. Both states are heavily committed to the use of artificial intelligence (AI) in military systems and operations, including logistics, command and control, and intelligence collection and analysis, as well as to the development of more autonomous weapons. As tensions rise, these countries are likely to employ capabilities that are enhanced by AI and machine learning in cyberattacks and misinformation and disinformation campaigns. Rising political temperatures might well encourage fast-tracking of more autonomous military systems as each side seeks to gain the advantage.

The United States and Russia have already tested several autonomous systems. Russia has made important advances on autonomous tanks, while the United States has demonstrated a number of capabilities, including swarming munitions, which have the ability to destroy a surface vessel using a swarm of drones. At the moment, the United States is at the forefront of the development of autonomous systems and military AI applications. However, Russia has approached China to partner with it in building its AI readiness, and such a partnership could be a game changer. One crucial concern is that the growing autonomy and use of AI in decision making in existing weapons platforms and in cyberspace will result in the deployment of immature systems; the result could be accidents that help to escalate conflict. At the same time, both Russia and the United States have prevented progress on new international norms and agreements on the development and use of autonomous systems that could help to avoid dangerous situations. The United States and its allies are developing norms on responsible military uses of AI, but little dialogue with potential adversaries has taken place. And so, the competition between the great powers is allowed to grow unchecked.

The United States and other NATO members are already bolstering Ukrainian cyber defences in expectation of cyberattacks by Russia on Ukraine’s infrastructure, including its electrical grid, communication systems and government departments. Yet Russia could use AI to overwhelm Ukrainian systems in conjunction with misinformation and disinformation campaigns, some of which might involve manufactured or manipulated images or video, known as deepfakes. While cyber and misinformation tactics are not new, AI and machine learning are offering novel ways to engage in them. And, while Western media and analysts focus on Russian cyber techniques, it is almost certainly true that the United States and other NATO members are also pursuing some of these same tactics against Russia.

#### Impact: NATO intervention on Ukraine will escalate probability of nuclear retaliation from Russia suggested by former statements made by Putin.

Fisher, 2022. (Max, an international reporter and columnist for The New York Times, March 16). As Russia Digs In, What’s the Risk of Nuclear War? ‘It’s Not Zero.’ The New York Times. <https://www.nytimes.com/2022/03/16/world/europe/ukraine-russia-nuclear-war.html>

As Russia and NATO escalate their standoff over Ukraine, nuclear strategists and former U.S. officials warn that there is a remote but growing risk of an unintended slide into direct conflict — even, in some scenarios, a nuclear exchange.

“The prospect of nuclear conflict,” António Guterres, the United Nations secretary general, warned this week, “is now back within the realm of possibility.”

Leaders on both sides emphasize that they consider such a war unthinkable, even as they make preparations and issue declarations for how they might carry it out. But the fear, experts stress, is not a deliberate escalation to war, but a misunderstanding or a provocation gone too far that, as each side scrambles to respond, spirals out of control.

The war in Ukraine heightens these risks to a level not seen since the Cuban Missile Crisis, and in some ways is potentially more dangerous than that, some experts say.

NATO forces, intended as defensive, are massing near Russian borders that, with much of Russia’s military bogged down in Ukraine, are unusually vulnerable. Increasingly paranoid Kremlin leaders, faced with economic devastation and domestic unrest, may believe that a Western plot to remove them is already underway.

Russia has said that it considers the weapons and other increased military aid that Western governments are sending to Ukraine tantamount to war, and has implied that it might strike NATO convoys. Over the weekend, Russian missiles struck a Ukrainian base mere miles from Polish territory.

“Those are the things that make me really concerned about escalation here,” said Ulrich Kühn, a nuclear strategist at the University of Hamburg in Germany. “The chance for nuclear weapons employment is extremely low. But it’s not zero. It’s real, and it might even increase,” he said. “Those things could happen.”

The Kremlin has turned to nuclear saber-rattling that may not be entirely empty of threat. Russian war planners, obsessed with fears of NATO invasion, have implied in recent policy documents and war games that they may believe that Russia could turn back such a force through a single nuclear strike — a gambit that Soviet-era leaders rejected as unthinkable.

The outcome of such a strike would be impossible to predict. A recent Princeton University simulation, projecting out each side’s war plans and other indicators, estimated that it would be likely to trigger a tit-for-tat exchange that, in escalating to strategic weapons like intercontinental missiles, could kill 34 million people within a few hours.

## 1NC Impact Scenario: Economic Collapse

#### Global economy is weak and miscalculation could lead to economic collapse.

Bloomberg and Horobin, 2022, (William, NA), “Shock of War Threatens Lasting Impact on Global Economy”. Time. 06/08. <https://time.com/6185394/global-economy-war/>

The world economy will pay a “hefty price” for the war in Ukraine encompassing weaker growth, stronger inflation and potentially long-lasting damage to supply chains, the Organisation for Economic Co-operation and Development (OECD) said. The organization slashed its outlook for global growth this year to 3% from the 4.5% it predicted in December and doubled its inflation projection to nearly 9% for its 38 member countries, according to forecasts released on Wednesday in Paris. In 2023, it expects growth to slow to 2.8%.The price of war could be “even higher,” it warned, describing a long list of risks ranging from an abrupt cut-off of Russian supply in Europe to vulnerabilities on financial markets from high debt and elevated asset prices. “There have been several significant changes in the global economic environment in recent months, including the worldwide spread of the Omicron variant of Covid and the greater-than-expected persistence of inflationary pressures,” the organization said in its economic outlook. “The single greatest change, however, is the economic impact of the war in Ukraine.”

