HENRY M. JACKSON SCHOOL OF INTERNATIONAL STUDIES

UNIVERSITY of WASHINGTON

TASK FORCE

The Donald C. Hellmann Task Force Program

Navigating New Threats: NATO's Posture on Emerging Technologies

2022

Navigating New Threats:
NATO's Posture on Emerging Technologies

Faculty Advisor
Dr. Sarah Lohmann

Evaluator
Dr. Carol Evans
Director of the Strategic Studies Institute
United States Army War College

Chief Liaison to COE-DAT / USAWC
Lucas Cox

Editor
Trevor Helmy

Coordinators
Katherine Lin
Yanchen Wu

Researchers
Christopher Chromyszak
Samuel Jacobson
Edreese Khosraw
Samuel Lavey
Martha Lewis
Samantha Mabe
Alex Olsen
Christopher Ryals
Kiara Sahagun
Isobel Williamson
Sydney Winstead

Henry M. Jackson School of International Studies
University of Washington, Seattle

Task Force Report Winter 2022

March 2, 2022

Contents

Executive Summary

The North Atlantic Treaty Organization (NATO) faces a volatile global security environment. Climate change will challenge international stability through natural disasters, migration crises, and land degradation. Russia's invasion of Ukraine upended peace in Europe, and the COVID-19 pandemic reminded the world of the lurking danger of public health emergencies. Emergent technologies are revolutionizing conflict between peer and non-peer states, undermining traditional defenses. These forces all threaten international stability and the welfare of NATO member states, but NATO can use emerging technologies to promote defense, deterrence, and resilience.

This report begins by assessing NATO's role in promoting critical infrastructure resilience. This first chapter, written for separate publication by the US Army War College and NATO Center of Excellence Defence Against Terrorism, discusses NATO's existing definitions of critical infrastructure and its framework for building resilience. The chapter also explores ways to mitigate vulnerabilities in NATO member states' critical infrastructure through civil-military cooperation and international partnership.

The report then turns to case studies of four emerging and disruptive technologies. The second chapter analyzes big data and advanced analytics programs, conducting case studies of COVID-19 contact tracing projects within NATO partner nations and counterterrorism surveillance operations. The third chapter investigates the security applications of artificial intelligence (AI). This chapter compares this foundational technology's development tracks in China and the United States. The fourth chapter explores drones and autonomous technologies, surveying NATO's and potential adversaries' offensive capabilities. This chapter also discusses defensive and commercial applications of automation. The fifth chapter assesses global development and deployment of hypersonic weapons, discussing the implications of Russian and Chinese hypersonic capabilities for transatlantic security.

Based on NATO's current posture on emerging technologies and the findings of our case studies, we recommend that NATO:

- coordinate the sharing of important counterterrorism data analytics without maintaining alliance-wide data sets whose scale presents greater vulnerability, thereby prioritizing the security and integrity of national products
- add a big data expert to the NCI agency to promote big data-specific training and to further cooperation between member states
- introduce international AI competitions to develop new military capabilities

- integrate NATO drone defense systems, sensor networks, and early warning systems into a "system-of-systems," using NATO Science for Peace and Security funding
- develop a NATO-wide hypersonics force doctrine that drastically increases spending on strengthening hypersonic defense measures and funds a cross-border hypersonics research consortium
- increase critical infrastructure redundancy using analog and non-networked solutions to reduce the impact of cyberattacks
- mandate a joint NATO-EU critical infrastructure review process that defines vulnerabilities in European critical infrastructure, mandates continent-wide security standards, and has authority over new foreign-backed critical infrastructure projects
- encourage greater funding of and participation in the NATO Innovation Fund

Chapter 1: Mission-Dependent Critical Infrastructure

This chapter discusses the vulnerabilities facing NATO critical infrastructure and proposes ways to promote critical infrastructure resilience. The chapter first summarizes NATO's definitions of critical infrastructure categories. Next, the chapter discusses resilience, detailing NATO's seven baseline resilience requirements. This section also explores riots in Kazakhstan to illustrate the importance of energy infrastructure and describes existing resilience testing procedures in the United States. Third, the chapter outlines the inherent vulnerabilities and external threats facing NATO critical infrastructure. Fourth, the chapter explains the evolution of civil-military cooperation in the operation and protection of critical infrastructure. Finally, the chapter discusses partnerships to promote resilience, focusing on collaborations between the United States and European Union.

Defining critical infrastructure

NATO defines critical infrastructure as "a general term describing a nation's infrastructure assets, facilities, systems, networks, and processes that support the military, economic, political and/or social life on which a nation and/or NATO depends."[1] Put differently, critical infrastructure refers to systems that would cause severe disruptions if destroyed. These systems include power generation, water supply, communications assets, transportation, and energy distribution, among other things.

The Alliance subdivides critical infrastructure into three categories: critical national infrastructure, mission-vital infrastructure, and key infrastructure. These categories are not mutually exclusive. For example, some assets could be both critical national infrastructure and mission-vital infrastructure.

NATO defines critical national infrastructure as "infrastructure identified by the Territorial Host Nation that are integral to the continued delivery and integrity of the essential services upon which the nation relies; the destruction or compromise of which would lead to severe military, economic, political, or social consequences to the nation."[2] Typically, territorial host nations create a National Homeland Defense Plan that identifies critical national infrastructure, which the country then shares with NATO. If a territorial host nation has not made such a plan, NATO itself can identify critical national infrastructure to ensure essential assets are adequately protected.[3]

[1] NATO, *Infrastructure Assessment*, ACO Directive 084-002, October 17, 2019.
[2] NATO ACO Directive 084-002 (2019).
[3] NATO ACO Directive 084-002 (2019).

According to NATO, mission-vital Infrastructure is defined as "infrastructure within the [Joint-Operations Area] which Host Nation and/or NATO/Troop Contributing Nation forces rely on for fielded capability", the destruction of which would create a decisive disadvantage to the NATO mission, likely rendering the entire mission a failure.[4] Meanwhile, key infrastructure is defined as infrastructure which forces rely on for fielded capacity, the destruction of which would bring "a significant challenge to the NATO mission while not precipitating the mission's complete failure."[5] For example, if NATO were operating in a foreign country and were primarily supplying its forces via a maritime port, the port would be considered mission-vital infrastructure. If the port were destroyed, the entire logistics chain would collapse, putting the mission in jeopardy. A railroad that linked the port to inland areas, however, would only be considered key infrastructure in this scenario. It would still be possible to truck in supplies via roads if the railroad were destroyed. While the destruction of the railroad would put NATO forces at a disadvantage, it would not jeopardize the entire mission. By its definition, critical infrastructure is present in every country on Earth, so understanding it is key to building resilience for NATO operations and undermining NATO adversaries.

Resilience

NATO defines resilience as the "collective and continuous effort of all member states to be prepared for and possess the flexibility to overcome any future threat to national security."[6] Today, NATO faces a changing geopolitical landscape, new technologies, and increasingly sophisticated terrorist networks. Russia threatens NATO's eastern flank, challenging NATO's territorial reach; adversaries can use hypersonic missiles to launch a devastating first strike; terrorist groups can exploit cybersecurity weaknesses to render critical infrastructure systems unusable. Attacks can come from anywhere at any time, and there is no guarantee that they would be detected quickly enough for prevention efforts to succeed. Given this environment, it is important that NATO increase its resilience to ensure one blow cannot cripple its infrastructure.

NATO has created seven baseline requirements of resilience for its allies: government continuity, energy, uncontrolled movement of people, food and water, mass casualties, telecommunications, and transportation.[7] High levels of resilience in these areas secure the continuity of government functions and essential services

[4] NATO ACO Directive 084-002 (2019).
[5] NATO ACO Directive 084-002 (2019).
[6] NATO, "Civil Preparedness," *NATO Newsroom*, March 23, 2021, https://www.nato.int/cps/en/natohq/topics_49158.htm.
[7] NATO, "Civil Preparedness."

during and after a crisis. Each area of resilience faces different challenges, and many are dependent on resilience in other areas. Additionally, the military, civilian, and commercial sectors are all dependent on the successful functioning of these areas during a crisis. The NATO baseline requirements serve as a starting point to resilience and as a framework to foster innovation against new emerging threats.

There are four primary means by which NATO and its member states can strengthen resilience: building persistence, capacity consideration, education, and training.[8] Building persistence requires a critical, continuous assessment of areas in which member states' baseline resilience plan can be more efficient and integrated. There must be a collective public effort to build persistence, achievable if the public is well-informed. Capacity consideration refers to recognizing that increasing resilience requires a holistic approach in which resources are dedicated to innovation and collaboration.[9] Education is another critical component of strengthening resilience, as a well-informed public will encourage innovation. Furthermore, education provides a pathway to training by conducting model simulations that test resilience.[10] Training to strengthen resilience requires total comprehension of possible risks, the realities of the complex environment, and how systems behave when exercised to the point of failure. NATO furthers resilience education by publishing resources like its Counter-Terrorism Reference Curriculum.[11]

Kazakhstan riots and the importance of energy sector resilience

Many examples of critical infrastructure failures have led to a deteriorated security situation. For NATO, monitoring and preventing terrorist attacks and malicious attacks by state actors is of the utmost importance. It is nevertheless critical to understand that critical infrastructure failure can occur due to systemic policy failures, which in turn can deteriorate into adverse security situations relevant to NATO. While not in the NATO Joint Area of Operations, this Task Force found it important to analyze recent developments in Kazakhstan to show how disruptions in civil energy infrastructure led to military intervention by a NATO adversary. This is relevant to NATO as a case study because, if it were to occur in-area, NATO would have an important role to play in securing critical

[8] NATO Supreme Allied Command Transformation (SACT) and City of Norfolk, *Building Resilience – Collaborative Proposals to Help Nations and Partners* (Norfolk, VA: June 2017), 2, https://www.act.nato.int/images/stories/events/2017/resilience/resilience-wp.pdf.
[9] NATO SACT and City of Norfolk, *Building Resilience.*
[10] Jan Hodicky et al., "Dynamic Modeling for Resilience Measurement: NATO Resilience Decision Support Model, " *Applied Sciences* 10, no. 8 (2020): 2639, https://doi.org/10.3390/app10082639.
[11] Sajjan Gohel and Peter Forster, *Counter-Terrorism Reference Curriculum* (NATO Defence Education Enhancement Programme, 2020).

infrastructure as well as deterring adversaries from using civil instability to debilitate partner nations. It also displays how the Russian Federation leverages critical infrastructure vulnerabilities and civil unrest to exert greater geopolitical influence in Central Asia and Eastern Europe. This trend is of increasing concern to NATO in the context of the Russian invasion of Ukraine.

The January 2022 protests and riots in Kazakhstan resulted from a critical infrastructure failure. On January 1st, the government of Kazakhstan lifted price caps on the cost of gasoline, causing the price of fuel to skyrocket.[12] Since fuel is essential to the functioning of modern society, the rapid price increase triggered protests against adverse economic conditions attributed to the government. After days of riots and unrest, the government reimplemented the gas cap to calm the situation.[13] The Kazakh state also called on Collective Security Treaty Organization forces to improve the security situation, leading to the deployment of Russian and other forces into the country.[14]

Increases in fuel prices and negative energy supply shocks in NATO member states adversely affect geopolitical stability and the Alliance's ability to supply its operations. Russia's invasion of Ukraine upended global energy markets, causing energy shortages in Europe and threatening the efficiency of NATO military forces.[15] The Kazakh example illustrates the multifaceted nature of critical infrastructure and how its non-military impacts could impact NATO member states. Unrest from critical infrastructure failure in NATO member states could allow an adversary to strike when the Alliance is vulnerable. Additionally, unrest in other regions can spiral into civil wars that could draw in troops from NATO member states. Ensuring critical infrastructure resilience within the Alliance and in strategic countries around the world is necessary to essential to the security of NATO member states.

Testing resilience

[12] Valerie Hopkins, "Kazakhstan Declares State of Emergency as Protests Over Fuel Prices Spread," *New York Times*, January 4, 2022, https://www.nytimes.com/2022/01/04/world/europe/kazakhstan-emergency-protests-fuel.html.
[13] "Kazakhstan unrest: Government Restores Fuel Price Cap After Bloodshed," *BBC*, January 6, 2022, https://www.bbc.com/news/world-asia-59896471.
[14] Mary Ilyushina, "Russia Sends Troops into Kazakhstan as Clashes Between Security Forces and Anti-Government Protesters Turn Deadly," *CBS News*, January 6, 2022, https://www.cbsnews.com/news/russia-sends-troops-into-kazakhstan-as-protests-turn-deadly.
[15] Herbert Lash and Marc Jones, "Oil Surges Above $100 a Barrel, Stocks Slide on Ukraine Conflict," *Reuters*, March 1, 2022, https://www.reuters.com/markets/europe/global-markets-wrapup-1-2022-03-01/; Kristian Knus Larsen, "Unfolding Green Defense: Linking Green Technologies and Strategies to Current Security Challenges in NATO and the NATO Member States," Centre for Military Studies, University of Copenhagen, December 2015, https://www.jstor.org/stable/resrep05270.4, 3-5.

Testing Alliance states' resilience is critical in identifying weaknesses and avenues for improvement. The following exercises already conducted by the United States can serve as a template for other NATO member states to identify shortcomings in their operations and develop testing regimes. These exercises represent a cross-governmental approach to infrastructure resilience testing, assess resilience across various sectors, and promote resilience before and after crises.

The United States government, cooperating with civil and private sector partners, regularly assesses the resilience of national energy infrastructure. For example, the US Department of Energy, in conjunction regulatory authorities like the North American Electric Reliability Corporation (NERC), has orchestrated energy resilience readiness exercises in which it cut power to military bases to test energy resilience in the continental United States. As of April 2020, five bases had undergone these assessments to test the "performance of the infrastructure, the efficiency of emergency generators, and impact on residents to the unannounced power outage."[16] In the coming years, the United States will also complete Installation Energy and Water Plans to assess shortcomings in its current ability to provide energy and water during a crisis.[17]

In 2010, the US Department of Homeland Security began collaborating with the private sector to promote and test cyber security.[18] The US Army War College's Center for Strategic Leadership and Development (CSLD) has led wargames, workshops, and training for Army leaders to model the best policy responses and illuminate vulnerabilities during a cyberattack. The CSLD has also worked extensively with Congresspeople, legislators, academics, and scientists to develop military and civilian resilience and maintain vital services during a crisis.[19] The Air Force has also collaborated with academic institutions to host cybersecurity and resilience workshops, examining vulnerabilities within current infrastructure, and creating more sophisticated disaster preparedness models.[20]

Additional US government agencies test infrastructure resilience in the United States. The DHS has a diverse array of procedures to run preventative tests and assess infrastructure capabilities in the aftermath of a crisis. The DHS's

[16] Alex Beehler and J.E. Surash, "Cutting the Cord to Test Energy Resilience," US Army, April 12, 2020, https://www.army.mil/article/234514/cutting_the_cord_to_test_energy_resilience.
[17] Beehler and Surash, "Cutting the Cord."
[18] US Department of Homeland Security (DHS), "First Responder / Disaster Resilience," accessed January 20, 2022, https://www.dhs.gov/science-and-technology/first-responder-disaster-resilience.
[19] Cynthia Ayers and Kenneth Chrosniak, *Terminal Blackout: Critical Electric Infrastructure Vulnerabilities and Civil-Military Resiliency* (Carlisle, PA: US Army War College, Center for Strategic Leadership and Development, October 2013), https://publications.armywarcollege.edu/pubs/2983.pdf.
[20] Kylie Foy, "Improving Resiliency in Military Systems Will Require Organizational and Cultural Shifts," MIT Lincoln Laboratory, November 6, 2019, https://www.ll.mit.edu/news/improving-resiliency-military-systems-will-require-organizational-and-cultural-shifts.

Cybersecurity & Infrastructure Security Agency (CISA), for example, has created several platforms that can assess the resilience of services vital to the military. The Infrastructure Visualization Platform and the Security Assessment at First Entry are such tools. CISA's information-sharing with civil authorities and private owners of critical infrastructure through its National Infrastructure Coordinating Center (NICC) displays best practices that could be replicated cross-nationally by NATO authorities.[21] Another CISA program, Emergency Support Platform #14, emphasizes services that would be cut off to both the military and civilians during a crisis. [22]

The DHS Science and Technology Directorate has also expanded the means of testing critical infrastructure resilience, including collaboration with the private sector to test new technology that could serve as back-ups to current infrastructure or help maintain supply chains.[23] This directorate created a Strategic Plan for AI and Machine Learning, which analyzes the risks of these technologies and how they can be incorporated into disaster resilience plans.[24] Additionally, the First Responder/Disaster Resilience research assists the DHS with testing for vulnerabilities immediately following a critical infrastructure failure and maintaining functionality during a crisis.[25] This extensive DHS resilience testing regime, embodies the United States' forward-looking approach to resilience testing. If member states' infrastructure systems were synchronized, NATO could adopt a similar framework for assessing critical infrastructure resilience.