The gloomy assessment, which echoes a similar warning from the World Bank, indicates a deeper and broader economic fallout from Russia’s invasion that will make it harder to set the right fiscal and monetary policies. This is the first detailed view from the OECD, which didn’t issue full forecasts in April because of the prevailing uncertainty. The early effects of surging prices have already forced central banks to tighten monetary policy, with the US Federal Reserve for example having just raised interest rates at a quickened pace of 50 basis points last month. Meanwhile governments are rethinking spending plans as they attempt to shelter households. While the OECD said it’s warranted for all monetary authorities to pare back stimulus, it urged caution particularly in the euro area, where surging prices mainly reflect supply pressures. “Central banks will have to conduct a delicate balancing act between keeping inflation under control and maintaining the post-pandemic economic rebound, especially where the recovery is not yet complete,” the organization said. Chief Economist Laurence Boone, speaking to reporters in Paris, said that disruption to the global economy could leave a lasting impact on investment. “We had a series of shocks, first the pandemic, then the war, and in some countries the supply side of the economy has not fully recovered,” she said. “The longer this lasts, the longer global supply chains are disrupted and the less there would be appetite for investment.” The OECD observed that inflation is hitting living standards and reducing consumer spending across the globe, and business are becoming less optimistic about future production. Crucially, that hit to confidence is deterring investment, which in turn threatens to hurt supply “for years to come,” it said. Still, the organization is cautious about whether the global economy is on the brink of stagflation despite similarities with the oil shock of the 1970s. Compared to that time, major economies are less energy intensive, central banks have more robust frameworks and independence, and consumers have a stock of excess savings leftover from the Covid pandemic, it said. “Nonetheless, there are clear risks that growth could slow more sharply than expected and inflationary pressures could intensify further,” the OECD said

#### Negative impact on global food supply, energy, and financial sector following effects of Russia-Ukraine conflict.

UNCTAD, 2022, (UNCTAD, the UN trade and development body. It supports developing countries to access the benefits of a globalized economy), “World on brink of “perfect storm” of crises, warns un chief calling for immediate action to avert cascading impacts of war in Ukraine”. UNCTAD. 04/13. https://unctad.org/press-material/world-brink-perfect-storm-crises-warns-un-chief-calling-immediate-action-avert

The war in Ukraine is setting in motion a three-dimensional crisis - on food, energy and finance - that is producing alarming cascading effects to a world economy already battered by COVID-19 and climate change, according to the new findings of the Global Crisis Response Group (GCRG). “We are now facing a perfect storm that threatens to devastate the economies of developing countries,” said UN Secretary-General António Guterres. “The people of Ukraine cannot bear the violence being inflicted on them. And the most vulnerable people around the globe cannot become collateral damage in yet another disaster for which they bear no responsibility.” “Our world cannot afford this. We need to act now,” stressed the Secretary-General calling for urgent, concrete and coordinated action to help countries and communities most at risk avert the interlinked crises. “We can do something about this three-dimensional crisis. We have the capacity to cushion the blow.”

As two of the world’s breadbaskets, Russia and Ukraine provide around 30% of the wheat and barley we consume. Russia remains the world’s top natural gas exporter, second-largest oil exporter and a significant producer of fertilizers. The war has severely affected food, energy and financial markets, sending commodity prices to soar record high. Global economic growth is forecast to decrease by 1% in 2022. Preliminary analysis suggests that as many as 1.7 billion people in 107 economies are exposed to at least one of three risks, mostly in Africa, Asia and the Pacific, and Latin America and the Caribbean. When combined with the already devastating impacts of the COVID-19 crisis and climate change, the exposure to just one risk is dire enough to cause debt distress, food shortages and blackouts.

## 2NC/1NR Link- AI Technology

#### Russia vamping up AI technology in military sector amid concerns of US security threats.

Eversden, 2021, (Andrew, American University Graduate, Congressional Reporting Fellow for Texas Tribune), “A Warning to DoD: Russia advances quicker than expected on AI, battlefield tech”. C4ISRNET. 05/24. <https://www.c4isrnet.com/artificial-intelligence/2021/05/24/a-warning-to-dod-russia-advances-quicker-than-expected-on-ai-battlefield-tech/>

WASHINGTON — The Russian military is more technologically advanced than the U.S. realized and is quickly developing artificial intelligence capabilities to gain battlefield information advantage, an expansive new report commissioned by the Pentagon warned. The federally funded Center for Naval Analyses examined the Kremlin’s whole-of-government approach for artificial intelligence development and found it is largely driven by the perceived threat from the United States, combined with lessons learned from its continuing conflicts in Syria and Ukraine about what the future battlefield will look like, the report released Monday said.

The Russian military has AI initiatives to improve command and control and decision-making; early warning and air defense; and training, logistics, maintenance and procurement — from the tactical level to the strategic planning level in Moscow. The Russian government is using artificial intelligence to analyze changing geopolitical events using data from previous global armed conflicts, the report found. Operationally, its military is trying to link platforms across different military branches to share information in order to “to better coordinate forces and make faster decisions,” similar to the Pentagon’s new joint war-fighting concept known as Joint All-Domain Command and Control.

Russia perceives that the U.S. will sow domestic unrest in its country by trying “to undermine Russian authorities and create instability within Russia to foment political change, leading to a justification for U.S. military action,” the report read. That view of how the U.S. could attack is driving technology investment in many areas, including global event analysis. An air assault from the United States is one of its biggest security fears for the Kremlin, hence its investments in AI technologies for early-warning systems and air defense. Its military strategists believe the processing power of AI will allow air defense systems to more quickly monitor, detect and respond to any aerial attack. “Russia is trying to understand what the Americans are up to or what the NATO is up to,” Bendett said. “So NATO and the United States are very much in focus. And a lot of the Russian efforts in AI, military autonomy are actually geared towards how can they best counter the U.S. threat perception.”

The story is similar for Russia’s perception of the future of autonomous weapons, another area where it’s investing. The CNA analysis found substantial debate over the ethics and future of autonomous weapons and having a human “in the loop” of the decision cycle. Russia’s military views completely autonomous weapons as an “inevitability” based on its perceptions of U.S. and China that the systems will become fully autonomous. “This is part of the overall Russian security mindset about the United States … that where we have an advantage, we’re just going to keep pushing,” Edmonds said.

## 2NC/1NR Link- Cyber Security

#### The plan continues to push NATO expansion triggering US cyber security attacks from Russia.

O’Connor & Jamali, 2022. (Tom  an award-winning senior writer of foreign policy at Newsweek, Naveed a Newseek editor and former FBI double agent, January 24). Russia Could Launch Cyber Attacks Against U.S. if Biden Sends Wrong Signals, Intel Warns. Newsweek. <https://www.newsweek.com/russia-could-launch-cyber-attacks-against-us-if-biden-sends-wrong-signals-intel-warns-1672280>

In a new memo obtained by Newsweek, the Department of Homeland Security has warned of Russia's potential to launch cyberattacks against the United States in response to a possible escalation of the crisis unfolding at the border with Ukraine. "We assess that Russia would consider initiating a cyber attack against the Homeland if it perceived a US or NATO response to a possible Russian invasion of Ukraine threatened its long-term national security," the memo, dated January 23 and attributed to the Office of Intelligence and Analysis, reads in bold text.

The warning came as President Joe Biden sent additional weapons to Ukrainian forces and reportedly weighed the option of sending thousands of U.S. troops to the Baltic states bordering Russia over concerns that Moscow was planning imminent military action against Ukraine. Kyiv has defied the Kremlin's protests by seeking membership in the NATO Western military alliance, something that Russian officials have said threatened their country's national security. The bloc has expanded eastward since the fall of the Soviet Union three decades ago and has refused to rule out including Ukraine as well.

The memo detailed a range of ways in which Russia may choose to unleash its cyber arsenal in the event of a flare-up while noting such an action would be unprecedented. "Russia maintains a range of offensive cyber tools that it could employ against US networks — from low-level denials-of-service to destructive attacks targeting critical infrastructure," the memo read. "However, we assess that Russia's threshold for conducting disruptive or destructive cyber attacks in the Homeland probably remains very high and we have not observed Moscow directly employ these types of cyber attacks against US critical infrastructure — notwithstanding cyber espionage and potential prepositioning operations in the past."

## 2NC/1NR Nuclear War Impact Extension

#### Miscalculation risks triggering global nuclear conflict leading to mass death and extinction.

Kallenborn, 2022, (Zachary, Research Affiliate with the Unconventional Weapons and Technology Division of the National Consortium for the Study of Terrorism and Responses to Terrorism (START), Policy Fellow at the Schar School of Policy and Government), “Giving an AI control of nuclear weapons: What could possibly go wrong?”. Bulletin of the Atomic Scientists. 02/01. <https://thebulletin.org/2022/02/giving-an-ai-control-of-nuclear-weapons-what-could-possibly-go-wrong/>

If artificial intelligences controlled nuclear weapons, all of us could be dead. That is no exaggeration. In 1983, Soviet Air Defense Forces Lieutenant Colonel Stanislav Petrov was monitoring nuclear early warning systems, when the computer concluded with the highest confidence that the United States had launched a nuclear war. But Petrov was doubtful: The computer estimated only a handful of nuclear weapons were incoming, when such a surprise attack would more plausibly entail an overwhelming first strike. He also didn’t trust the new launch detection system, and the radar system didn’t have corroborative evidence. Petrov decided the message was a false positive and did nothing. The computer was wrong; Petrov was right. The false signals came from the early warning system mistaking the sun’s reflection off the clouds for missiles. But if Petrov had been a machine, programmed to respond automatically when confidence was sufficiently high, that error would have started a nuclear war.

The huge problem with autonomous nuclear weapons, and really all autonomous weapons, is error. Machine learning-based artificial intelligences—the current AI vogue—rely on large amounts of data to perform a task. Google’s AlphaGo program beat the world’s greatest human go players, experts at the ancient Chinese game that’s even more complex than chess, by playing millions of games against itself to learn the game. For a constrained game like Go, that worked well. But in the real world, data may be biased or incomplete in all sorts of ways. For example, one hiring algorithm concluded being named Jared and playing high school lacrosse was the most reliable indicator of job performance, probably because it picked up on human biases in the data.

In a nuclear weapons context, a government may have little data about adversary military platforms; existing data may be structurally biased, by, for example, relying on satellite imagery; or data may not account for obvious, expected variations such as imagery in taken during foggy, rainy, or overcast weather.The deeper challenge is high false positive rates in predicting rare events. There have thankfully been only two nuclear attacks in history. An autonomous system designed to detect and retaliate against an incoming nuclear weapon, even if highly accurate, will frequently exhibit false positives.