Vulnerabilities in critical infrastructure

To maintain the resilience of their critical infrastructure systems, states must recognize the external threats to critical infrastructure and these systems' inherent vulnerabilities. External threats include cyberattacks, climate change, and public health crises. The Alliance and its members' societies must be prepared for any threat and hazard that might arise, whether from nation-state, a non-state actor, or

[21] Chris Anderson, "National Infrastructure Coordinating Center INSight Application," *U.S. Department of Homeland Security*, November 23, 2007, https://www.dhs.gov/sites/default/files/publications/privacy_pia_nppd_nicc.pdf, 2-7.
[22] US Federal Emergency Management Agency, "Emergency Support Function #14 - Cross-Sector Business and Infrastructure," October 2019, 1, https://www.fema.gov/sites/default/files/2020-07/fema_ESF_14_Business-Infrastructure.pdf.
[23] William Bryan, "The Power of Testing Critical Infrastructure in Operational Settings," US Department of Homeland Security (blog), November 19, 2018, https://www.dhs.gov/science-and-technology/blog/2018/11/19/power-testing-critical-infrastructure-operational-settings.
[24] US Cybersecurity and Infrastructure Security Agency (CISA), "Critical Infrastructure Vulnerability Assessments," accessed January 20, 2022, https://www.cisa.gov/critical-infrastructure-vulnerability-assessments.
[25] US DHS, "First Responder / Disaster Resilience."

the environment. For example, increased cyberattacks have added to the spread of disinformation and have damaged election integrity.[26] These attacks disturb the continuity of government by sowing mistrust in the validity of these elections. Energy resilience allows energy infrastructure to recover quickly from cyberattacks, climate change, and other challenges.[27] Climate change or supply chain issues can diminish food and water supplies in times of crisis and thus threaten access to these vital resources. The coronavirus pandemic and resulting mass casualties overextended many states' healthcare systems to the point of near collapse.[28]

NATO critical infrastructure systems also have multiple inherent vulnerabilities that leave dependent populations at risk. One such danger is the interconnectedness of different types of infrastructure. For example, over 7,000 power plants in the United States are dependent on the functionality of other critical infrastructure facilities and outside supply chains.[29] Additionally, transport system failures can debilitate supply chains during emergencies.[30] As such, NATO has identified that stable critical infrastructure requires self-reliant facilities.[31]

The current American system has additional interdependencies that leave facilities at risk. Current government efforts to prevent these mass shutdowns often require voluntary participation from the private sector owners of these critical infrastructure facilities, but that participation is difficult to ensure.[32] This lack of voluntary preparedness is another inherent vulnerability of critical infrastructure systems. Currently, governments offer information and education about possible hazards to incentivize the private sector to prepare privately-owned critical infrastructure systems for potential disasters.[33] The United States' 2013 National

---

[26] Jamie Shea, "Resilience: A Core Element of Collective Defence," *NATO Review*, March 30, 2016, https://www.nato.int/docu/review/articles/2016/03/30/resilience-a-core-element-of-collective-defence/index.html.
[27] NATO, "Energy Security," *NATO Newsroom*, September 28, 2021, https://www.nato.int/cps/en/natohq/topics_49208.htm.
[28] US National Counterintelligence and Security Center (NCSC), "Insider Threat Mitigation for US Critical Infrastructure Entities: Guidelines from an Intelligence Perspective," March 2021, https://www.dni.gov/files/NCSC/documents/news/20210319-Insider-Threat-Mitigation-for-US-Critical-Infrastru-March-2021.pdf.
[29] Brian E. Humphreys, *Critical Infrastructure: Emerging Trends and Policy Considerations for Congress*, Congressional Research Service (CRS) Report R45809 (Washington, DC: CRS, July 8, 2019), 1, https://www.everycrsreport.com/reports/R45809.html.
[30] US NCSC, "Insider Threat Mitigation."
[31] NATO SACT and City of Norfolk, *Building Resilience*, 2.
[32] Humphreys, *Critical Infrastructure*, 20.
[33] US Cybersecurity and Infrastructure Security Agency (CISA), "A Guide to Critical Infrastructure Security and Resilience," November 2019, 12, https://www.cisa.gov/sites/default/files/publications/Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf.

Infrastructure Protection Plan identified that this method varies in effectiveness, especially when owners are asked to prepare for high-risk and low-probability disasters, including terrorist attacks.[34] This inaction is dangerous because the US Department of Defense (DoD) relies on privately-owned companies to produce their technology.[35] In combination with the interconnectedness of critical infrastructure facilities, this dynamic results in system-wide vulnerability.

In some instances, the very protocols used to analyze critical infrastructure vulnerabilities are not standardized, demonstrating another inherent vulnerability of Alliance critical infrastructure. In 2013 in the United States, the Government Accountability Office found that some states purposely ignored phone calls from the Department of Homeland Security (DHS). They stated that they could not comply with the DHS's security standards because of existing burdens, poor technology, and their own cost-benefit calculations. Some states have also stated that they lacked the expertise to create disaster scenarios and prepare as the DHS wanted.[36] In April of 2007, the Estonian government was attacked in the same way. The government servers were hacked and shut down for hours. In addition to being unable to access these servers for day-to-day government operations, Estonian infrastructure relied on this technology.[37]

Given the high degree of infrastructural interdependence, a critical infrastructure failure in one state can lead to cascading cross-border failures.[38] The risk of cascading failures increases as technologies and critical infrastructure systems become more interdependent. Should one piece of critical infrastructure fail—due to terrorist attacks, biohazards, or the effects of climate change—infrastructure interdependencies will put other connected systems at risk of collapse.

Civil-military cooperation

Building resilience and civil preparedness requires persistent interconnectedness between the civil, private, and military sectors.[39] Civil-military cooperation influences many aspects of security. These general areas of civil-military cooperation include counterterrorism, cybersecurity, natural disasters, biohazards, technological hazards, energy, supply chain challenges, and research and development in hypersonic and other emerging technologies. NATO faces a

[34] Humphreys, *Critical Infrastructure*, 20.
[35] Clay Wilson, *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*, Congressional Research Service (CRS) Report RL32115 (Washington, DC: CRS, January 29, 2008), https://www.everycrsreport.com/reports/RL32114.html.
[36] Humphreys, *Critical Infrastructure*, 7.
[37] Wilson, *Botnets, Cybercrime, and Cyberterrorism*, 6.
[38] Gohel and Forster, *Counter-Terrorism Reference Curriculum*, 95.
[39] NATO SACT and City of Norfolk, *Building Resilience*, 1.

critical point in its existence, needing to determine the extent to which (if at all) it desires to coordinate the development of allies' mission-vital and key infrastructure. Whether NATO commits to civil-military cooperation impacts the future international security environment and, by extension, the future security of critical infrastructure systems.

NATO has become increasingly dependent on civilian infrastructure since the end of the Cold War. Falling defense budgets have intensified the reliance on civil and commercial assets and capabilities.[40] Today, military forces (especially those deployed during crises and war) heavily rely on the civilian and commercial sectors for transport, communications, and basic supplies such as food and water. Around 90 percent of military transport for large military operations is chartered or requisitioned from the commercial sector. On average, the commercial sector provides over 30 percent of satellite communications used for defense purposes. Some 75 percent of host nation support to NATO operations is sourced from local commercial infrastructure and services.[41] Moreover, military medical systems depend on civilian medical infrastructure. Finally, military operations use local civilian expertise and human resources (such as translators) to function successfully.[42] Each of these assets is highly vulnerable, and the prevalence of civilian and commercial assets in military operations reveals a general vulnerability in key- and mission-vital infrastructure.

Significance of civil-military cooperation

Partnerships between the military and civilian sectors can promote infrastructure resilience in two ways. First, civil-military cooperation can increase the mobility and efficiency of military operations. Whenever civilian infrastructure is required to execute a military task, the private and military sectors share the responsibility to address and mitigate the risk.[43] Furthermore, as warfare shifts onto the hybrid digital-social landscape, cooperation between military and private sectors will be integral in defending against cognitive and misinformation attacks.[44]

---

[40] NATO, "Resilience and Article 3," *NATO Newsroom*, June 11, 2021, https://www.nato.int/cps/en/natohq/topics_132722.htm

[41] NATO, "Resilience and Article 3."

[42] NATO, "Civil Preparedness."

[43] Henrik Beckvard and Phillipe Zotz, *Cyber Considerations for Military Mobility*, (Estonia, Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2021), 3, https://ccdcoe.org/uploads/2021/05/Releasable_Cyber-Considerations-for-Military-Mobility_Beckvard_Zotz.pdf.

[44] Johns Hopkins University & Imperial College London, "Countering Cognitive Warfare: Awareness and Resilience," *NATO Review*, May 20, 2021, https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html.

As private companies own platforms on which these attacks occur, civil-military collaboration will be critical in creating response protocols and improved algorithms to detect false information. These partnerships reduce public distrust and social division by countering misinformation, ultimately promoting political stability. These platforms are therefore critical social and political infrastructure.[45]

Second, civil-military cooperation in the construction of nongovernmental-owned infrastructure "can accelerate the technological process" by which new technologies are researched, developed, and put into use.[46] For example, the United States is "supporting an integrated model that leverages government, industry and university resources" to advance the nation's missile capabilities. NATO needs to invest more into cooperation among the civilian and military sectors within certain parameters.[47] There are three specific means by which civil-military cooperation promotes innovation: technology road-mapping, talent recruitment, and cost-efficiency. Technological road-mapping allows companies to address gaps in the technology by "pointing to specific university research that will contribute to closing those gaps."[48] Talent recruitment allows industry employees to work directly with university students who want to work in specific industries, allowing them easier transitions into their careers. Cost efficiency allows for government-funded projects to address challenges within industries. In sum, more cooperation among civilian and military sectors can enable "impactful research that will transition directly to the industry."[49]

Research and development of hypersonic technologies highlights the innovative pressure of civil-military cooperation. In the United States, most weapons research currently takes place inside the US DoD and with industry partners, including non-traditional military partners. In an important example of civil-military cooperation, the US DoD has provided $25.5 million over three years for 18 projects at 29 universities to conduct advanced research on hypersonics to develop the next generation of hypersonic weapons.[50]

---

[45] Johns Hopkins University, Imperial College London & Georgia Institute of Technology, "Countering Disinformation: Improving the Alliance's Digital Resilience," *NATO Review*, August 12, 2021, https://www.nato.int/docu/review/articles/2021/08/12/countering-disinformation-improving-the-alliances-digital-resilience/index.html.

[46] Lockheed Martin, "The Hypersonics Force Multiplier: University Engagement," January 28, 2021, https://www.lockheedmartin.com/en-us/news/features/2021/the-hypersonics-force-multiplier--university-engagement.html.

[47] Lockheed Martin, "The Hypersonics Force Multiplier."

[48] Lockheed Martin, "The Hypersonics Force Multiplier."

[49] Lockheed Martin, "The Hypersonics Force Multiplier."

[50] US Department of Defense, "Defense Department Awards $25.5 Million Over Three Years for Applied Hypersonics Research," October 5, 2021, https://www.defense.gov/News/Releases/Release/Article/2800008/defense-department-awards-255-million-over-three-years-for-applied-hypersonics/.

By contrast, limited cooperation between the public and private sectors can leave civilian assets vulnerable. Privatization incentivizes efficiency and profit, not redundancy and resilience in times of crisis. Some states have also begun voicing their discontent with European cooperation with Russian and China-owned companies, arguing that some countries are putting "economic benefits above the objectives of the Energy Union and broader geopolitical concerns."[51] This dynamic is evident in the European energy market. Germany, for example, partnered with Gazprom, a Russian "state-owned entity," to construct the controversial Nord Stream 2 pipeline.[52] Other European investors such as Engie from France, Shell, a British and Dutch company, and OMW of Austria financially supported the pipeline.[53] If the pipeline had become operational, Russia, through Gazprom, would have become a more dominant supplier of European energy. Analysts in the United States and other NATO member states feared the pipeline would give Russia significant geopolitical leverage and dangerous control over Europe's energy market.[54] Until Olaf Scholz's government canceled the pipeline's certification after Russia's invasion of Ukraine, many therefore feared that Germany's hands-off, pro-commerce attitude on the pipeline was creating vulnerabilities in European critical infrastructure.[55]

NATO's role in facilitating civil-military cooperation

NATO has already worked to promote civil-military cooperation to defend against adversaries. For example, NATO developed guidelines for enhancing civil-military cooperation in response to a chemical, biological, radiological, or nuclear (CBRN) incident. NATO guidance also advises national authorities on warning the public and alerting emergency responders. Moreover, after 2001, the use of civilian aircraft as a weapon in the 9/11 terrorist attacks facilitated NATO's efforts in improving civil-military coordination of air traffic control.[56]

---

[51] Moiek de Jong and Thijs Van de Graaf, "Lost in Regulation: Nord Stream 2 and the Limits of the European Commission's Geo-Economic Power," *Journal of European Integration* 43, no. 4 (August 6, 2021): 495-510, DOI: 10.1080/07036337.2020.1800680.
[52] NATO, "Civil Preparedness;" Andrew Michta, "The Three Seas Initiative Will Reorder NATO's Eastern Flank," *1945* (website), November 2, 2021, https://www.19fortyfive.com/2021/11/the-three-seas-initiative-will-reorder-natos-eastern-flank/.
[53] Michta, "The Three Seas Initiative."
[54] de Jong and de Graaf, "Lost in Regulation."
[55] Melissa Eddy, "Germany Puts a Stop to Nord Stream 2, a Key Russian Natural Gas Pipeline," *New York Times*, February 22, 2022, https://www.nytimes.com/2022/02/22/business/nord-stream-pipeline-germany-russia.html?smid=url-share.
[56] NATO, "Countering Terrorism," *NATO Newsroom*, September 14, 2021, https://www.nato.int/cps/en/natohq/topics_77646.htm.

As the world becomes more connected and the impacts of climate change worsen, critical infrastructure faces environmental threats, including biohazards and natural disasters. War, natural disasters, and biohazards also have secondary impacts on energy infrastructure and supply chains. For instance, the COVID-19 pandemic and war in Ukraine caused dramatic shifts in oil prices.[57]

NATO can facilitate responses to these emerging crises. For instance, NATO partner countries' militaries supported the civilian medical supply during the COVID-19 pandemic by reducing the cost of aircraft transportation. Additionally, the military and civilian sectors are pursuing research and development in renewable energy for households, commercial consumption, and military defense.[58] Military sectors can rely on advanced equipment to rapidly assess the destruction and send out response teams when responding to natural disasters.[59] For example, partnership between NATO members through the NATO Innovation Fund can foster close research relationships between the government and private firms.[60] Nations can use their NATO connections to strengthen its member states' critical infrastructure through creation and innovation. Moreover, this funding relationship establishes the basis for closer working relationships that expedite responses to security failures.

Promoting resilience through partnerships

NATO's greatest strength lies in its ability to ensure the security of its members through coordination and partnerships. This is especially important when it comes to mission-critical infrastructure. Foreign acquisition by NATO adversaries of such critical infrastructure can make it vulnerable to lower security standards or open to direct hacking threats. As NATO moves towards a near-limitless technological frontier of both opportunities and threats, NATO members can leverage this advantage and collaborate to enhance their cyber security and technological security standards, as well as resilience and civil preparedness. The next generation of technologies will present a wide range of new security and defense applications and vulnerabilities.