In the extremely unlikely event those problems can all be solved, autonomous nuclear weapons introduce new risks of error and opportunities for bad actors to manipulate systems. Current AI is not only brittle; it’s easy to fool. A single pixel change is enough to convince an AI a stealth bomber is a dog. The decision to unleash nuclear force is the single most significant decision a leader can make. It commits a state to an existential conflict with millions—if not billions—of lives in the balance. Such a consequential, deeply human decision should never be made by a computer.

#### Political and technological miscalculations can trigger nuclear war.

Fisher, 2022. (Max, an international reporter and columnist for The New York Times, March 16). As Russia Digs In, What’s the Risk of Nuclear War? ‘It’s Not Zero.’ The New York Times. <https://www.nytimes.com/2022/03/16/world/europe/ukraine-russia-nuclear-war.html>

“The escalation dynamics of a conflict between the U.S. and Russia could easily spiral into a nuclear exchange,” said Dmitry Gorenburg, an analyst of Russian military policy.

Partly this is because, unlike Cold War proxy battles, Ukraine’s war is raging in the heart of Europe, with NATO and Russian forces massed a relatively short drive away from Moscow and several Western capitals. Partly it is because of Russia’s lowered nuclear threshold and heightened sense of vulnerability. But Moscow also seemingly believes that a sort of NATO-Russia conflict has already begun.In these circumstances, Moscow could misconstrue NATO’s troop buildup, or steps of military support for Ukraine, as preparations for just the sort of attack that Russian nuclear policy is designed to meet. “Between volunteers from NATO countries, all this NATO weaponry, reinforcement of Poland and Romania,” Mr. Charap said, “they might connect dots that we didn’t intend to be connected and decide they need to pre-empt.”

In such a climate, a few mishaps or miscalculations — say, an errant strike or clumsy provocation by one side that sets off a stronger-than-expected retaliation by the other — could escalate, in only a few steps, to the point of triggering Moscow’s fears of an attack.

Mr. Putin has already said that direct Western intervention in the Ukraine war might trigger Russian nuclear retaliation. Now, each uptick in Western support for Ukrainian forces tests those limits. “Part of our problem is that I’m not sure we have a clear sense of exactly where the lines are,” Dr. Gorenburg said, adding, “This is why we’re seeing all the hemming and hawing back and forth with the question of providing aircraft. There’s just uncertainty as to how the Russians would take that.”

The truth is that even Mr. Putin may not know his nuclear red lines for sure. But American fears of Russian nuclear escalation may be dangerous, too. Any nuclear conflict, however initially limited, carries an escalatory risk that strategists call “use it or lose it.” Both sides know that rapid nuclear strikes could wipe out their military forces in Europe, even their entire nuclear arsenals, leaving them defenseless. This means that both sides face an incentive to launch widely before the other can do so first — even if leaders believe that the conflict may have begun in error. Recent advances in short-range missile technology means that leaders now have as little as a few minutes to decide whether or not to launch, drastically increasing the pressure to launch quickly, widely and with only partial information from the ground.

## 2NC/1NR Answers to Russian Aggression

#### NATO expansion triggers Russian aggression.

Bender, 2015, (Jermy, BA in Middle Eastern Studies, Fulbright Fellow), “This is the simplest explanation of why Putin is so opposed to NATO”. Business Insider. 02/12. <https://www.businessinsider.com/simplest-explanation-of-why-putin-hates-nato-2015-2>

Putin's suspicion of NATO can be boiled down to one simple explanation: geography. At the height of the Cold War and the Soviet Union's power, the USSR and its allied Warsaw Pact countries encompassed half of Europe and almost the entirety of Central Asia. But after the demise of the USSR in 1989, lands once within Moscow's orbit quickly peeled away to join NATO. Today, only Belarus remains firmly within Moscow's influence, and even that partnership has teetered recently. For Putin, the peeling away of countries from Russia towards NATO comes as both an existential threat and a personal insult. As a former agent in the KGB and an avowed nationalist, Putin has dreams of resurrecting the glories of Imperial Russia — a goal that is seriously hampered by the inclusion of what Putin would deem rightful Russian lands, such as the Baltics, into the NATO alliance. With this in mind, it is easy to see why Putin signed off on Russia's new military doctrine in December 2014. The doctrine, which placed explicit focus on NATO being Moscow's main existential enemy and threat, called on the further militarization of three geopolitical frontlines: the Russian Baltic Sea exclave of Kaliningrad near Poland, the annexed Crimean Peninsula, and the Arctic.

#### Russia targets the United States in cyberattacks following sanctions in response to the invasion of Ukraine.

Sganga, 2022, (Nicole, CBS News reporter covering homeland security and justice), “"It's coming": President Biden warns of "evolving" Russian cyber threat to U.S.”. CBS News. 03/21. <https://www.cbsnews.com/news/russia-cyber-attack-threat-biden-warning/>

President Biden warned Monday that "evolving intelligence" suggests Russia is exploring options for potential cyberattacks targeting U.S. critical infrastructure. "The magnitude of Russia's cyber capacity is fairly consequential," Mr. Biden said, addressing the Business Roundtable, an association of some of the nation's largest corporations. "And it's coming."

While there's no evidence of any specific cyberattack threat, Anne Neuberger, Mr. Biden's deputy national security adviser for cyber and emerging technology, told reporters Monday afternoon that U.S. officials have observed "preparatory work" linked to nation-state actors. Such activity could indicate increased levels of scanning websites and hunting for vulnerabilities among U.S. companies.

Further details on U.S. intelligence remain unclear, but as Moscow could look for ways to retaliate against economic sanctions imposed following their invasion of Ukraine, potential targets include the U.S. financial sector, electric grid, water treatment plants and hospitals.

## 2NC/1NR Answers to NATO Necessary

#### NATO is not an effective force against Russian cyberattacks given limitations within Article 5.

Lonergan & Moller, 2022, (Erica is an assistant professor in the Army Cyber Institute and a research scholar at the Saltzman Institute of War and Peace Studies at Columbia University, Sara is a former Eisenhower Fellow at the NATO Defense College), “NATO’s Credibility Is on the Line with its Cyber Defense Pledge. That’s a Bad Idea.”. Politico. 04/27. <https://www.politico.com/news/magazine/2022/04/27/nato-credibility-cyber-defense-pledge-russia-ukraine-00027829>

President Joe Biden has issued grave warnings that Russia might launch a cyberattack against the United States in retaliation for the punishing sanctions levied after Moscow’s invasion of Ukraine. He’s advised American companies to “accelerate efforts to lock their digital doors,” and many officials expect an attack against critical U.S. infrastructure to be inevitable.

One way Biden and other Western leaders are attempting to deter potential Russian cyber retaliation during the Ukraine crisis is through NATO’s Article 5 collective defense pledge — that an attack on one is an attack against all. That’s because since the 2014 NATO summit in Wales (which, coincidentally, took place following another Russia-Ukraine crisis), the alliance has affirmed that Article 5 extends to cyberspace. In other words, a cyberattack against any NATO member could conceivably represent an attack against the entire alliance. The pledge is the embodiment of the allies’ security guarantee to each other and the beating heart of NATO.

After Russia invaded Ukraine, NATO Secretary General Jens Stoltenberg confirmed that NATO policy on collective defense and cyberspace holds strong, noting that NATO has “decided to make clear that a cyberattack can trigger Article 5.” And following an extraordinary meeting of heads of state and government on March 24, the alliance reinforced that it is “ready to impose costs on those who harm us in cyberspace.”

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

## 2NC/1NR Answers to No Miscalculation

#### Putin miscalculated threat of NATO expansion triggering war with Ukraine.

Wright, 2022, (Robin, Former correspondent for the Washington Post, CBS News, the Los Angeles Times, and the Sunday Times of London, Recipient of U.N. Correspondents Association Gold Medal), “Putin’s Historic Miscalculation May Make Him a War Criminal”. The New Yorker. 02/24. <https://www.newyorker.com/news/daily-comment/putins-historic-miscalculation-may-make-him-a-war-criminal>

In the eyes of the world and almost certainly history, Vladimir Putin’s invasion of Ukraine on Thursday was an epic miscalculation, drawing comparisons to Adolf Hitler and Saddam Hussein for cold-blooded aggression that could challenge the world order and change its borders. The Russian leader appeared almost delusional in a pre-dawn speech from the Kremlin announcing a “special military operation” to “protect” Donbas, the eastern region where Russian-backed separatists have waged a war for eight years. Putin, instead, immediately ordered Russian tanks into Ukraine and air strikes on the capital and more than a dozen cities in a country of forty million people. “Peace on our continent has been shattered,” the NATO secretary-general Jens Stoltenberg told reporters. “We now have war in Europe on a scale and of a type we thought belonged to history.” Putin’s “reckless” attack risks “countless innocent lives,” Stoltenberg warned.

Putin’s invasion is based on wild accusations, including a claim that he needed to “denazify” Ukraine, a country led by President Volodymyr Zelensky, who is, in fact, Jewish. Putin vowed to end the “humiliation and genocide perpetrated by the Kiev regime,” when, in fact, separatists backed by Russia have for years waged a war in eastern Ukraine. Putin also claimed that the Kyiv government sought to acquire nuclear weapons when, in fact, Ukraine, once the third-largest nuclear power, denuclearized after the Soviet Union collapsed and it became an independent country again. He described the government in Kyiv as a “junta,” even though it was democratically elected in 2019. And Zelensky, in fact, won in a landslide with seventy-three per cent of the vote, defeating thirty-eight others who ran for President. In a plaintive final appeal, Zelensky spoke directly to the Russian people, hours before the attack. “You are being told this is a plan to free the people of Ukraine,” Zelensky said, in an official video in Russian. “But the Ukrainian people are free.” He implored Russian citizens to embrace peace. “Many of you have visited Ukraine. Many of you have relatives here,” he said. “You know our character, you know our people, and you know our principles. You know what we value. . . . Hear us.”

Putin was, in fact, the one who sparked the crisis with an erroneous—even fictional—claim that Ukraine would soon gain membership in NATO. Joining the Western military alliance is an aspirational goal for Ukraine, which it enshrined in a constitutional amendment in 2019. But NATO’s leadership has openly said that Ukraine does not yet qualify for membership. It would have to introduce and enact multiple reforms that may be years away.

#### Russia and China’ strong relationship emboldens Putin to engage in risky AI technological warfare.

Xi, 2021, (Jie, N/A), “NATO’s New Focus Reflects China’s Rise”. VOA News. 10/22. https://www.voanews.com/a/nato-s-new-focus-reflects-china-s-rise-/6282496.html

WASHINGTON —China wasn’t on the agenda at this week’s NATO defense ministers meeting, but by the time the gathering concluded, the secretary-general had said the military alliance needs to respond to the challenges presented by China’s rise. “We see the whole global balance of power is shifting because of the rise of China,” Jens Stoltenberg told reporters Thursday at a press conference in Brussels.