Partnership between the EU and NATO is a natural relationship due to their shared interest in maintaining Euro-Atlantic security. There is significant potential

[57] Kevin M. Camp et al., "From the Barrel to the Pump: The Impact of the COVID-19 Pandemic on Prices for Petroleum Products," *Monthly Labor Review*, US Bureau of Labor Statistics, October 2020, https://doi.org/10.21916/mlr.2020.24.
[58] Constantine Samaras et al., "Energy and the Military: Convergence of Security, Economic, and Environmental Decision-Making," *Energy Strategy Reviews*, no. 26 (November 2019): 8, https://doi.org/10.1016/j.esr.2019.100409.
[59] NATO, "Resilience and Article 3."
[60] NATO, "Emerging and Disruptive Technologies," *NATO Newsroom*, October 22, 2021, https://www.nato.int/cps/en/natohq/topics_184303.htm.

to meet mutual needs and increase resilience between these two organizations. There have already been significant security partnerships between NATO and the EU. One example is the European Centre of Excellence for Countering Hybrid Threats (Hybrid COE) between EU & NATO, which became operational in April 2017. Since this program's inception, both NATO and the EU staff have participated in joint workshops that addressed how hybrid threats can disrupt security.[61] Furthermore, coordination in critical infrastructure and defense capabilities of the EU and NATO will limit unnecessary duplications of infrastructure and contingencies, which will increase resilience in the Euro-Atlantic region.[62] Joint training operations between the EU and NATO, the United States and NATO, and the EU and the US—particularly those relating to hybrid warfare and emerging technologies—will foster further cooperation and increase the Alliance's counterterrorism capacity and collective security.[63]

There is an important role for NATO to play in ensuring the security of privately-owned critical infrastructure, specifically in the foreign acquisition process. Certain EU and/or NATO members have, through structural and legal loopholes, acquired infrastructure technology contracts from countries like China that may compromise critical infrastructure security. The current European Union Foreign Direct Investment (FDI) regime allows individual member states to develop their own regulations and does not have authority to block foreign acquisitions of critical infrastructure.[64] For example, Italy has given conditional approval for Huawei, a corporation with links to Chinese security services, to develop 5G infrastructure across the country[65]. As a security organization that works closely with EU regulators, NATO can provide a supervisory and coordination role for the protection of critical infrastructure that requires foreign investment.

NATO and the EU also encourage civil-military cooperation on emerging technologies to promote critical infrastructure resilience. For example, thirty-four NATO and European Union members and more than 30 private sector partners

---

[61] Sonia Krimi, *The NATO-EU Partnership in a Changing Global Context* (Brussels, BE: NATO Parliamentary Assembly, November 2020), 6, https://www.nato-pa.int/document/2020-revised-draft-report-nato-eu-partnership-changing-global-context-krimi-037-pcnp-20-e.

[62] NATO, "Brussels Summit Communiqué," *NATO Newsroom*, June 14, 2021, https://www.nato.int/cps/en/natohq/news_185000.htm.

[63] Michael Rühle and Clare Roberts, "Enlarging NATO's toolbox to counter hybrid threats," *NATO Review*, March 19, 2021, https://www.nato.int/docu/review/articles/2021/03/19/enlarging-natos-toolbox-to-counter-hybrid-threats/index.html.

[64] Sarah Erikson, "Recent Developments in EU Foreign Investment Screening," *Center for Strategic International Studies*, April 19, 2021, https://www.csis.org/blogs/strategic-technologies-blog/recent-developments-eu-foreign-investment-screening.

[65] Elvira Pollina and Giuseppe Fonte, "Italy gives Vodafone 5G deal with Huawei conditional approval – sources," *Reuters*, May 31, 2021, https://www.google.com/search?client=safari&rls=en&q=italy+huawei&ie=UTF-8&oe=UTF-8.

attended the "Interdependency in Resilience" conference in May 2017. The conference was held to "improve understanding and visibility of what resilience means across these sectors; establish knowledge transfer between key stakeholders; and develop actionable proposals to improve mutual collaborations with partner nations."[66] The 2016 Joint Declaration further promotes NATO-EU cooperation on technological resilience: "As each organization has made EDT advances, staff-level coordination and broad information sharing have helped to better align their efforts."[67] In the future, standardizing technological procedures across NATO and the EU will be essential to minimize redundancy between allies.[68]

The strategic alignment of NATO and the EU is on full display as Russia invades Ukraine. Mutual concerns about the crisis in Ukraine have prompted further unity between the two organizations, with the EU financing €500 million of emergency weapons shipments to Ukraine. This aid package is a "watershed moment" for the EU, according to European Commission President Ursula von der Leyen.[69] The EU is also responding to the crisis' humanitarian consequences by granting temporary residency to Ukrainian refugees.[70] These developments highlight the EU's complementary role in European security. The fast-tracking of Ukraine's request for EU accession indicates that Ukraine and the EU are fully aware of this role.[71]

There are, of course, still impediments to NATO-EU cooperation, including the global rise of isolationist movements.[72] Furthermore, only 55% of European citizens "totally" or "somewhat" support the creation of a "European army."[73]

---

[66] NATO SACT and City of Norfolk, *Building Resilience.*
[67] Karlijn Jans and Lauren M. Speranza, "Bridging the Gap: Time for an EU-NATO Strategic Dialogue on Defensive Tech," *University of Leiden* (blog), March 23, 2021, https://www.universiteitleiden.nl/en/wiisnl/news/2021/blog-post--bridging-the-gap-time-for-an-eu-nato-strategic-dialogue-on-defense-tech.
[68] Giovanna de Maio, "Opportunities to Deepen NATO-EU Cooperation," *Brookings Institute*, Foreign Policy at Brookings, https://www.brookings.edu/wp-content/uploads/2021/12/FP_20211203_nato_eu_cooperation_demaio.pdf.
[69] John Chalmers, "Dramatic Zelenskiy Call Prompted EU Move to Provide Arms," *Reuters*, March 2, 2022, https://www.reuters.com/world/europe/dramatic-call-with-ukraine-leader-prompted-historic-eu-move-provide-arms-2022-03-02/.
[70] Philip Blenkinsop and Gergely Szakacs, "EU Backs Move to Give Ukraine Refugees Temporary Residency," *Reuters*, March 3, 2022, https://www.reuters.com/world/europe/eu-prepares-millions-refugees-ukraine-2022-03-03/.
[71] Humeyra Pamuk, Tom Hogue, ed., and Grant McCool, ed., "EU Chief Says Bloc Wants Ukraine as Member," *Reuters*, February 27, 2022, https://www.reuters.com/world/europe/eu-chief-says-bloc-wants-ukraine-member-they-are-one-us-2022-02-28/.
[72] Tad A. Schnaufer II, "The US-NATO Relationship: The Cost of Maintaining Political Pressure on Allies," *Georgetown Journal of International Affairs* (website), January 15, 2021, https://gjia.georgetown.edu/2021/01/15/the-us-nato-relationship-the-cost-of-maintaining-political-pressure-on-allies/.
[73] Krimi, *The NATO-EU Partnership*, November 2020, 12.

Nevertheless, as the response to Russia's invasion of Ukraine shows, partnership between NATO and the EU is essential to transatlantic security and the resilience of member states' critical infrastructure.

Conclusions

NATO bears the responsibility of protecting its members against all threats. Article 3 of the North Atlantic Treaty expresses this requirement in service of the allied goal of developing "individual and collective capacity to resist armed attack."[74] In an age of interconnectedness and cross-border technologies, one ally's vulnerability is a vulnerability of the entire Alliance. Energy and communications networks rely on interwoven, often automated patchworks of infrastructure that involve private corporations, civil administration, and military support. This critical infrastructure can fail if not resilient, causing irreparable harm to NATO readiness, allied defense, and human life. By settling for a posture of deterrence rather than pursuing a posture of resilience, NATO decreases the security of its members' critical infrastructure. Deterrence, which NATO defines deterrence as the "threat of force in order to discourage" actors from harming one another, no longer adequately protects the Alliance.[75] Facing unpredictable, unanticipated, and inevitable threats, NATO can ensure the resilience of its members' critical infrastructure.

Understanding both threats to critical infrastructure and NATO's seven baseline requirements for resilience is essential to effective policymaking. NATO and its member states can work to meet the baseline requirements for resilience through persistence, by taking a holistic approach to capacity consideration, and by informing policymakers and the public of the importance of resilience. Infrastructure systems must be resilient to both external threats and inherent vulnerabilities. As the Alliance faces the impacts of climate change, future public health catastrophes, and adversaries with increased technological capabilities, prioritizing critical infrastructure resilience at the national and transnational levels is more important than ever.

It is important that a comprehensive strategy to ensure resilience promote civil-military cooperation and collaboration between member states. Civil-military cooperation is essential for research and development and operational purposes. Privatization of critical infrastructure systems without significant military involvement exposes these systems to harm due to deliberate attacks and environmental happenstance. Strong NATO partnerships will provide stability in a rapidly changing critical infrastructure environment. Intentional partnerships and

[74] NATO, "The North Atlantic Treaty," 1949, *https://doi.org/10.1177/002070204900400206.*
[75] Michael Rühle, "Deterrence: what it can (and cannot) do," *NATO Review,* April 20, 2015, https://www.nato.int/docu/review/articles/2015/04/20/deterrence-what-it-can-and-cannot-do/.

coordinated cybersecurity projects will demonstrate the Alliance's strength to a global audience. Existing NATO-EU partnerships, particularly those that weave civil-military cooperation and emerging technologies, exemplify the cross-disciplinary partnerships of the future. The NATO-EU relationship also shows the fragility of security partnerships in the face of domestic politics.

Ensuring the resilience of NATO member states is vital to the success of NATO missions and the integrity of the Alliance itself. Without resilience, the Alliance and its member states' critical infrastructure systems are vulnerable to various threats, including terrorist attacks, hybrid attacks, asymmetrical warfare, and even CBRN strikes. While technological innovation and compounding infrastructure interdependencies heighten the risks of cascading effects, the systems that provide resilience against these threats are becoming obsolete. If NATO does not create new defenses, it will be possible for a NATO adversary, whether a terrorist organization or a nation-state, to strike a single decisive blow. Therefore, NATO and its member states can work together to strengthen their collective resilience against known and emerging threats, building a future that provides robust security for the transatlantic region.

Selected Bibliography

Anderson, Chris. “National Infrastructure Coordinating Center INSight Application.” *U.S. Department of Homeland Security*, November 23, 2007. https://www.dhs.gov/sites/default/files/publications/privacy_pia_nppd_nicc.pdf.

Ayers, Cynthia, and Kenneth Chrosniak. *Terminal Blackout: Critical Electric Infrastructure Vulnerabilities and Civil-Military Resiliency.* Carlisle, PA: US Army War College, Center for Strategic Leadership and Development. https://publications.armywarcollege.edu/pubs/2983.pdf.

Beckvard, Henrik, and Philippe Zotz. *Cyber Considerations for Military Mobility.* Estonia, Tallinn: NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2021/05/Releasable_Cyber-Considerations-for-Military-Mobility_Beckvard_Zotz.pdf.

Beehler, Alex, and Surash, J.E. “Cutting the Cord to Test Energy Resilience.” US Army, April 12, 2020. https://www.army.mil/article/234514/cutting_the_cord_to_test_energy_resilience.

Camp, Kevin M., David Mead, Stephen B. Reed, Christopher Sitter, and Derek Wasilewski. “From the Barrel to the Pump: The Impact of the COVID-19 Pandemic on Prices for Petroleum Products.” *Monthly Labor Review*, US Bureau of Labor Statistics, October 2020. https://doi.org/10.21916/mlr.2020.24.

de Jong, Moiek, and Thijs Van de Graaf. “Lost in Regulation: Nord Stream 2 and the Limits of the European Commission's Geo-Economic Power.” *Journal of European Integration* 43, no. 4 (August 6): 495-510. https://doi.org/10.1080/07036337.2020.1800680.

de Maio, Giovanna. “Opportunities to Deepen NATO-EU Cooperation.” *Brookings Institute*, Foreign Policy at Brookings. https://www.brookings.edu/wp-content/uploads/2021/12/FP_20211203_nato_eu_cooperation_demaio.pdf.

Erikson, Sarah. “Recent Developments in EU Foreign Investment Screening.” *Center for Strategic International Studies,* April 19, 2021, https://www.csis.org/blogs/strategic-technologies-blog/recent-developments-eu-foreign-investment-screening.

Foy, Kylie. “Improving Resiliency in Military Systems Will Require Organizational and Cultural Shifts.” MIT Lincoln Laboratory, November 6, 2019. https://www.ll.mit.edu/news/improving-resiliency-military-systems-will-require-organizational-and-cultural-shifts.

Gohel, Sajjan, and Peter Forster. *Counter-Terrorism Reference Curriculum*. NATO Defence Education Enhancement Programme, 2020.

Hodicky, Jan, Gökhan Özhan, Hilmi Özdemir, Petr Stodola, Jan Drozd, and Wayne Buck. "Dynamic Modeling for Resilience Measurement: NATO Resilience Decision Support Model." *Applied Sciences* 10, no. 8 (2020): 2639. https://doi.org/10.3390/app10082639.

Humphreys, Brian E. *Critical Infrastructure: Emerging Trends and Policy Considerations for Congress*. Congressional Research Service (CRS) Report R45809. Washington, DC: CRS, July 8, 2019. https://www.everycrsreport.com/reports/R45809.html.

Jans, Karlijn, and Lauren M. Speranza. “Bridging the Gap: Time for an EU-NATO Strategic Dialogue on Defensive Tech.” *University of Leiden* (blog), March 23, 2021, https://www.universiteitleiden.nl/en/wiisnl/news/2021/blog-post--bridging-the-gap-time-for-an-eu-nato-strategic-dialogue-on-defense-tech.

Krimi, Sonia. *The NATO-EU Partnership in a Changing Global Context*. Brussels, BE: NATO Parliamentary Assembly, November 2020. https://www.nato-pa.int/document/2020-revised-draft-report-nato-eu-partnership-changing-global-context-krimi-037-pcnp-20-e.

Johns Hopkins University & Imperial College London. “Countering Cognitive Warfare: Awareness and Resilience.” *NATO Review*, May 20, 2021. https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html.

Johns Hopkins University, Imperial College London, and Georgia Institute of Technology. “Countering Disinformation: Improving the Alliance’s

Digital Resilience." *NATO Review*, August 12, 2021. https://www.nato.int/docu/review/articles/2021/08/12/countering-disinformation-improving-the-alliances-digital-resilience/index.html.

NATO. *Infrastructure Assessment*, ACO Directive 084-002. October 17, 2019.

NATO. "Civil Preparedness." *NATO Newsroom*, March 23, 2021. https://www.nato.int/cps/en/natohq/topics_49158.htm.

NATO. "Countering Terrorism." *NATO Newsroom*, September 14, 2021, https://www.nato.int/cps/en/natohq/topics_77646.htm.

NATO. "Emerging and Disruptive Technologies." *NATO Newsroom*. October 22, 2021, https://www.nato.int/cps/en/natohq/topics_184303.htm.

NATO. "Energy Security." *NATO Newsroom*, September 28, 2021. https://www.nato.int/cps/en/natohq/topics_49208.htm.

NATO. "Military Medical Support." *NATO Newsroom*, June 30, 2021. https://www.nato.int/cps/en/natohq/topics_49168.htm.

NATO. "Resilience and Article 3." *NATO Newsroom*, June 11, 2021. https://www.nato.int/cps/en/natohq/topics_132722.htm.

NATO Supreme Allied Command Transformation (SACT) and City of Norfolk. *Building Resilience – Collaborative Proposals to Help Nations and Partners*. Norfolk, VA: June 2017. https://www.act.nato.int/images/stories/events/2017/resilience/resilience-wp.pdf.

Pollina, Elvira and Fonte, Giuseppe. "Italy gives Vodafone 5G deal with Huawei conditional approval – sources." *Reuters*, May 31, 2021, https://www.google.com/search?client=safari&rls=en&q=italy+huawei&ie=UTF-8&oe=UTF-8.

Reding, D.F., and J. Eaton. *Science & Technology Trends 2020-2040.* Brussels, BE: NATO Science & Technology Organization, March 2020.

Rühle, Michael, and Clare Roberts. "Enlarging NATO's toolbox to counter hybrid threats," *NATO Review*.

https://www.nato.int/docu/review/articles/2021/03/19/enlarging-natos-toolbox-to-counter-hybrid-threats/index.html.

Samaras, Constantine, William J. Nuttal, and Morgan Bazilian. “Energy and the Military: Convergence of Security, Economic, and Environmental Decision-Making.” *Energy Strategy Reviews*, no. 26, (November 2019): 8. https://doi.org/10.1016/j.esr.2019.100409.

Shea, Jamie. “Resilience: A Core Element of Collective Defence.” *NATO Review,* March 30, 2016. https://www.nato.int/docu/review/articles/2016/03/30/resilience-a-core-element-of-collective-defence/index.html.

US Cybersecurity and Infrastructure Security Agency (CISA). “A Guide to Critical Infrastructure Security and Resilience.” November 2019. https://www.cisa.gov/sites/default/files/publications/Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf.

US Cybersecurity and Infrastructure Security Agency (CISA). “Critical Infrastructure Vulnerability Assessments.” Accessed January 20, 2022. https://www.cisa.gov/critical-infrastructure-vulnerability-assessments.