China is “heavily modernizing its military capabilities, including advanced nuclear systems and long-range missile systems," and "we see China coming much closer to us, not least in cyberspace,” he said. And in response, the allies agreed “to do more together." Without giving details, Stoltenberg said NATO would cooperate on a strategy involving areas such as artificial intelligence and technologically advanced weapon systems, “relevant to the challenges posed by the rise of China.” He said that applies not only to Europe, NATO’s traditional focus, but also to challenges in the Asia Pacific, where “the rise of China just makes it even more important that Europe and North America stand together in NATO.” At their June meeting, the allies had agreed to strengthen their relationships with partners in the Asia Pacific, which include New Zealand, Australia, South Korea and Japan.

“China is coming to us. It’s about China being present in Europe as sort of a power that includes investments in defense-related supply chain, investments in ports,” Hamilton said in a phone interview. In their June joint communique, NATO leaders expressed concern over China’s military cooperation with Russia in the Euro-Atlantic region. “China and Russia are collaborating more closely together, and that might affect the risk calculation each of them might take with regards to Western interests,” Hamilton said.“Russia might feel a bit more emboldened when it comes to issues like Ukraine or Belarus or military exercises if it feels China is supporting it,” he added. “Similarly, China might feel it has Russian support, then it might be able to be a bit more adventurous than otherwise it would ordinarily be.”

#### Russia is using killer drones in Ukraine conflict.

Knight, 2022, (Will, Former Senior Editor at MIT Technology Review, Former Editor and Writer at New Scientist), “Russia's Killer Drone in Ukraine Raises Fears About AI in Warfare”. Wired. 03/17. <https://www.wired.com/story/ai-drones-russia-ukraine/>

A RUSSIAN “SUICIDE drone” that boasts the ability to identify targets using artificial intelligence has been spotted in images of the ongoing invasion of Ukraine. Photographs showing what appears to be the KUB-BLA, a type of lethal drone known as a “loitering munition” sold by ZALA Aero, a subsidiary of the Russian arms company Kalashnikov, have appeared on Telegram and Twitter in recent days. The pictures show damaged drones that appear to have either crashed or been shot down. With a wingspan of 1.2 meters, the sleek white drone resembles a small pilotless fighter jet. It is fired from a portable launch, can travel up to 130 kilometers per hour for 30 minutes, and deliberately crashes into a target, detonating a 3-kilo explosive. ZALA Aero, which first demoed the KUB-BLA at a Russian air show in 2019, claims in promotional material that it features “intelligent detection and recognition of objects by class and type in real time.” The drone itself may do little to alter the course of the war in Ukraine, as there is no evidence that Russia is using them widely so far. But its appearance has sparked concern about the potential for AI to take a greater role in making lethal decisions.

“The notion of a killer robot—where you have artificial intelligence fused with weapons—that technology is here, and it's being used,” says Zachary Kallenborn, a research affiliate with the National Consortium for the Study of Terrorism and Responses to Terrorism (START). Advances in AI have made it easier to incorporate autonomy into weapons systems and have raised the prospect that more capable systems could eventually decide for themselves who to kill. A UN report published last year concluded that a lethal drone with this capability may have been used in the Libyan civil war. It is unclear if the drone may have been operated in this way in Ukraine. One of the challenges with autonomous weapons may prove to be the difficulty of determining when full autonomy is used in a lethal context, Kallenborn says.

Despite such uncertainties, the issue of AI in weapons systems has become contentious of late because the technology is rapidly finding its way into many military systems, for example to help interpret input from sensors. The US military maintains that a person should always make lethal decisions, but the US also opposes a ban on the development of such systems. To some, the appearance of the KUB-BLA shows that we are on a slippery slope toward increasing use of AI in weapons that will eventually remove humans from the equation.

## 2NC/1NR Answers to Diplomacy Reduces Russia Aggression

#### NATO and the United States are already working on AI regulations, further developments will simply be provocation for Russian attacks.

Wiggers, 2021, (Kyle, Artificial intelligence writer for VentureBeat), “NATO launches AI strategy and $1B fund as defense race heats up”. Venture Beat. 10/21. <https://venturebeat.com/2021/10/21/nato-launches-ai-strategy-and-1b-fund-as-defense-race-heats-up/>

The North Atlantic Treaty Organization (NATO), the military alliance of 30 countries that border the North Atlantic Ocean, this week announced that it would adopt an 18-point AI strategy and launch a “future-proofing” fund with the goal of investing around $1 billion. Military.com reports that U.S. Defense Secretary Lloyd Austin will join other NATO members in Brussels, Belgium, the alliance’s headquarters, to formally approve the plans over two days of talks.

Speaking at a news conference, Secretary-General Jens Stoltenberg said that the effort was in response to “authoritarian regimes racing to develop new technologies.” NATO’s AI strategy will cover areas including data analysis, imagery, cyber defense, he added.

NATO said in a July press release that it was “currently finalizing” its strategy on AI” and that principles of responsible use of AI in defense will be “at the core” of the strategy. Speaking to Politico in March, NATO assistant secretary general for emerging security challenges David van Weel said that the strategy would identify ways to operate AI systems ethically, pinpoint military applications for the technology, and provide a “platform for allies to test their AI to see whether it’s up to NATO standards.” van Weel said

In 2020, the U.S. Department of Defense (DoD) launched the AI Partnership for Defense, which consists of 13 countries from Europe and Asia to collaborate on AI use in the military context. More recently, the department announced that it plans to invest $874 million next year in AI-related technologies as a part of the army’s $2.3 billion science and technology research budget. Much of the DoD’s spending originates from the Joint Artificial Intelligence Center (JAIC) in Washington, D.C., a government organization exploring the use and applications of AI in combat. (In news related to today’s NATO announcement, JAIC is expected to finalize its AI ethics guidelines by the end of this month.) According to an analysis by Deltek, the DoD set aside $550 million of AI obligations awarded to the top ten contractors and defense accounted for 37% of total AI spending by the U.S. government, with contractors receiving the windfall.