US National Counterintelligence and Security Center. “Insider Threat Mitigation for US Critical Infrastructure Entities: Guidelines from an Intelligence Perspective.” March 2021. https://www.dni.gov/files/NCSC/documents/news/20210319-Insider-Threat-Mitigation-for-US-Critical-Infrastru-March-2021.pdf.

Wilson, Clay. *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*. Congressional Research Service (CRS) Report RL32115. Washington, DC: CRS, January 29, 2008. https://www.everycrsreport.com/reports/RL32114.html.

Chapter 2: Big Data and Advanced Analytics

By: Trevor Helmy, Katherine Lin, Samantha Mabe, and Alex Olsen

Big data and advanced analytics can improve NATO's offensive capabilities and resilience and its member states. This chapter first describes the foundational roles and emerging applications of these technologies. Next, the chapter uses a case study of Germany's pandemic response to discuss the role of big data and advanced analytics in improving operational capacity and protecting critical infrastructure. This study also demonstrates that data anonymization and clearly defined restrictions to data access are crucial to maintaining public acceptance of these programs. The chapter also explores the role of big data-adjacent technologies in 5G development, the Russian invasion of Ukraine, and the United States' surveillance programs. This chapter concludes by recommending that NATO use its Communications and Information Agency to support member states' national big data capabilities data sets without sacrificing interoperability.

Technological opportunities

Big data refers to data with significant volume, velocity, variety, veracity, or visualization challenges.[1] The term covers information collected from human (social media, bioinformatics, etc.), physical (sensors), and information (cyber, analysis, etc.) domains.[2] It is an outgrowth of increased digitalization, the proliferation of new sensors, the rise of the internet of things, and socio-cognitive virtualization. The emergence of big data naturally creates a need to make sense of massive data sets through advanced analytic methods.

Big data and advanced analytics provide significant opportunities to policymakers. Advanced analysis of the vast quantities of data available across physical, human, and information battlespaces can provide critical insights, improve predictions, and support real-time decisions. By utilizing big data, NATO can make critical infrastructure more resilient against all types of hazards, including terrorist attacks. Predictions become more accurate with higher quantities of data, thereby helping avoid disasters or minimizing their impact. By combining national databases, NATO members can also collaborate on big data and advanced analytics to track the movements of suspicious figures and trace terrorist operations across borders.[3] Decision-makers who can leverage emerging technologies to view

[1] D.F. Reding and J. Eaton, *Science & Technology Trends 2020-2040* (Brussels, BE: NATO Science & Technology Organization, March 2020), 41.
[2] Reding and Eaton, *Science & Technology Trends*, 42.
[3] David Kohlbrenner (computer science professor, University of Washington), interview with author, January 13, 2022.

battlespaces with greater fidelity and from broader perspectives will better estimate the impacts of their decisions in the next stage of human warfare.

These technologies also present NATO with new ways to respond to terrorist attacks and infrastructure failures. By 2030, NATO will be able to use digital twins—virtual simulations reconstructed through data collected from their real-life counterparts—to improve its logistical efficiency when responding to traditional infrastructure failures. Data partnerships between member states can build larger data sets, improving these simulations' fidelity and predictive value.[4] With its 2020 law enforcement data-sharing plan to aid the prosecution of terrorists, NATO is already using big data to support retributive responses to terrorist attacks.[5] Big data and advanced analytics capabilities will be essential in informing NATO's initial decision to respond to an emerging crisis. The North Atlantic Council's role in determining whether to respond to a crisis already relies on integrating intelligence and data.[6]

In conjunction with improving defense and mission capacities, NATO can also use big data and advanced analytics preventatively by supporting the resilience of critical infrastructure. Situational awareness is vital in crafting swift and informed responses to crises such as natural disasters and pandemics. In the case of the COVID-19 pandemic, consistent data streams are integral in protecting critical infrastructure systems, such as hospitals and health agencies, and preventing them from becoming overwhelmed. Further, controlling COVID-19 outbreaks and preventing spikes in infection rates is necessary to prevent a shutdown of the economy and portions of the supply chain, which has far-reaching consequences for all critical infrastructure sectors.

Big data is a foundational technology for all other emerging technologies, particularly artificial intelligence (AI). Artificial intelligence relies on big data to train powerful analytics systems to inform decision-making. Once sufficiently developed, AI will draw on big data systems to interpret real-time situations.[7] These big data and AI systems can also be integrated into autonomous drone, hypersonic, and space technologies. When combined with artificial intelligence, drones with big data capacities will enable more accurate understandings of real-time battlespaces. This will allow for more effective operations, minimizing the risk to human life and resources.[8] Big data technologies can also support weapons systems, potentially increasing the precision of hypersonic weapons through advanced

---

[4] Reding and Eaton, *Science & Technology Trends*, 46.
[5] NATO, "Countering Terrorism," September 14, 2021, *NATO Newsroom*, https://www.nato.int/cps/en/natohq/topics_77646.htm.
[6] NATO, "Crisis Management," *NATO Newsroom*, October 8, 2020, https://www.nato.int/cps/en/natohq/topics_49192.htm.
[7] Reding and Eaton, *Science & Technology Trends*, 52.
[8] Reding and Eaton, *Science & Technology Trends*, 60.

visualization systems.[9] In space, big data systems will be necessary to understand the new frontier and ensure the security of critical satellite infrastructure.[10]

As a foundational technology, big data capacities are crucial for the construction of resilient critical infrastructure and the execution of effective security missions. For example, in security sector reform initiatives, the interoperability of national military datasets can improve capacity-building efforts by minimizing redundancies, improving logistical efficiency, and ensuring mutual understanding between host countries and donors.[11] In any counterterrorism effort, nation-states can employ big data and advanced analytics to track and evaluate counterterrorism measures in more granular detail than has been previously possible.[12] Within the next ten years, NATO will be able to capitalize on synergies between social media and ubiquitous sensors to detect and prevent terrorist attacks before they occur.[13] Any investments in systems to effectively respond to terrorist attacks will also be advantageous in the event of natural disasters, pandemics, or other critical infrastructure failures.

Where big data is being used

Germany's direct participation in NATO's information networks makes a case study of Germany's big data efforts especially useful. Germany contributes to the NATO Communications and Information Agency (NCI Agency) and is an original member of the related CS3 Partnership. These institutions exist to support the individual development of data and intelligence systems within NATO member states, support interoperability, aid missions by bridging informational gaps, and promote cybersecurity of information systems.[14] Ramstein, Germany, hosts one of the NCI Agency's communications and information systems support units. The state itself has received intelligence from the NCI Agency that has assisted disaster response and missions planning. In July 2021, after flash floods, the NCI Agency provided relief using geospatial intelligence to generate real-time data streams that

[9] Reding and Eaton, *Science & Technology Trends*, 92.
[10] Reding and Eaton, *Science & Technology Trends*, 81.
[11] Sajjan Gohel and Peter Forster, *Counter-Terrorism Reference Curriculum* (NATO Defence Education Enhancement Programme, 2020), 119-121.
[12] Gohel and Forster, *Counter-Terrorism Reference Curriculum*, 120-123.
[13] Reding and Eaton, *Science & Technology Trends*, 46.
[14]NATO, "NATO Communications and Information Agency (NCI Agency)," *NATO Newsroom*, September 15, 2021, https://www.nato.int/cps/en/natohq/topics_69332.htm.; NATO Communications and Information Agency, "CIS3 Partnership for CIS Security Standards Development," accessed February 24, 2022, https://www.ncia.nato.int/what-we-do/cyber-security/cis3-partnership-for-cis-security-standards-development.html.

would allow for informed disaster response and rescue efforts.[15] The NCI Agency also aided a German navy climate trial in early 2020 by supplementing Germany's national satellite communications capabilities.[16]

Epidemiological tracking during the COVID-19 pandemic is the most prominent example of governmental big data and advanced analytics projects. A case study of Germany's pandemic response provides valuable insight into the logistics of large-scale data. Germany, a key NATO member, launched a swift initial response to the virus, and the country has maintained a strict COVID-19 tracking and monitoring system for over two years. Germany's program is particularly instructive due to its high data privacy standards and its legacy of surveillance. This legacy has impacted the German public's willingness to allow the government access to its data, complicating the pandemic tracking project.

Germany's ability to use big data analytics to contract trace COVID-19 exposure shows the rapid development in the ability to use cell phone data to protect the public in a public health emergency. As manual contact tracing, sequencing, and isolation regimes collapsed due to exploding case numbers, Germany created a mobile application to track and trace those who are infected and notify people of exposure. The app collects anonymous data using Bluetooth, informing users when they cross paths with someone who has tested positive for the virus. While this is not the first case of a country using an app to track and trace infections (Austria, Spain, Belgium, the United Kingdom, and outside of Europe, South Korea and Israel all created similar apps), Germany is unique in its views with data privacy.[17]

Germany's cultural attitude towards data protection prevented the creation of a centralized system for their COVID-19 infection app data, which would have allowed the government to access personal contacts and personal information saved on the device. This centralized system was the original plan for the app; however, the app was adapted to an anonymous system after data protection groups heavily protested the app's creation and use.[18] This case study illuminates how NATO

[15]NATO Communications and Information Agency, "NCI Agency Volunteers Provide Critical Support Following Devastating Floods," July 29, 2021, https://www.ncia.nato.int/about-us/newsroom/nci-agency-volunteers-provide-critical-support-following-devastating-floods.html.
[16]NATO Communications and Information Agency, "NATO Agency Delivers Satellite Coverage During German Test Campaign in the Caribbean," May 26, 2020, https://www.ncia.nato.int/about-us/newsroom/nato-agency-delivers-satellite-coverage-during-german-test-campaign-in-the-caribbean.html.
[17] Catherine Stupp, "Europe Tracks Residents' Phones for Coronavirus Research," *Wall Street Journal*, Mar 27, 2020, https://www.proquest.com/newspapers/europe-tracks-residents-phones-coronavirus/docview/2383478175/se-2?accountid=14784.
[18] Arne Bloomberg and Sarah Syed, "Germany Rolls Out Coronavirus-Tracing App to Prevent Second Wave," *Toronto Star*, June 17, 2020, https://www.proquest.com/newspapers/germany-rolls-out-coronavirus-tracing-app-prevent/docview/2413882927/se-2?accountid=14784.

member state governments can safely collect relevant data without compromising the data privacy of its citizens.

However, despite the benefits of tracking and tracing COVID-19 infections, the latest German tracking application has unveiled new security vulnerabilities. A security flaw in how restaurants and bars stored their contact tracing data left more than 4 million entries exposed on cloud software. Eighty-seven thousand of these entries were later found freely available online because of the security flaw, including politicians' emails and postal addresses.[19] New decryption technologies present another security vulnerability in big data-powered systems. While the data in the German Corona-Warn-App is supposedly anonymized, new decryption technology could make the information easily identifiable. This creates a risk that personal data could be easily hacked. This case study provides important lessons for the future of data analysis in both civil and military intelligence collection applications.

Despite its operational success, the COVID-19 tracking app in Germany has been controversial, with significant implications for future uses of big data for counterterrorism operations. Early opponents of the program warned against the collection of personal identifying information. Owing to the legacy of Stasi surveillance in East Germany, data privacy is highly regulated in modern Germany, and the German public is skeptical of state surveillance. The initial public hesitancy to accept pandemic-related big data projects suggests that similar counterterrorism programs could meet public resistance even if well-explained to the public.

German law, with its rigorous data privacy standards, regulates the security of personal data.[20] The adverse reaction of the German public, despite the legal frameworks in place, show room for improvement in data privacy standards across the EU and NATO partner nations. Like the proposed role in cybersecurity standardization, NATO can play an important role in implementing both data privacy standards through legislative coordination with the EU and facilitating data sharing and best practices. NATO currently has the infrastructure in place to assist this process through the coordination power of the NCI Agency. In the particular case of public health crises, the NATO Center of Excellence for Military Medicine (MILMED COE) assists with interoperability, lessons learned and innovation, and training.[21]

Researchers across the globe have also turned to Wastewater Based Epidemiology (WBE) as an "early warning system." At least 1,488 wastewater monitoring sites worldwide monitor sewage systems for SARS-Cov-2 RNA, which

---

[19] *Asia News Monitor,* "Germany: Coronavirus Contact Data."
[20] "Germany: Luca App Makes Contact Tracing Easier," *DW News,* April 4, 2021, video, https://p.dw.com/p/3rU24.
[21] *NATO-Accredited Centers of Excellence, "*2022 Catalogue", https://www.coemed.org/files/COE%20Catelogue%202022%20LR.pdf.

allow for anonymized data collection. These WBE systems are nationalized in Finland, Hungary, Luxembourg, Netherlands, Spain, and Turkey. The United States and Canada also oversee national WBE networks, and there are regional programs in parts of Australia, Brazil, France, South Africa, Switzerland, and the United Kingdom. Data from these regional programs are not well-linked, limiting the utility of these wastewater sensors for public health policymakers.[22] This limitation reflects the broader interoperability challenges that threaten all big data programs in international policymaking.

Germany's experience with the COVID-19 testing apps provides important lessons to consider when governments broaden their data collection capabilities in domestic settings. First, states and intergovernmental organizations should consider privacy and the ethics of collecting and storing personal data. This would both protect the rights of individuals and foster trust in governments and organizations. Second, organizations should prioritize the ease of use of data systems. NATO should carefully balance these priorities when designing standards for big data and supporting data partnerships between member states.

Current events and big data

Recent events, including contested elections, 5G development in NATO member states, and the Russian invasion of Ukraine, are impacting the adoption of big data and revealing new applications of this emerging technology.

The improved responsiveness and transfer speeds of 5G technology promise to enhance civilian and military communication. 5G technology will enable larger data streams and faster movement of data, which will be vital in developing big data and advanced analytics systems. To date, only Chinese companies offer this technology cheaply. This creates a predicament for countries who want the benefits of 5G but are worried about possible espionage. While there have been no confirmed cases of espionage from Huawei, a dominant Chinese 5G infrastructure supplier, its staff members have been linked to espionage. Huawei built Security Assessment Centers in the United Kingdom, Germany, and Belgium in response to these allegations. Many countries, including the United States, the Czech Republic, Australia, and Japan, have nevertheless issued strict restrictions on companies with close ties to foreign governments, including Huawei.[23] This intersection of security and development concerns threatens the equitable adoption of big data and

[22] Colleen Naughton et al., "Show us the Data: Global COVID-19 Wastewater Monitoring Efforts, Equity, and Gaps," *MedRxiv* (preprint, last modified March 14, 2021), https://doi.org/10.1101/2021.03.14.21253564.

[23] Kadri Kaska et al., *Huawei, 5G, and China as a Security Threat*. (Tallinn, EE: NATO Cooperative Cyber Defence Centre of Excellence, 2019), 4-21, https://ccdcoe.org/library/publications/huawei-5g-and-china-as-a-security-threat/.

advanced analytics. NATO member states with varying 5G capabilities will face additional hurdles to complete data interoperability.

Satellite imagery, a big data-adjacent technology, is playing a critical role in the Russian invasion of Ukraine. Western states and companies captured and publicized extensive satellite imagery of Russian military buildups around Ukraine in the lead-up to the invasion.[24] These images, which provide both military intelligence and diplomatic leverage, were products of the same ubiquitous sensors that will be critical as big data reaches maturity. The crisis in Ukraine demonstrates the utility of such sensors in modern military and hybrid conflicts. Cybersecurity systems, another group of technologies relevant to big data, are also central to the conflict. By hacking government sites and broadcasting claims that Ukrainians' personal data would be publicized, Russia at once stressed the strategic importance of cybersecurity and displayed its willingness to exploit the public's desire for privacy.[25] Given the possibility that these cyberattacks will soften public resistance to a Russian invasion, these attacks and disinformation campaigns also highlight the political risks of interconnected data systems.