#### Amid Russia-Ukraine conflict Russia considers AI development a priority, any sign of a NATO threat pushes Russia towards further AI innovation and use.

Kahn, 2022, (Jermey, Former Technology Reporter and Senior Writer for Bloomberg Markets, Published in The New York Times, The International Herald Tribune, Newsweek, The Atlantic, Smithsonian, The Boston Globe, and Portfolio), “A.I. is on the front lines of the war in Ukraine”. Fortune. 03/01. <https://fortune.com/2022/03/01/russia-ukraine-invasion-war-a-i-artificial-intelligence/>

Meanwhile, the development of autonomous weapons has continued at a quickening pace. Right now, those weapons are still in their infancy. We won’t see humanitarian groups’ worst nightmares about swarms of “slaughterbot” drones realized in the Ukraine conflict. But weapons with some degree of autonomy are likely to be deployed by both sides. Already, Ukraine has been using the Turkish-made TB2 drone, which can take off, land, and cruise autonomously, although it still relies on a human operator to decide when to drop the laser-guided bombs it carries. (The drone can also use lasers to guide artillery strikes.) Russia meanwhile has a “kamikaze” drone with some autonomous capabilities called the Lantset, which it reportedly used in Syria and could use in Ukraine. The Lantset is technically a “loitering munition” designed to attack tanks, vehicle columns, or troop concentrations. Once launched, it circles a predesignated geographic area until detecting a preselected target type. It then crashes itself into the target, detonating the warhead it carries.

Russia has made A.I. a strategic priority. Vladimir Putin, the country’s president, said in 2017 that whoever becomes the leader in A.I. “will become the ruler of the world.” But at least one recent assessment, from researchers at the U.S. government–funded Center for Naval Analyses, says Russia lags the U.S. and China in developing A.I. defense capabilities. In an interview last week with Politico, one of the study’s authors, Samuel Bendett, told the publication that Russia would definitely use A.I. in Ukraine to help analyze battlefield data, including surveillance footage from drones. He also said that it was possible that China would provide Russia with more advanced A.I.-enabled weapons to use in Ukraine in exchange for gaining insights into how Russia effectively integrates drones into combat operations, an area in which Russia has battle-tested expertise from Syria that China lacks.

A.I. might also play a vital role in the information war. Many fear that A.I. techniques such as deepfakes—highly realistic video fakes created using an A.I. technique—will supercharge Russian disinformation campaigns, although so far there is no evidence of deepfakes being used. Machine learning can also be used to help detect disinformation. The large social media platforms already deploy these systems, although their track record in accurately identifying and removing disinformation is spotty at best. Some people have also suggested A.I. can help analyze the vast amount of open source intelligence coming out of Ukraine—everything from TikTok videos and Telegram posts of troop formations and attacks uploaded by average Ukrainians to publicly available satellite imagery. This could allow civil society groups to fact-check the claims made by both sides in the conflict as well as to document potential atrocities and human rights violations. That could be vital for future war crimes prosecutions.

## 2NC/1NR Answer to Non-Unique- Cybersecurity

#### As Russia feels threatened by the increasing NATO cooperation, they are increasingly likely to launch cyberattacks. The USFG and private sector cybersecurity firms are not prepared to face Russian attacks.

O’Connor & Jamali, 2022. (Tom  an award-winning senior writer of foreign policy at Newsweek, Naveed a Newseek editor and former FBI double agent, January 24). Russia Could Launch Cyber Attacks Against U.S. if Biden Sends Wrong Signals, Intel Warns. Newsweek. <https://www.newsweek.com/russia-could-launch-cyber-attacks-against-us-if-biden-sends-wrong-signals-intel-warns-1672280>

Given past cyber-attacks Washington has attributed to Moscow and the current level of escalation, however, others emphasized a need to reinforce digital defenses.

"Russia has telegraphed that they are willing to attack critical infrastructure here in the U.S.," Brian Harrell, who served as former Department of Homeland Security Assistant Secretary for Infrastructure Protection before his resignation in August 2020, told Newsweek.

"The private sector should work to understand enemy tactics, including spear-phishing and brute force attacks while conducting proactive threat hunting efforts," he added. "We have absolutely entered a heightened period of awareness given the threats that have been made and the demonstrated attacks we've seen from the Russian GRU and Foreign Intelligence Service."

Kyiv has already accused Moscow of employing covert cyber tactics throughout the course of the current dispute, which first began to grab global attention in March of last year and then again in November as up to 100,000 Russian troops amassed near the country's restive border with Ukraine, where Russia-aligned separatists have been active since 2014. An apparent cyber-attack gripped the post-Soviet Eastern European state earlier this month, but Russian officials have dismissed any allegations their government was behind the incident.

In an interview with NBC News on Sunday, Secretary of State Antony Blinken warned that "in the event that there is a renewed Russian incursion, Russian forces going into Ukraine, there is going to be a swift, a severe, and united response" and also threatened such a reaction in response to other things "Russia could do short of sending forces into Ukraine again to try to destabilize or topple the government – cyber attacks, hybrid means, et cetera."

That same day, Peskov too criticized what he called "information hysteria" when it came to the situation between Russia and Ukraine. He placed the blame on the U.S. and NATO, however, and said Western powers were also responsible for real-world provocations as well. "As for concrete actions, we see the statements published by NATO about the increase of the contingent and relocations of forces and means to the eastern flank," Peskov said. "All this leads to an escalation of tensions."

## 2NC/1NR Answers to No-Impact- Cybersecurity

#### Russia is coordinating cyberattacks with military technology making Russian attacks increasingly dangerous in conflict.

The Economist, 2022, “Russia seems to be co-ordinating cyber-attacks with its military campaign”. The Economist. 05/10. <https://www.economist.com/graphic-detail/2022/05/10/russia-seems-to-be-co-ordinating-cyber-attacks-with-its-military-campaign>

In the initial weeks of the Russian invasion, American officials expected Russian cyber-attacks to wreak havoc on Ukraine’s electricity grid, banking system and the like. To their surprise, that did not happen. But a report released by Microsoft suggests that Russian military and cyber-attacks have operated in tandem throughout the war, albeit on a smaller scale than expected. In many cases cyber-attacks occurred within days or hours of missile strikes on similar targets, indicating the attackers may have had overlapping objectives.

On March 1st a Russian hacker group used malicious software against a major Ukrainian broadcaster and other Kyiv-based media organizations; the same day, a Russian missile strike pulverized a television tower in the capital. On March 2nd a nuclear-power company was hacked; the next day, the Russian army occupied Ukraine’s largest nuclear-power station. On March 4th a group affiliated with gru, Russia’s military intelligence service, carried out cyber-operations against a government agency’s network in the city of Vinnytsia. Two days later, Russian missiles struck an airport in the same city. While the cyber-attacks have been limited in scope, their use alongside the military is probably designed to disrupt Ukrainian administration.

The number of Russian cyber-operations has doubled every month since December, when 15 were reported. This only includes attacks that Microsoft was able to detect in its own networks—the true number is likely to be higher. But because the Russians are conducting disruptive attacks, they are much more likely to be found out than pure espionage, such as Chinese intelligence gathering against America, reckons Benjamin Read, director of espionage analysis at Mandiant, a cybersecurity firm.

At least six Russian hacking groups were responsible for these operations in Ukraine, which were designed mainly to destroy files in computer systems, but also to gather intelligence, cut off access to information and support efforts to spread misinformation. The attacks, which seem to be more frequent than previously appreciated, highlight a new kind of hybrid warfare. “There has not been a situation before where this much disruption has been going on in a concentrated area in the history of cyber,” says Mr Read. Other governments, wary of Russia, will be watching closely.

## 2NC/1NR Answers to No-Link- Cybersecurity

#### Russia has a history of committing cyberattacks harming critical infrastructure beyond Ukraine given spillover.

Madnick, 2022, (Stuart, Professor of Engineering Systems in the MIT School of Engineering, and Director of Cybersecurity at MIT Sloan (CAMS): the Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity.), “What Russia’s Ongoing Cyber Attacks in Ukraine Suggest About the Future of Cyber Warfare”. Harvard Business Review. 03/07. https://hbr.org/2022/03/what-russias-ongoing-cyberattacks-in-ukraine-suggest-about-the-future-of-cyber-warfare

Unlike conventional attacks, cyberattacks can be hard to accurately attribute. Plausible deniability exists because in many cases, cyberattacks can be launched from an unwitting host. For example, partial control of your home computer could be taken over, without you knowing it and used to initiate a chain of attacks. One such event occurred in 2013 when smart refrigerators were made part of a botnet and used to attack businesses. In 2016, many thousands of home security cameras were taken over and used to disrupt the operations of Twitter, Amazon, Spotify, Netflix and many others. But there’s strong evidence tying Russian hackers to a string of attacks in Ukraine. Going back to 2015, after the Russian invasion of the Crimean Peninsula, suspected Russian hackers managed to knock out electric power for around 230,000 customers in western Ukraine. Attackers repeated the trick the following year, expanding the list of targets to include government agencies and the banking system. In the hours before Russian troops invaded, Ukraine was hit by never-before-seen malware designed to wipe data — an attack the Ukrainian government said was “on a completely different level” from previous attacks.

It’s easy to understand why Ukraine is an appealing target for testing cyberwar capabilities. The country has similar infrastructure to that found in Western Europe and North America. But unlike the United States, the United Kingdom, and the European Union (EU), Ukraine has more limited resources to counter-attack (though the U.S. and EU have both provided support in bolstering its cyber defenses). And while Russia is the obvious suspect, it’s certainly possible that other countries, such as Iran, North Korea, or China, have been testing their own cyber weaponry in Ukraine, too. The larger point here is that there’s little chance that cyberattacks will be limited to Ukraine. Governments and corporations should closely heed what’s going on there, because cyberwar can — and has — quickly spread across borders.

Given that the U.S. and EU have banded together in support of Ukraine, the scope of a cyberwar could be broad. Large scale cyber skirmishes can become global due to a spillover effect. There’s some precedent for what a spillover would look like. In 2017, a suspected Russian attack featuring a piece of malware dubbed “NotPetya” disrupted Ukrainian airports, railways, and banks. But, NotPetya did not to stay in Ukraine. It spread rapidly around the world, infecting — and for a period of time largely shut down — a diverse array of multinational companies including the global shipping company Maersk, the pharmaceutical giant Merck, FedEx’s European subsidiary TNT Express, and among others.

## 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.

## AFF Extension- No Russian Aggression due to NATO Expansion

#### 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.

## AFF Extension- No Nuclear War Impact

#### 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.

## AFF Extension- No Economic Collapse Impact

#### 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.”