Past privacy controversies have also impacted the development of big data. In 2014, Cambridge Analytica, a firm that combined big data with psychographic profiling to create targeted advertisements, gained access to the private data of as many as 87 million Facebook users.[26] They used this information to aid the campaigns of US presidential candidates Ted Cruz and Donald Trump.[27] Similarly, in 2016, Cambridge Analytica used its farmed data to support the "Vote Leave" and related "BeLeave" Brexit campaigns.[28] News of these projects triggered swift public and political backlash. The US Congress called Facebook CEO Mark Zuckerberg to testify on Facebook's mishandling of personal data, users deleted their Facebook profiles, and Facebook throttled the amount of data that third-party firms can access.[29] The situation with Cambridge Analytica complicated the future

[24] Christoph Koetl, "New Satellite Images Show More Russian Forces Massing on Three Sides of Ukraine," *New York Times*, February 10, 2022, https://www.nytimes.com/2022/02/10/world/europe/russia-ukraine-forces.html?smid=url-share.
[25] Pavel Polityuk and Steve Holland, "Cyberattck Hits Ukraine as US Warns Russia Could be Preparing for War," *Reuters*, January 14, 2022, https://www.reuters.com/world/europe/expect-worst-ukraine-hit-by-cyberattack-russia-moves-more-troops-2022-01-14/.
[26] Nicholas Confessore, "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far," *New York Times*, April 4, 2018, https://nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.
[27] Nicholas Confessore and Danny Hakim, "Data Firm Says 'Secret Sauce' Aided Trump; Many Scoff," *New York Times*, March 6, 2017, https://www.nytimes.com/2017/03/06/us/politics/cambridge-analytica.html.
[28] David D. Kirkpatrick, "Using Digital Firm, Brexit Campaigners Skirted Spending Laws, Ex-Employee Says," *New York Times*, March 24, 2018, https://www.nytimes.com/2018/03/24/world/europe/uk-brexit-vote-leave-shahmir-sanni.html.
[29] Confessore, "Cambridge Analytica and Facebook."

of big data and advanced analytics because users who realized data could be exploited became suspicious of the technology.

The mixed reactions to state surveillance systems suggest that individuals have less reason to oppose big data programs when their personal data is not at risk. Big data and advanced analytics are therefore not necessarily unpopular when they track impersonal data. NATO could employ advanced analytics to inform logistics or aggregate massive amounts of satellite imagery without triggering public opposition. By contrast, counterterrorism programs that compile personal identifying information are likely to face legal and political backlash. NATO and its member states both currently take note of overreaching big data projects and recognize that a harmful perception of NATO counterterrorism programs can undermine the legitimacy of the Alliance.

Conclusions

The rise of big data and advanced analytics offers incredible promise and exposes new vulnerabilities. As such, we recommend NATO promote the development and integration of big data in civil and military spheres to reap its benefits and outpace potential adversaries. Big data technologies foster resilience by tracking terrorist operations, monitoring public health crises, and providing situational awareness on the battlefield far surpassing human capacities. Most importantly, big data technology is foundational for all facets of future warfare. It provides the basis for artificial intelligence, which in turn will allow NATO to fully take advantage of drones, hypersonics, space technologies, and quantum computing.[30] Each of these technologies is within reach or is already being deployed by NATO member states and potential adversaries. By developing big data and advanced analytics and integrating them into its operations, NATO could establish a significant advantage over potential adversaries and build resilience against today's environmental threats.

The German government's big data-powered COVID-19 responses, the crisis in Ukraine, and counterterrorism surveillance controversies reveal limitations NATO can consider when crafting big data systems. To maintain citizens' privacy and trust in government, it is important that designers of NATO big data operations rely on anonymized data, assuaging fears of surveillance. Furthermore, it is of high importance that collected data be protected by high cybersecurity standards to ensure private information remains private. Third, policymakers can firmly and transparently restrict access to data collected from the public while strictly adhering to the program's original intentions. Finally, and most critically, NATO can

[30] Reding and Eaton, *Science & Technology Trends*, 41-52.

account for the diversity of privacy cultures and regulations among its member states.

These baseline standards will promote public tolerance of data collection for security purposes. As NATO adversaries develop advanced analytic capabilities of their own, NATO will need to integrate big data technologies into its decision-making processes to maintain a competitive edge. The need to leverage big data for decision-making will only increase as technology advances, and NATO member states will need the public's trust to fully exploit big data and advanced analytics to protect critical infrastructure. A set of ethical big data standards based on the lessons of past surveillance systems is a crucial first step towards this goal.

Policy recommendations

We recommend that NATO prioritize the security and integrity of national products in all NATO counterterrorism big data efforts. NATO can coordinate the sharing of important counterterrorism data analytics without maintaining alliance-wide data sets where shared access could create greater vulnerabilities. The cross-border maintenance of big data systems without common standards of security leaves the entire alliance vulnerable to a single failure point. Technology developed by individual member states can be used securely to NATO's advantage without sacrificing interoperability.

Such redirected efforts may resemble the United Kingdom's counterterrorism strategy (CONTEST), which in its 2018 revision emphasized increased investment in biometric data collection systems and the development of analysis programs to identify and track the movement of suspicious figures more accurately.[31] Although CONTEST includes some opportunities for international partnerships, the strategy emphasizes expanding the UK's own data collection and analysis.[32] Developed as a domestic policy, CONTEST adheres to EU data privacy restrictions. It is well-adapted to work in the intersections between the UK's police system, military, security agencies, and private tech sector and has been largely successful.[33]

Developing big data-powered counterterrorism systems at the domestic level circumvents many challenges NATO currently faces in adopting big data technology. As discussed above, differing legal and technical requirements across member states present security vulnerabilities and hinder the development of Alliance-wide big data systems. Furthermore, differing societal structures and cultural relationships with technology make it difficult for such a program to meet

[31] UK Secretary of State for the Home Department (SSHD), *CONTEST: The United Kingdom's Strategy for Countering Terrorism*, CM 9068 (London: Crown, June 2, 2018), 11.
[32] UK SSHD, *CONTEST*, 80.
[33] UK SSHD, *CONTEST*, 9.

the demands of all member states. Many of these issues would be made irrelevant by deemphasizing the need for singular data sets across member states. Member states could develop systems uniquely tailored to their specific needs.

This greater emphasis on individualized technological development would not compromise NATO's resilience. Instead, this change in posture would catalyze the development of these national systems, allowing member states to improve their own security expediently. Due to the interconnections of national critical infrastructure systems, this individualized, accelerated development and integration would improve the security of the whole Alliance against terrorist activities and natural disasters. Most importantly, locally developed big data-powered counterterrorism systems would not be limited by the lowest common denominator of another state's privacy or security standards. This is not a call to actively discourage cooperation or move away from interoperability, but an acknowledgment that such endeavors conflict with the Alliance's current priorities.

Furthermore, we recommend *NATO add a big data expert to its Communications and Information Agency (NCI).* This agency is tasked with providing information systems to and protecting the cybersecurity of NATO missions and member states.[34] As the NCI is a hub for education, training, cybersecurity, and innovation, the NCI needs a big data expert who can make the best recommendations for protecting big data.[35] Counterterrorism measures, for example, rely on hackable big data systems, creating a target for both state and non-state adversaries.[36] We understand that intelligence-sharing networks such as INTERPOL and the Five Eyes already have similar experts in place, but we still find it important to recommend adding additional expertise to the NCI. NATO and the NCI can mitigate the effects of these hacks through training, as human error is one of the largest sources of cyber vulnerabilities.[37] The NCI already handles cybersecurity training, and by adding a big data expert, NATO would fine-tune this training to the specific needs of this foundational technology. Coupled with a flexible NATO posture on big data sharing, this improvement to the NCI would significantly improve the resilience of NATO's big data systems and critical infrastructure.

---

[34] NATO Communications and Information Agency, "NATO's Cyber Security Centre," NATO, https://www.ncia.nato.int/what-we-do/cyber-security.html.
[35] NATO, "NCI Agency."
[36] Henrik Beckvard et al, *Recent Cyber Events: Considerations for Military and National Security Decision Makers*, (Tallinn, EE: NATO Cooperative Cyber Defence Centre of Excellence, 2021), 2-4, https://ccdcoe.org/uploads/2021/09/Report_The_Global_Threat_A4-1.pdf.
[37] NATO Supreme Allied Command Transformation (SACT) and City of Norfolk, *Building Resilience – Collaborative Proposals to Help Nations and Partners* (Norfolk, VA: June 2017), 2, https://www.act.nato.int/images/stories/events/2017/resilience/resilience-wp.pdf.

Selected Bibliography

Beckvard, Henrik, Sungbaek Cho, Amy Ertan, Ben Valk, Ann Väljataga, and Jan Wünsche. *Recent Cyber Events: Considerations for Military and National Security Decision Makers.* Tallinn, EE: NATO Cooperative Cyber Defence Centre of Excellence, 2021. https://ccdcoe.org/uploads/2021/09/Report_The_Global_Threat_A4-1.pdf.

Böehmer, Merle M., Udo Buchholz, Victor Corman, Martin Hoch, Katharina Katz, Durdica Marosevic, Stefanie Böhm et al. "Investigation of a COVID-19 Outbreak in Germany Resulting from a Singe Travel-Associated Primary Case: A Case Series." *The Lancet: Infectious Diseases* 20, no. 8 (May 2020): 920–928. https://doi.org/10.1016/S1473-3099(20)30314-5.

Gohel, Sajjan, and Peter Forster. *Counter-Terrorism Reference Curriculum*. NATO Defence Education Enhancement Programme, 2020.

Kaska, Kadra, and Lorena Trinberg. *Regulating Cross-Border Dependencies on Critical Information Infrastructure.* Tallinn, EE: NATO Cooperative Cyber Defence Centre of Excellence, 2015. https://ccdcoe.org/library/publications/regulating-cross-border-dependencies-of-critical-information-infrastructure/.

Kaska, Kadri, Henrik Beckvard, and Tomáš Minárik. *Huawei, 5G, and China as a Security Threat*. Tallinn, EE: NATO Cooperative Cyber Defence Centre of Excellence, 2019. https://ccdcoe.org/library/publications/huawei-5g-and-china-as-a-security-threat/.

Koetl, Christoph. "New Satellite Images Show More Russian Forces Massing on Three Sides of Ukraine." *New York Times*, February 10, 2022. https://www.nytimes.com/2022/02/10/world/europe/russia-ukraine-forces.html?smid=url-share.

Lewandowsky, Stephan, Simon Dennis, Andrew Perfors, Yoshihisa Kashima, Joshua White, Paul Garrett, Daniel Little, and Muhsin Yesilada. "Public Acceptance of Privacy-Encroaching Policies to Address the COVID-19 pandemic in the United Kingdom." *PLOS One* 16, no. 1 (January 22, 2021). https://doi.org/10.1371/journal.pone.0245740.

Murariu, Madalina. *Data Sharing Between the United States and the European Union.* Cambride, MA: Harvard Kennedy School Belfer Center, July 2021. https://www.belfercenter.org/sites/default/files/2021-07/DataSharingUSEU.pdf.

NATO-Accredited Centers of Excellence, *"*2022 Catalogue", https://www.coemed.org/files/COE%20Catelogue.

NATO. "Countering Terrorism." *NATO Newsroom*, September 14, 2021. https://www.nato.int/cps/en/natohq/topics_77646.htm.

NATO. "Crisis Management." *NATO Newsroom*, October 8, 2020. https://www.nato.int/cps/en/natohq/topics_49192.htm.

NATO. "NATO Communications and Information Agency (NCI Agency)." *NATO Newsroom*, September 15, 2021. https://www.nato.int/cps/en/natohq/topics_69332.htm.

NATO Communications and Information Agency. "CIS3 Partnership for CIS Security Standards Development." Accessed February 24, 2022. https://www.ncia.nato.int/what-we-do/cyber-security/cis3-partnership-for-cis-security-standards-development.html.

NATO Communications and Information Agency. "NATO Agency Delivers Satellite Coverage During German Test Campaign in the Caribbean." May 26, 2020, https://www.ncia.nato.int/about-us/newsroom/nato-agency-delivers-satellite-coverage-during-german-test-campaign-in-the-caribbean.html.

NATO Communications and Information Agency. "NATO's Cyber Security Centre." https://www.ncia.nato.int/what-we-do/cyber-security.html.

NATO Communications and Information Agency. "NCI Agency Volunteers Provide Critical Support Following Devastating Floods." July 29, 2021. https://www.ncia.nato.int/about-us/newsroom/nci-agency-volunteers-provide-critical-support-following-devastating-floods.html.

NATO Supreme Allied Command Transformation (SACT) and City of Norfolk. *Building Resilience – Collaborative Proposals to Help Nations and Partners*. Norfolk, VA: June 2017.

https://www.act.nato.int/images/stories/events/2017/resilience/resilience-wp.pdf.

Naughton, Colleen, Fernando Roman Jr., Ana Grace Alvarado, Arianna Tariqi, Matthew Deeming, Kyle Bibby, Aaron Bivins, Joan Rose, Gertjan Medema, Warish Ahmed, Panagis Katsivelis, Vajra Allan, Ryan Sinclair, Yihan Zhang, and Maureen Kinyua. "Show us the Data: Global COVID-19 Wastewater Monitoring Efforts, Equity, and Gaps." *MedRxiv* (preprint), last modified March 14, 2021. https://doi.org/10.1101/2021.03.14.21253564.

Pavel Polityuk and Steve Holland, "Cyberattck Hits Ukraine as US Warns Russia Could be Preparing for War," *Reuters*, January 14, 2022, https://www.reuters.com/world/europe/expect-worst-ukraine-hit-by-cyberattack-russia-moves-more-troops-2022-01-14/.

Reding, D.F., and J. Eaton. *Science & Technology Trends 2020-2040*. Brussels, BE: NATO Science & Technology Organization, March 2020.

Schulze, Matthias. "Patterns of Surveillance Legitimization: The German Discourse on the NSA Scandal." *Surveillance & Society* 13, no. 2 (2015). https://doi.org/10.24908/ss.v13i2.5296.

UK Secretary of State for the Home Department (SSHD), *CONTEST: The United Kingdom's Strategy for Countering Terrorism*, CM 9068 (London: Crown, June 2, 2018), 11.

USA FREEDOM Reauthorization Act of 2020, H.R. 6172 (2020), S2397. https://www.congress.gov/congressional-record/2020/05/13/senate-section/article/S2388-2.

Wieler, Lothar, Ute Rexroth, and René Gottschalk. "Emerging COVID-19 Success Story: Germany's Push to Maintain Progress." *Our World in Data*, March 20, 2021. https://ourworldindata.org/covid-exemplar-germany?country=.

Zastrow, Mark. "South Korea is Reporting Intimate Details of COVID-19 Cases: Has it Helped?" *Nature*, March 18, 2020. https://www.nature.com/articles/d41586-020-00740-y.

Chapter 3: Artificial Intelligence

By: Edreese Khosraw, Christopher Ryals, Kiara Sahagun, Isobel Williamson

Artificial intelligence (AI) is a pressing focus for NATO because strategic AI use can allow nations to achieve resilient critical infrastructure as well as exploit vulnerabilities in that of adversaries. This chapter examines AI applications in two countries: China and the United States. Beijing and Washington, a key NATO member, are the principal balancing powers in the race to incorporate AI into the security sphere as well as the protection of critical infrastructure. China uses AI extensively in surveillance, urban planning, and in the commercial sector, as well as the modernization of its military. China's domestic use of AI is directly transferrable to its ability to exploit NATO critical infrastructure and military capabilities. The United States is integrating AI into defense capabilities and security operations to remain competitive. This chapter recommends that NATO create redundant backup analog infrastructure to protect against AI-integrated cyberattacks; and invest in AI education to promote research and development.

AI and Critical Infrastructure

Artificial intelligence is found in many networked or computerized systems, making AI a cornerstone of modern society. For example, in the field of transportation, AI-driven autonomous vehicles are becoming more sophisticated, potentially spelling the end of a need for human drivers.[38] It is even being used in public safety, where AI-controlled drones are hypothesized to be able to protect swimmers from shark attacks.[39] Artificial intelligence also serves as a foundational technology for the analysis of big data and for autonomous weaponry navigation. Big data analytics rely on AI because the volume of data is too massive for humans or traditional computing to parse. Artificial intelligence makes it possible to process these vast amounts of data, enabling the synthesis of complex data into easily understood visuals.[40] This feature has applications for autonomous weaponry. Artificial intelligence developments could allow these weapons to function without human oversight, greatly expanding their capabilities on the battlefield.

---

[38] Xiaozhe Yang, "Accelerated Move for AI Education in China," *ECNU Review of Education 2*, no. 3 (September 2019): 347–52, https://doi.org/10.1177/2096531119878590.
[39] Xiaohui Li, Hailong Huang, and Andrey V. Savkin, "A Novel Method for Protecting Swimmers and Surfers from Shark Attacks Using Communicating Autonomous Drones," *IEEE Internet of Things Journal* 7, no. 10 (October 2020): 9884-9894, https://doi.org/10.1109/JIOT.2020.2987997.
[40] Daniel E. O'Leary, "Artificial Intelligence and Big Data," *IEEE Intelligent Systems* 28, no. 2 (March-April 2013): 96-99, https://doi.org/10.1109/MIS.2013.39.

Most NATO mission-critical infrastructure incorporates artificial intelligence. In October 2021, NATO staff released an official Artificial Intelligence Strategy, dictating that AI use should respect six key guidelines: lawfulness, responsibility and accountability, explainability and traceability, reliability, governability, and bias mitigation.[41] Lawfulness refers to respecting international and humanitarian law. Responsibility and accountability mean that, even when technology with significant levels of autonomy is used, the users can still be held accountable. Explainability and traceability refer to either NATO or national-level oversight and transparency. AI applications should be thoroughly tested and used only in specific, pre-approved circumstances to fulfill the reliability guideline. Governable AI requires some human oversight and options for disengagement of the technology, and bias mitigation signifies active steps to reduce bias within AI algorithms.[42] To address the growing role of AI in government, industry, and national security, President Biden has announced through a congressional mandate the creation of a National AI Research Resource Task Force.[43] This group will develop a plan for national cyberinfrastructure that would expand participation in AI innovation. The United States does not yet federally regulate the use of AI, but there is increased lobbying and pressure from local governments and NGOs to create such a policy.[44]

NATO and the EU have cooperated in recent years to promote the regulation of AI, especially concerning cybersecurity. These collaborations will become even more essential as states refine their AI technology to standardize AI usage within the Alliance and present cohesive protocol in the face of adversaries.[45] This chapter will provide additional information on the United States' and China's use of AI and bring to light concerns around AI and critical infrastructure that are essential for NATO to incorporate into policy going forward.

The NATO Partners and China: AI Balancing Powers

[41]Zoe Stanley-Lockman and Edward Hunter Christie, "An Artificial Intelligence Strategy for NATO," *NATO Review*, October 25, 2021, https://www.nato.int/docu/review/articles/2021/10/25/an-artificial-intelligence-strategy-for-nato/index.html.

[42] Stanley-Lockman and Christie, "Artificial Intelligence Strategy for NATO."

[43] Tracy Ryan, "US Launches Task Force to Study Opening Government Data for AI Research," *Wall Street Journal*, June 10, 2021, https://www.wsj.com/articles/u-s-launches-task-force-to-open-government-data-for-ai-research-11623344400.

[44] US National Security Commission on Artificial Intelligence (NSCAI), "Final Report," (Washington, DC: 2021), 19, https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.

[45] Peter Poptchev, "NATO-EU Cooperation in Cybersecurity and Cyber Defence Offers Unrivalled Advantages," *Information and Security: An International Journal*, 45 (2020): 35-55, https://isij.eu/article/nato-eu-cooperation-cybersecurity-and-cyber-defence-offers-unrivalled-advantages.

A critical reason for NATO investment and research on artificial intelligence is to compete against adversaries. Currently, the world's leading powers are racing to develop artificial intelligence to improve their populations' quality of life, influence diplomacy, and change how wars are fought. For example, fifteen countries launched the Global Partnership on Artificial Intelligence in June 2020 to advance artificial intelligence while protecting democratic values and human rights.[46] While not a NATO project, this Global Partnership shows how states can work together to develop artificial intelligence responsibly.

The United States is deploying AI for military and commercial uses. In 2020, the United States incorporated AI into military operations through Project Maven, which used this technology to identify enemy combatants in Iraq and Syria.[47] The United States also found significant positive benefits in using AI for supply chain resilience, contact tracing, and scenario planning during the pandemic. Commercially, the United States relies heavily on AI for customer service, economic savings, and decision-making.[48]

NATO has designated China a security threat to the alliance, and its use of artificial intelligence to control its population has proven that Beijing has the upper hand in the development of AI technology. This technology is directly transferrable to military intelligence, surveillance, and reconnaissance applications, as well as countering and debilitating Allied defenses. This Task Force found these disturbing trends important to highlight in relation to NATO's role as a balancing power to Beijing.

Recent internal developments in China show concerning surveillance developments that could be translated to target and debilitate NATO operations. China first started developing artificial intelligence in the 1970s. Since then, the nation has undergone what experts refer to as an "artificial intelligence revolution."[49] Beijing's capabilities to surveil, coerce and control populations with the aid of artificial intelligence threaten not only other countries but also their own citizens. Some Chinese AI companies, for example, enabled the genocide against

[46] Audrey Plonk, "The Global Partnership on AI Takes Off–at the OECD," *OECD.AI*, July 09, 2020, https://oecd.ai/en/wonk/oecd-and-g7-artificial-intelligence-initiatives-side-by-side-for-responsible-ai

[47] Richard Schultz and Richard Clarke, "Big Data at War: Special Operations Forces, Project Maven, and Twenty-First-Century Warfare," Modern War Institute, August 25, 2020, https://mwi.usma.edu/big-data-at-war-special-operations-forces-project-maven-and-twenty-first-century-warfare/.

[48] US NSCAI, "Final Report," 116.

[49] Ross Andersen, "The Panopticon is Already Here," *The Atlantic*, September 2020, https://www.theatlantic.com/magazine/archive/2020/09/china-ai-surveillance/614197/.

Uyghurs in Xinjiang.[50] China's use of AI to track Uyghurs when they reach the edge of or leave their neighborhoods is particularly concerning. AI systems can also identify their vehicles and extend near-complete surveillance over Uyghur populations. China is currently developing a new AI system to assess the political threat of individual Uyghur people. This system could be modified to allow AI-enabled surveillance of the entire Chinese and/or foreign populations, not just of Uyghurs.[51]

China is also using AI to promote commerce and the efficiency and resilience of infrastructure. For example, China uses a technology called "City Brains" to collect data and monitor infrastructure continuously. These projects aim to develop a comprehensive database that can monitor many aspects of city functioning, including traffic and environmental concerns.[52] China also recently rolled out three initiatives to shape AI advancement for economic, surveillance, and developmental purpose.[53] These technologies are directly transferrable to military uses both at home and abroad.

These Chinese AI projects should concern NATO and the global community. Beyond committing further human rights violations, Beijing could undermine NATO operations if it continues to develop AI without obstruction. These AI programs—particularly "City Brains" and the programs that track Uyghurs—could be expanded to monitor Alliance military operations and model troop movements, both of which would give China a strategic edge.

AI on the battlefield

One can best understand AI's role on the battlefield at the tactical level, where AI is becoming more integral to the battlespace thanks to the increasing sophistication of weaponry and defense systems. Many countries, for example, use close-in weapons systems. These are defense systems designed to intercept incoming rockets and projectile fire, with examples including the United States' Phalanx, Russia's Kashtan, and China's Type 730 close-in weapons systems. Each

[50] Michael Chertoff and N. Macdonnell Ulsch, "AI Companies are Enabling Genocide in China," *Washington Post*, April 12, 2021, https://www.washingtonpost.com/opinions/2021/04/12/china-is-using-ai-repress-uyghurs-it-must-stop/.

[51] Andersen, "The Panopticon is Already Here."

[52] Chris Buckley et. al., "In China, Covid-Era Controls May Outlast the Coronavirus," *New York Times*, January 30, 2022, https://www.nytimes.com/2022/01/30/world/asia/covid-restrictions-china-lockdown.html

[53] Matt Sheehan, "China's New AI Governance Initiatives Shouldn't be Ignored," Carnegie Endowment for International Peace, January 4, 2022, https://carnegieendowment.org/2022/01/04/china-s-new-ai-governance-initiatives-shouldn-t-be-ignored-pub-86127.

of these systems requires the rapid identification and interception of incoming threats, making humans too slow to be able to operate them. Instead, these systems all use AI-powered aiming control systems that can process information and act within a fraction of a second.[54] Artificial intelligence could be used in a similar role to intercept emerging threats like hypersonic missiles, as the reaction times needed to intercept such a weapon successfully are unfathomably small. No such defenses are currently known to exist, however. The increasing prevalence of autonomous weapons on the battlefield showcases the importance of AI in tactical situations. Its ability to react quicker than humans in rapidly evolving battlefields will provide actors with autonomous weapons tactical supremacy over those with only traditional weaponry.

At the operational and strategic levels of warfare, AI plays a major role in data analysis and planning. AI's ability to process large volumes of data allows it to contribute to operational thinking: where to commit forces, what plan would get the closest to the strategic objective, etc. While not currently widely used in this specific capacity, certain AI systems can perform better than military professionals at the tactical level.[55] This holds promise for AI involvement at high levels of military decision-making in the future.

Cyberspace is an emerging strategic theater, but its importance cannot be understated. It provides a crucial link between critical infrastructure that simultaneously increases critical infrastructure capabilities and vulnerabilities. Due to the importance of critical infrastructure, maintaining supremacy in cyberspace operations is essential to the integrity of the Alliance. Artificial intelligence provides both offensive and defensive capabilities towards that end. On the offensive side, AI can be used in cyberattack scenarios to find and exploit network vulnerabilities, potentially resulting in the destruction or incapacitation of critical infrastructure.[56] Sophisticated malware that exploits new vulnerabilities will be easier to create and deploy as more powerful AI becomes available; adversaries will be better able to locate and exploit vulnerabilities thanks to their computational abilities.

Similarly, AI-powered processing can help protect networks from attacks, though it is unclear if AI is more useful for an attacker or defender in such a

---

[54] Demetrios Serakos, "Stability, Aim Bias Compensation and Noise Sensitivity of Phalanx CIWS Control System," *First IEEE Regional Conference on Aerospace Control Systems* (May 1993): 17-23, https://doi.org/10.1109/AEROCS.1993.720885.

[55] Jonathan Boron and Chris Darken, "Developing Combat Behavior Through Reinforcement Learning in Wargames and Simulations," *IEEE Conference on Games*, October 2020, 728-731, https://doi.org/10.1109/CoG47356.2020.9231609.

[56] Erik Zouave et. al., *Artificially Intelligent Cyberattacks*, Totalförsvarets forskningsinstitut (FOI) Report FOI-R--4947—SE, (Stockholm, SE: FOI, March 2020), 17, https://www.statsvet.uu.se/digitalAssets/769/c_769530-l_3-k_rapport-foi-vt20.pdf.

scenario.[57] Integration of AI into cybersecurity systems will also allow network intrusions into critical infrastructure to be more easily detected than before, allowing for a rapid response that can prevent long-term damage. China is making rapid progress relative to NATO member states in this field, threatening to overtake the Alliance's capabilities completely.[58] China already outcompetes any single nation regarding AI integration into cyberwarfare. The Alliance can only overcome this disadvantage with a united stance on AI.

Opportunities and Vulnerabilities

While AI presents NATO with many opportunities, AI also opens new vulnerabilities, including bias, the potential for malicious use, and unanticipated threats. First, data from a single source can lead to racial and perspective bias.[59] Any bias will limit the technology from achieving its full potential, so it is imperative to assess the quality of the data used for AI technology. Second, the inputting of malicious data into algorithms can produce disastrous consequences. Artificial intelligence is commonly used to supplement cybersecurity for its ability to recognize patterns of threats.[60] This defensive capability can itself be a vulnerability, as AI technology is subject to cyber threats, potentially resulting in the breach of critical infrastructure systems. AI cybersecurity operates through the input of data and machine learning to filter out threats from their systems. These cybersecurity protections are still vulnerable to hybrid threats, as these threats are meticulously designed to bypass detection. One such technique is known as "spearfishing," where attachments are sent with emails containing malware.[61] Russian hackers have successfully used this technique, as seen in 2015 with the cyberattack that shut down Ukraine's power grid and infiltrated the energy infrastructure in the United States in 2018.[62] Cyber threats and hybrid threats prove how any kind of informational change made to AI technology could be disastrous.

---

[57] Zouave et al., *Artificially Intelligent Cyberattacks*, 35.
[58] Chris C. Demchak, "China: Determined to Dominate Cyberspace and AI," *Bulletin of the Atomic Scientists* 75, no. 3 (April 2019): 99-104, https://doi.org/10.1080/00963402.2019.1604857.
[59] Ifeoma Elizabeth Nwafor, "AI Ethical Bias: A Case for AI Vigilantism (AIlantism) in Shaping the Regulation of AI," *International Journal of Law and Information Technology* 29, no. 3 (Autumn 2021): 225-240, https://doi.org/10.1093/ijlit/eaab008.
[60] Reding and Eaton, *Science & Technology Trends,* 56.
[61] Meg King and Jacob Rosen, "The Real Challenges of Artificial Intelligence: Automating Cyber Attacks," *AMP* (blog), Wilson Center Science and Technology Innovation Program, November 28, 2018, https://www.wilsoncenter.org/blog-post/the-real-challenges-artificial-intelligence-automating-cyber-attacks.
[62] US Cybersecurity Infrastructure and Security Agency, "ICS Alert (IR-Alert-H-16-056-01)," February 25, 2016, https://www.cisa.gov/uscert/ics/alerts/IR-ALERT-H-16-056-01.

Finally, additional vulnerabilities might present themselves in unanticipated behavior in AI technology.

NATO's continued authority in the international community will depend on its use of AI. Artificial intelligence offers NATO a variety of tools to promote resilience, and AI can be merged with other technologies to amplify current capabilities. Generally, AI will produce better decision-making, supporting defense operations and security operations.[63] Military capabilities will be improved through associated technologies like virtual reality, quantum computing, autonomy, modeling, space, materials research, manufacturing logistics, and big data analytics.[64] Artificial intelligence can be an essential aspect of the next generation of NATO operations, military hardware, and critical infrastructure. Driven by these key opportunities and by potential adversaries' advancements in AI, NATO has a strong incentive to promote further AI innovation.

Policy recommendations

As described in the case studies above, the field of artificial intelligence is highly competitive, particularly in the adversarial relationship between NATO and China. Through its domestic surveillance regime, Beijing has been able to develop robust AI technology that can be applied in strategic competition with the West as well as concrete battlefield capabilities. NATO partner nations' common values and privacy laws prohibit the domestic applications of AI developed by the Chinese government. NATO nonetheless needs to ensure that member states maintain high AI standards, promote technological development, and test their AI capabilities to locate deficiencies. *To this end, we recommend NATO hold international AI competitions that explore the most critical aspects of AI utilization in military contexts.* NATO can hold traditional wargames to hone its AI doctrine in military contexts and public events that showcase new ideas and AI solutions.

NATO member states already host international wargames, making it simple to hold AI-oriented wargames under existing frameworks. For example, many NATO and non-NATO partners participate in the Strong Europe Tank Challenge, which seeks to showcase and develop efficient and effective armored operations.[65] Similarly, the United States DoD provides a wargaming fund, which

[63] Center for Security and Emerging Technology, "Collaborative S&T Development: Creating a NATO Decision Advantage in AI," YouTube video, accessed on February 28, 2022, https://www.youtube.com/watch?v=yXn_pKnlwyI.
[64] D.F. Reding and J. Eaton, *Science & Technology Trends 2020-2040* (Brussels, BE: NATO Science & Technology Organization, March 2020), 53-54.
[65] US Army, "Strong Europe Tank Challenge," *7th Army Training Command*, https://www.7atc.army.mil/TankChallenge/.

has been integral for "revealing critical gaps and suggesting solutions."[66] These wargames allow leaders to develop their decision-making capacities in lower-stakes environments, which translates to more effective disaster mitigation during an actual crisis.[67]

Public competitions could focus on cybersecurity innovation and tactical AI. Cybersecurity will only become more important as time goes on, so effective preparation and experience are key as new offensive and defensive AI solutions become available.[68] Tactical AI holds promise as the "commander of the future," and perfecting tactical AI will be crucial to winning the battlefields of tomorrow.[69] We recommend NATO incentivize innovation in these competitions with a monetary reward. These funds could be drawn from the existing NATO Innovation Fund, which NATO established to help promote innovation to retain NATO's technological edge.[70] These public competitions will provide NATO personnel with fresh outlooks on AI technologies. NATO can then integrate these findings into its doctrine to deploy AI more effectively.

[66] Garrett Heath and Oleg Svet, "Better Wargaming is Helping the US Military Navigate a Turbulent Era," *Defense One,* August 2018, *https://www.defenseone.com/ideas/2018/08/better-wargaming-helping-us-military-navigate-turbulent-era/150653/.*
[67] Peter Perla and E.D. McGrady, "Why Wargaming Works," *Naval War College Review* 64, no. 3, Article 8, 2011, https://digital-commons.usnwc.edu/nwc-review/vol64/iss3/8.
[68] Zouave et al., *Artificially Intelligent Cyberattacks*, 17.
[69] Boron and Darken, "Developing Combat Behavior."
[70] NATO, "NATO Allies take the lead on the development of NATO's Innovation Fund," *NATO Newsroom,* October 22, 2021, https://www.nato.int/cps/en/natohq/news_187607.htm.

Selected Bibliography

Andersen, Ross. “The Panopticon is Already Here.” *The Atlantic,* September 2020. https://www.theatlantic.com/magazine/archive/2020/09/china-ai-surveillance/614197/.

Bragazzi, Nicola Luigi, Haijiang Dai, Giovanni Damiani, Masoud Behzadifar, Mariano Martini, and Jianhong Wu. “How Big Data and Artificial Intelligence Can Help Better Manage the COVID-19 Pandemic.” *International Journal of Environmental Research and Public Health* 17, no. 9 (2020): 3176. https://doi.org/10.3390/ijerph17093176.

Boron, Jonathan, and Chris Darken. “Developing Combat Behavior through Reinforcement Learning in Wargames and Simulations.” *2020 IEEE Conference on Games* (October 2020): 728-731. https://doi.org/10.1109/CoG47356.2020.9231609.

Briganti, Giovanni, and Olivier Le Moine. “Artificial Intelligence in Medicine: Today and Tomorrow.” *Frontiers in Medicine* 7 (February 5, 2020). https://doi.org/10.3389/fmed.2020.00027.

Center for Security and Emerging Technology. “Collaborative S&T Development: Creating a NATO Decision Advantage in AI.” YouTube video, accessed on February 28, 2022. https://www.youtube.com/watch?v=yXn_pKnlwyI.

Chertoff, Michael, and N. Macdonnell Ulsch. “AI Companies are Enabling Genocide in China.” *Washington Post*, April 12, 2021. https://www.washingtonpost.com/opinions/2021/04/12/china-is-using-ai-repress-uyghurs-it-must-stop/

Demchak, Chris C. Demchak. “China: Determined to Dominate Cyberspace and AI.” *Bulletin of the Atomic Scientists* 75, no. 3 (April 2019): 99-104. https://doi.org/10.1080/00963402.2019.1604857.

Escobar, Jesús Jaime Moreno, Oswaldo Morales Matamoros, Ricardo Tejeida Padilla, Ixchel Lina Reyes, and Hugo Quintana Espinosa. “A Comprehensive Review on Smart Grids: Challenges and Opportunities.” *Sensors* 21, no. 21 (October 21, 2021): 6978. https://doi.org/10.3390/s21216978.

Hu, Zixin, Qiyang Ge, Shudi Li, Li Jin, and Momiao Xiong. “Artificial Intelligence Forecasting of Covid-19 in China.” *arXiv* (2020). https://arxiv.org/ftp/arxiv/papers/2002/2002.07112.pdf.

King, Meg, and Jacob Rosen. “The Real Challenges of Artificial Intelligence: Automating Cyber Attacks.” *AMP* (blog), Wilson Center Science and Technology Innovation Program, November 28, 2018. https://www.wilsoncenter.org/blog-post/the-real-challenges-artificial-intelligence-automating-cyber-attacks.

Li, Xiaohui, Hailong Huang, and Andrey V. Savkin. “A Novel Method for Protecting Swimmers and Surfers from Shark Attacks Using Communicating Autonomous Drones.” *IEEE Internet of Things Journal* 7, no. 10 (October 2020): 9884-9894. https://doi.org/10.1109/JIOT.2020.2987997.

NATO. “NATO Allies take the lead on the development of NATO’s Innovation Fund.” *NATO Newsroom*, October 22, 2021. https://www.nato.int/cps/en/natohq/news_187607.htm.

Nwafor, Ifeoma Elizabeth. “AI Ethical Bias: A Case for AI Vigilantism (AIlantism) in Shaping the Regulation of AI.” *International Journal of Law and Information Technology* 29, no. 3 (Autumn 2021): 225-240. https://doi.org/10.1093/ijlit/eaab008.

O’Leary, Daniel E. “Artificial Intelligence and Big Data.” *IEEE Intelligent Systems* 28, no. 2 (March-April 2013): 96-99. https://doi.org/10.1109/MIS.2013.39.

Pham, Quoc-Viet, Dinh C. Nguyen, Thien Huynh-The, Won-Joo Hwang. “Artificial Intelligence (AI) and Big Data for Coronavirus (COVID-19) Pandemic: A Survey on the State-of-the-Arts.” *IEEE Access 8,* July 2020. https://doi.org/10.1109/ACCESS.2020.3009328.

Plonk, Audrey. “The Global Partnership on AI Takes Off–at the OECD.” *OECD.AI,* July 09, 2020. https://oecd.ai/en/wonk/oecd-and-g7-artificial-intelligence-initiatives-side-by-side-for-responsible-ai

Poptchev, Peter. “NATO-EU Cooperation in Cybersecurity and Cyber Defence Offers Unrivalled Advantages.” *Information and Security: An*

International Journal, 45 (2020): 35-55. https://isij.eu/article/nato-eu-cooperation-cybersecurity-and-cyber-defence-offers-unrivalled-advantages.

Perla, Peter, and E.D. McGrady. "Why Wargaming Works." *Naval War College Review* 64, no. 3, Article 8, 2011. https://digital-commons.usnwc.edu/nwc-review/vol64/iss3/8.

Reding, D.F., and J. Eaton. *Science & Technology Trends 2020-2040.* Brussels, BE: NATO Science & Technology Organization, March 2020.

Ryan, Tracy. "US Launches Task Force to Study Opening Government Data for AI Research." *Wall Street Journal*, June 10, 2021. https://www.wsj.com/articles/u-s-launches-task-force-to-open-government-data-for-ai-research-11623344400.

Schultz, Richard, and Richard Clarke. "Big Data at War: Special Operations Forces, Project Maven, and Twenty-First-Century Warfare." Modern War Institute, August 25, 2020. https://mwi.usma.edu/big-data-at-war-special-operations-forces-project-maven-and-twenty-first-century-warfare/.

Serakos, Demetrios. "Stability, Aim Bias Compensation and Noise Sensitivity of Phalanx CIWS Control System." *First IEEE Regional Conference on Aerospace Control Systems* (May 1993): 17-23. https://doi.org/10.1109/AEROCS.1993.720885.

Sheehan, Matt. "China's New AI Governance Initiatives Shouldn't be Ignored." Carnegie Endowment for International Peace, January 4, 2022. https://carnegieendowment.org/2022/01/04/china-s-new-ai-governance-initiatives-shouldn-t-be-ignored-pub-86127.

Stanley-Lockman, Zoe, and Edward Hunter Christie. "An Artificial Intelligence Strategy for NATO." *NATO Review*, October 25, 2021. https://www.nato.int/docu/review/articles/2021/10/25/an-artificial-intelligence-strategy-for-nato/index.html.

UN Office of Counter-Terrorism and UN Interregional Crime and Justice Research Institute. "Countering Terrorism Online with AI - an Overview for Law Enforcement." July 28, 2021. https://issuu.com/unicri/docs/countering_terrorism_online_with_artificial_intell.

US Army. “Strong Europe Tank Challenge.” *7th Army Training Command*. https://www.7atc.army.mil/TankChallenge/.

US Cybersecurity Infrastructure and Security Agency. “ICS Alert (IR-Alert-H-16-056-01).” February 25, 2016. https://www.cisa.gov/uscert/ics/alerts/IR-ALERT-H-16-056-01.

US National Security Commission on Artificial Intelligence (NSCAI). “Final Report.” Washington, DC: 2021. https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.

USAF College of Aerospace Doctrine, Research and Education (CADRE). “Three Levels of War,” *Air and Space Power Mentoring Guide* 1. Maxwell AFB, AL: CADRE, 1997.

Weinstein, Emily. “China’s Use of AI in its COVID-19 Response.” CSET Data Brief, *CSET*, August 2020. https://cset.georgetown.edu/publication/chinas-use-of-ai-in-its-covid-19-response/.

Yang, Xiaozhe. “Accelerated Move for AI Education in China.” *ECNU Review of Education 2*, no. 3 (September 2019): 347–52. https://doi.org/10.1177/2096531119878590.

Zouave, Erik, Marc Bruce, Kajsa Colde, Margarita Jaitner, Ioana Rodhe, and Tommy Gustafsson. *Artificially Intelligent Cyberattacks*, Totalförsvarets forskningsinstitut (FOI) Report FOI-R--4947—SE. Stockholm, SE: FOI, March 2020. https://www.statsvet.uu.se/digitalAssets/769/c_769530-l_3-k_rapport-foi-vt20.pdf.

Chapter 4: Drones and Autonomous Technology

By: Christopher Chromyszak, Samuel Jacobson, and Martha Lewis

Autonomous technology is changing how armed conflicts are fought. NATO adversaries and terrorist organizations around the globe are utilizing and investing in these disruptive technologies. The Russian invasion of Ukraine necessitates that NATO pays special attention to offensive autonomous technologies. The continued coordination of NATO's Science and Technology Organization (STO) and Science for Peace and Security (SPS) programs would allow promising innovations for the future of NATO's resilience against autonomous weapons. We recommend the Alliance integrate current defensive capabilities into a system-of-systems, meaning an inter-operable technological platform that integrates several technologies to operate seamlessly to defend against autonomous systems.

Applications of autonomous technology

Advancements in autonomous technology create opportunities to increase security capabilities, resilience, and the productivity of the military and civilian industrial sectors. On the other hand, these same opportunities allow aggressor states or non-states to compromise critical infrastructure, use autonomous weapons to cripple security infrastructure, and undermine social stability. Russia's aggressive posture in Eastern Europe has increased the need for NATO countries to develop and innovate on mission-capable autonomous technology.

The global defense and security environment is growing more complicated with the development of autonomous technology and other emerging technologies.[71] NATO adversaries such as Russia are increasing their usage and development of autonomous weapons, creating a severe threat to NATO security. We recommend NATO protect its interests and critical infrastructure sufficiently from autonomous weapons such as drones. State and non-state actors are increasing the advancement and usage of such weapon systems, exposing gaps in critical infrastructure security.

Policymakers in NATO member states can develop a shared understanding of adversaries' autonomous weapons capabilities and lessons from prior conflicts involving autonomous weapons. There is precedent for this kind of partnership. Following the terrorist attacks in the United States on September 11th, NATO

[71] D.F. Reding and J. Eaton, *Science & Technology Trends 2020-2040* (Brussels, BE: NATO Science & Technology Organization, March 2020).

members launched a Partnership Action Plan Against Terrorism.[72] This partnership pushed members to share all information on terrorist threats. As these weapons systems continue to mature, the threat of drone usage by terrorists remains a security priority. The continuation of the Defence Against Terrorism Programme of Work (DAT POW) framework as agreed upon by defense ministers in 2019 is vital. This continuation includes increased cooperation between the NATO Science & Technology Organization and DAT POW to increase capabilities to counter autonomous weapons.[73] Through sharing information and resources, the speed of technology advancement within NATO can enhance communication about and protection from autonomous attacks.

Furthermore, to improve critical infrastructure security against autonomous systems, NATO can balance laws, ethics, and regulations. It is important that NATO states have a forward-thinking regulatory process and consider the possibilities of new emerging technologies.[74] Autonomous technology reduces emotional decision-making and can remove the threat of physical harm; however, it also raises other concerns that need to be considered. There are dangers concerning autonomous weapons regarding their respect for human life, ability to identify between civilians and militants, and the possibility of malicious actors corrupting the technology.[75] There are also debates on whether autonomous weapons can adhere to the Law of Armed Conflict.[76] It is paramount for policymakers to consider these legal and ethical debates and the minimum degree of human involvement in autonomous. Doing otherwise would set a dangerous precedent in the use of this technology.

Autonomous weapons have a vast range of uses, including surveillance, protection, offensive strikes, and terrorist use. Autonomous weapons create endless possibilities and significant military advantage in an ever more technical world.[77] Militaries across the world are therefore heavily investing in this technology. The United States has allocated $1.7 billion for autonomous weapon investment in the 2021 Department of Defense budget.[78] Russia and China are also increasing their research and investing in autonomy, with Russia developing five programs to

[72] NATO, "The Partnership Action Plan against Terrorism (PAP-T) (Archived)," April 13, 2021, https://www.nato.int/cps/en/natohq/topics_50084.htm.
[73] NATO, "Countering Terrorism," *NATO Newsroom*, September 14, 2021https://www.nato.int/cps/en/natohq/topics_77646.htm.
[74] Reding and Eaton, *Science & Technology Trends.*
[75] James M. Anderson et al., "Autonomous Systems: Issues for Defence Policymakers" (Norfolk, VA: NATO Supreme Allied Command Transformation, September 30, 2015),
[76] Anderson et al., "Autonomous Systems."
[77] Reding and Eaton, *Science & Technology Trends.*
[78] US Department of Defense, "DOD Releases Fiscal Year 2021 Budget Proposal," accessed February 13, 2022, https://www.defense.gov/News/Releases/Release/Article/2079489/dod-releases-fiscal-year-2021-budget-proposal/.

increase the automation of its nuclear arsenal, part of a $8.5 billion annual investment as of 2019.[79] Due to technological innovations and shrinking computer components, autonomous weapons will become essential assets in a country's military capabilities.[80] In 2014, Russia planned to gain 500 Unmanned Aerial Vehicles (UAV) by 2020.[81] These innovations, along with other technological advances in military capabilities, have created a tense international political environment. Similarly, China has exponentially increased its investment in autonomous capabilities, constituting a major portion of its Research, Development, Test, and Evaluation (RDT&E) expenditures. Autonomous technologies were the fastest growing additional spending item in the Chinese defense budget, amounting to an estimated $25 billion in 2019.[82]

Russian and Chinese autonomous technologies

Russia has invaded Ukraine under the pretense that Russia was threatened by NATO expansion and influence. On February 24th, 2022, Russian President Vladimir Putin announced that Russia would conduct military operations in Ukraine, infringing on Ukrainian sovereignty. Russia has already deployed tanks, fighter jets, artillery, and helicopters.[83] The NATO alliance has condemned the Russian invasion, and many NATO countries have imposed sanctions on Russia.[84] This conflict will showcase the full impact of drones and other emerging technologies on modern warfare.

In 2005, Russian Federation president Vladimir Putin gave a speech calling the collapse of the USSR "the greatest geopolitical catastrophe of the century."[85] Since the invasion of Georgia in 2008 by the Russian Armed Forces, there have been security concerns for neighboring post-Soviet states. These post-Soviet states

[79] Center for Naval Analyses, "Artificial Intelligence and Autonomy in Russia," Russia Studies Program, accessed March 3, 2022, https://www.cna.org/centers/cna/sppp/rsp/russia-ai.
[80] Liran Antebi, "Changing Trends in Unmanned Aerial Vehicles: New Challenges for States, Armies and Security Industries" 6, no. 2 (2014): 25.
[81] Antebi, "Changing Trends in Unmanned Aerial Vehicles."
[82] Nan Tian and Fei Su, "An Estimate of China's Military Expenditure," *SIPRI*, January 2021, https://www.sipri.org/sites/default/files/2021-01/2101_sipri_report_a_new_estimate_of_chinas_military_expenditure.pdf, 18.
[83] Yuras Karamanau et al., "Russia Attacks Ukraine; Peace in Europe 'Shattered,'" *AP News*, February 24, 2022, https://apnews.com/article/russia-ukraine-putin-attack-a05e7c4563ac94b963134bba83187d46.
[84] Sabine Siebold and Philip Blenkinsop, "EU Tightens Russian Sanctions and Buys Weapons for Ukraine," *Reuters*, February 27, 2022, https://www.reuters.com/world/europe/eu-close-airspace-russia-curb-media-target-belarus-2022-02-27/.
[85] "Putin: Soviet Collapse a 'Genuine Tragedy,'" *NBC News*, April 25, 2005, https://www.nbcnews.com/id/wbna7632057.

see the Georgian conflict and Putin's statements as indications of Russian ambitions in Eastern Europe and the Baltics.[86] The annexation of Crimea in 2014 and the current war between Ukraine and Russia demonstrate the importance of a comprehensive understanding of Russian military assets and capabilities.

Over the last decade, Russia has greatly increased investment in researching and acquiring autonomous technologies to bolster its economic and military capabilities.[87] Autonomous technologies, such as drones and sensor networks, have reinforced Russian intelligence, surveillance, and reconnaissance (ISR) and command and control capabilities. New autonomous industrial technology has also increased productivity in the Russian industrial sector, limiting the risks of extracting valuable resources in hazardous arctic environments.[88] Autonomous technologies allow Russia to avoid traditional economic and military development obstacles.

A large part of Russia's economy centers around extracting and exporting natural resources. Since the 1930s, Russia has exploited the natural gas reserves in the Russian Arctic. The Russian government has invested five trillion rubles into 150 development projects.[89] Many of these developmental projects exist in extreme terrain conditions. The challenge of maintaining equipment in such a hazardous environment limits resource exploitation. The use of robotic extraction tools, submarines, and other platforms can nevertheless limit human risk in the extraction and refining of these resources. Incorporating autonomous technology as sensor networks to predict weather patterns and monitor possible natural gas leaks further reduces the risk of disaster during extraction.[90] The use of this technology helps increase the Russian economy's prominence by growing in regional prominence in the energy sector.

Automation is a promising and rapidly developing field of technology that is used in a wide range of roles, especially in Russia. As well as supporting Russian economic prosperity, drones and other autonomous technologies can also act as early warning systems or even as a deterrent to adversaries. Autonomous networks and vehicles continue to become more critical and integral in the defense of critical infrastructure. Submarines have long been used for discreet reconnaissance and as

---

[86] Tomas Valasek, "What Does the War in Georgia Mean for EU Foreign Policy?," Center for European Reform, 2008, 5, https://www.cer.org.uk/publications/archive/briefing-note/2008/what-does-war-georgia-mean-eu-foreign-policy.

[87] Leonid Gokhberg, Alexander Sokolov, and Alexander Chulok, "Russian S&T Foresight 2030: Identifying New Drivers of Growth," *Foresight* 19, no. 5 (January 1, 2017): 441–56, https://doi.org/10.1108/FS-07-2017-0029.

[88] Natalia Romasheva and Diana Dmitrieva, "Energy Resources Exploitation in the Russian Arctic: Challenges and Prospects for the Sustainable Development of the Ecosystem," *Energies* 14, no. 24 (December 15, 2021): 8300, https://doi.org/10.3390/en14248300.

[89] Romasheva and Dmitrieva, "Energy Resources Exploitation in the Russian Arctic," 8300.

[90] Gokhberg, Sokolov, and Chulok, "Russian S&T Foresight 2030."

a tool in nuclear arsenals, but the deployment of innovative underwater drones is threatening that dimension of warfare. Networks of autonomous underwater sensors can be strategically placed at geographic chokepoints or by critical infrastructure to limit the ability of submarines to navigate those waters undetected.[91] Outside of the water, sophisticated drone networks now allow controllers to use a mass of drones to survey a large area for human movement or other important information.[92] High-imaging drones combined with identity databases can provide a security network to identify threats remotely and before terrorist activities can be conducted.[93] These uses of drones limit an aggressor's options while acting as an early warning system.

Russia is not the only potential adversary NATO faces. Russia has strong diplomatic ties with China, another world leader in autonomous weapons.[94] The two countries have worked together on security, energy, and intelligence issues. These two potential NATO adversaries may share information and technology to further their use and production of drones. This partnership pressures NATO countries to continue growing their drone capabilities. We believe therefore that NATO continue to share, develop, and use drones for protection, surveillance, and military action when necessary. NATO nevertheless has the opportunity to implement autonomous technology cautiously and responsibly.

Global autonomous weapons capabilities

The most common state uses of autonomous weapons are currently reconnaissance and precise aerial missile strikes. The United States and NATO have primarily used these capabilities in counterterrorism missions; however, armed conflicts between equally capable states can be devastating. Autonomous weapons work hand in hand with other emerging technologies, such as machine learning, facial recognition, and Artificial Intelligence (AI).[95] Turkey's drone Kargu-2 allegedly can use facial recognition technology and machine learning to

[91] Megan Eckstein, "Sonar Equipped Drone Fleets Could Be Key to Future Submarine Warfare," *USNI News* (blog), March 9, 2020, https://news.usni.org/2020/03/09/sonar-equipped-drone-fleets-could-be-key-to-future-submarine-warfare.
[92] Donggeun Oh and Junghee Han, "Smart Search System of Autonomous Flight UAVs for Disaster Rescue," *Sensors* 21, no. 20 (October 15, 2021): 6810–6810, https://doi.org/10.3390/s21206810.
[93] NATO, "DEEP - Counter-Terrorism Reference Curriculum," *NATO Newsroom*, September 30, 2020, https://www.nato.int/cps/en/natohq/topics_176310.htm.
[94] David Leonhardt, "A New Axis," *New York Times*, February 9, 2022, sec. Briefing, https://www.nytimes.com/2022/02/09/briefing/china-russia-alliance.html.
[95] Reding and Eaton, *Science & Technology Trends.*

"hunt down" a specific target.[96] Many countries, including the US, have worked on drone swarming technology to overcome and overwhelm opposition forces.[97] With these new capabilities and the increase of lethality with autonomy, conflicts are far more advanced and dangerous than previously thought

Drones also play a decisive role in intelligence gathering and reporting. Advancements in technologies allow Unmanned Aerial Surveillance (UAS) to collect intelligence through many means such as advanced imaging, acoustics, and signals across the radio frequency spectrum.[98] The Future Combat Air System initiative between France, Germany, and Spain integrates this technology and others. This platform will then act as a *system-of-systems* interlinked to work together, either autonomously or manually, in operations and strikes.[99] Alliances and military partnerships continue to create and modernize interconnected systems and networks of defense across the globe.

Russia has also made large advancements in its drone capabilities and arsenal. Russia is projected to add the Sukhoi S-70 Okhotnik-B (Hunter) Unmanned Combat Aerial Vehicle (UCAV) to its military arsenal in 2024. The Hunter-B drone is a stealth drone that can work in tandem with the Russian SU-57 fighter jet, increasing the awareness of one fighter jet. The Hunter-B UCAV can carry two thousand kilograms of payload and execute precision strikes with "dumb" bombs thanks to the SVP-24 aiming system.[100] The artificial intelligence onboard the Hunter-B UCAV uses the same interface as the SU-57 and can operate entirely autonomously, tracking and targeting enemies.[101] This incorporation of UCAVs into a fighter jet's capabilities will revolutionize how fighter jets operate. The Altius-U reconnaissance drone is another important advancement of Russian

---

[96] Zachary Kallenborn, "Applying Arms-Control Frameworks to Autonomous Weapons," *Brookings* (blog), October 5, 2021, https://www.brookings.edu/techstream/applying-arms-control-frameworks-to-autonomous-weapons/.

[97] NATO, "Autonomous Military Drones: No Longer Science Fiction," *NATO Review*, July 28, 2017, https://www.nato.int/docu/review/articles/2017/07/28/autonomous-military-drones-no-longer-science-fiction/index.html.

[98] Joint Air Power Competence Centre (JAPCC), "A Comprehensive Approach to Countering Unmanned Aircraft Systems" (Kalkar, DE: JAPCC, December 17, 2020), https://www.japcc.org/portfolio/c-uas/.

[99] Airbus, "The Future Combat Air System (FCAS)," accessed February 9, 2022, https://www.airbus.com/en/products-services/defence/multi-domain-superiority/future-combat-air-system-fcas.

[100] Новостник, "Sighting and Navigation Complex SVP-24 'Hephaestus' Will Be Modernized," Военное обозрение, accessed February 14, 2022, https://en.topwar.ru/157691-pricelno-navigacionnyj-kompleks-svp-24-gefest-budet-modernizirovan.html.

[101] Mark Episkopos, "Russia's Okhotnik-B Stealth Drone Is a Big Problem for NATO," *The National Interest*, The Center for the National Interest, August 28, 2021, https://nationalinterest.org/blog/reboot/russia%E2%80%99s-okhotnik-b-stealth-drone-big-problem-nato-192701.

autonomous technology. This long-endurance drone answers the United States' RQ-4 Global Hawk. It retains the ability to fly fully autonomous and perform reconnaissance missions, strike capabilities, and electronic attacks.[102] Other drones are slotted for more conventional roles or "predator-style" attack systems. The Orion drone allegedly has a system that can shoot down another drone, introducing the idea of drone-style dogfights.[103] Russia, its competitors, and its peers are likely responding by researching and developing their variation of drones

Russia used drones when it annexed the Crimean Peninsula in 2014, supporting pro-Russian separatist forces. Russia supplied the separatist forces with equipment and UAVs in the conflict. Separatist forces found initial success in using small intelligence, surveillance, and reconnaissance (ISR) UAVs against Ukrainian forces, who were lacking in the number and utilization of UAVs. The separatist forces also used drones to draw fire from concealed Ukrainian forces, giving away their positions. The greatest tactical and strategic use of the UAVs have been as ISR platforms that allow separatist forces to coordinate artillery strikes and ground assaults.[104] Before drones, forward observers were needed to acquire targets visually, radio over the coordinates, and adjust artillery fire.

Nevertheless, modern drone technology has innovative targeting acquisition that can accurately direct rocket artillery fire, with devastating results. Such was the case when Russian-backed forces attacked a group of Ukrainian ground forces on July 11, 2014, near the village Zeleopillya, extracting a large toll of casualties and equipment. Pro-Russian forces preemptively attacked with the support of reconnaissance drones buzzing overhead. These drones coordinated artillery strikes on Ukrainian positions as the ground forces seized and secured territory.[105] Separatist forces used these techniques again in January 2015 against the city of Debaltseve. A pro-Russian separatist force began besieging the city against the entrenched Ukrainian forces. Russian-backed forces used UAVs to support and adjust artillery fire throughout the battle, with devastating results as Ukrainian and civilian casualties continued to mount. These sophisticated techniques have

---

[102] "Russia's Top Long-Range Attack Drones," *Airforce Technology* (blog), November 27, 2020, https://www.airforce-technology.com/features/russias-top-long-range-attack-drones/.

[103] David Hambling, "Russia Reveals New Drone Capabilities, Hinting at What It Could Bring to Bear in Ukraine," *Forbes*, December 23, 2021, https://www.forbes.com/sites/davidhambling/2021/12/23/russia-reveals-new-drone-precision-bomber-dogfighter-and-more/?sh=7dcb59732252.

[104] Douglas Barrie et al., "Armed Uninhabited Aerial Vehicles and the Challenges of Autonomy," International Institute for Strategic Studies, accessed January 12, 2022, https://www.iiss.org/blogs/research-paper/2021/12/armed-uninhabited-aerial-vehicles-and-the-challenges-of-autonomy.

[105]Amos Fox, "The Russian–Ukrainian War: Understanding the Dust Clouds on the Battlefield," Modern War Institute, January 17, 2017, https://mwi.usma.edu/russian-ukrainian-war-understanding-dust-clouds-battlefield/.

extracted heavy casualties on Ukrainian forces.[106] Understanding the strategic significance of such capabilities, Ukraine began to increase its arsenal to a comparable level of UAVs.[107] Both sides continue to deploy UAVs, predominantly in an Intelligence, Surveillance, and Reconnaissance (ISR) role.

Another example of Russian drone use is in Syria. Russia has remained a steadfast ally of the Assad regime in Syria, and Russia is directly challenging NATO in this region and shows no signs of resigning. The Russo-Syrian alliance has allowed Russia to deploy its troops and equipment to the region. These deployments have allowed Russian forces to develop combat experience and test equipment against an active enemy force. Russian UAVs were pivotal to the Assad regime in fighting the ISIS caliphate, which established control over a large portion of the country. Russian bombing campaigns and real-time UAV surveillance were instrumental in the Syrian Army's recapture of Palmyra and Aleppo in 2016.[108] Russian UAVs in Syria have been used as an ISR platform, enabling up-to-date aerial surveillance, battle damage assessments, and as a forward observation to adjust Russian and Syrian artillery strikes.[109] This conflict has seen Russian equipment pitted directly against Turkish capabilities in the region.[110]

The war between Azerbaijan and Armenia in 2020 also saw wide-scale use of drones and autonomous weapons. The depth and scope of drone usage proved critical in determining the war's outcome. Azerbaijan quickly dominated the drone warfare campaign with effective and superior technology and application. Turkey supplied most of the Azerbaijani drones that devastated Armenian defenses. Azerbaijan used drones to provide ground forces with air support and ISR capabilities.[111] Key takeaways in the Nagorno-Karabakh conflict stress the importance of drones in warfare and the wide range of uses.

The steady increase in the availability and sophistication of autonomous weapons will continue to threaten key critical infrastructure systems. In September of 2019, the Iranian-backed Houthi organization claimed responsibility for a drone attack that targeted oil processing facilities owned and operated by Saudi Aramco. The damage cut Saudi oil production by half and destabilized global financial

---

[106]Randy Noorman, "The Battle of Debaltseve: A Hybrid Army in a Classic Battle of Encirclement," *Small Wars Journal*, July 17, 2020, https://smallwarsjournal.com/jrnl/art/battle-debaltseve-hybrid-army-classic-battle-encirclement#_ftn63.

[107] Barrie et al., "Armed Uninhabited Aerial Vehicles."

[108] Anton Lavrov, "The Russian Air Campaign in Syria: A Preliminary Analysis" (Arlington VA: The Center of Naval Analyses, June 2018), https://apps.dtic.mil/sti/pdfs/AD1057649.pdf.

[109] Samuel Bendett et al., "Improvisation and Adaptability in the Russian Military," Center for Strategic and International Studies, April 2020, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200430_Mankoff_Russian%20Military_web_v3_UPDATED%20FINAL.pdf?w8E_tmNl65QbUPtiv6FomIF5U7yGzqBl.

[110] Barrie et al., "Armed Uninhabited Aerial Vehicles."

[111] IISS, "Armed Uninhabited Aerial Vehicles."

markets. The attack is testament to the danger autonomous weapons pose to key infrastructure.[112] This attack highlights the need for NATO to encourage sustained, innovative resilience-building operations.

These case studies display the increasing use and efficiency of autonomous weapons. The Syrian and the Ukrainian conflicts showcase Russia's drone technology, and the Nagorno-Karabakh conflict highlights drones' devastating and strategic implications for conventional warfare. The Abqaiq attack displayed the vulnerability of energy infrastructure and the ease with which state and non-state actors can use autonomous weapons to exploit those vulnerabilities. Some NATO countries are still actively involved in global counterterrorism efforts. Given the political climate after the Russian invasion of Ukraine, there remains a driving force necessitating the advancement and application of autonomous weapons.[113]

As shown in these conflicts, autonomous weapons platforms and monitoring systems are strategically important factors in operational success. Systems could be put into place to monitor incursions into airspace accurately. Pilots would no longer risk their lives, reducing the human cost of conflict. This increases long-term operational integrity and secures political and social backing for any military endeavor.[114] Integrating UACs can also fulfill the role of an Airborne Warning and Control System (AWACS) while keeping human lives out of harm's way. This system bolsters the resilience of early warning and combat air control systems by replacing a few vulnerable planes with a host of autonomous aerial relays.[115] Both air defense and offensive networks stand to benefit from the integration of autonomous technologies, and drones can negate numerical and technological disadvantages in the battlespace.

Current measures such as the Counter-Rocket, Artillery, Mortar (C-RAM), and Iron Dome System have shown limited success in intercepting autonomous weapons. Both operate by utilizing a system-of-systems program that identifies incoming threats. The Iron Dome fires rockets as an interceptor, and the C-RAM fires 4,500 20mm rounds per minute from a minigun to intercept the projectile.[116]

---

[112] Thomas Warrick, "What the Abqaiq Attack Should Teach Us About Critical Infrastructure," *Atlantic Council* (blog), September 18, 2019, https://www.atlanticcouncil.org/blogs/menasource/what-the-abqaiq-attack-should-teach-us-about-critical-infrastructure/.

[113] NATO, "Countering Terrorism."

[114] Amy Zegart, "Cheap Fights, Credible Threats: The Future of Armed Drones and Coercion," *Journal of Strategic Studies* 43, no. 1 (January 2, 2020): 6–46, https://doi.org/10.1080/01402390.2018.1439747.

[115] Zegart, "Cheap Fights, Credible Threats."

[116] "How Israel's Iron Dome Missile Shield Works," *BBC News*, May 17, 2021, sec. Middle East, https://www.bbc.com/news/world-middle-east-20385306; US Army, "Counter-Rocket, Artillery, Mortar (C-RAM) Intercept Land-Based Phalanx Weapon System (LPWS)," *US Army Acquisition Center* (blog), accessed February 24, 2022, https://asc.army.mil/web/portfolio-item/ms-c-ram_lpws/.

NATO can consider adopting these systems to scale around critical infrastructure. Though effective, it is vital that these systems be consistently tested and updated to stay up to date in the fast-paced world of technology. The private and public sectors of defense and science continue to look at alternatives such as the Electromagnetic Pulses (EMP), which enable greater protection from drone attacks. The United States and China have developed EMP technology capable of disarming drones without kinetic force.[117] The energy surge caused by the EMP disrupted the functionality of the drones and caused them to crash. This technology can prove vital in protecting critical infrastructure from adversaries during events such as drone swarming, targeting, and loitering munitions.

Russian and Chinese autonomous weapons are serious threats to NATO. These drones can serve both offensive and intelligence purposes. With potential adversaries developing this technology, NATO countries must protect themselves and their critical infrastructure. Without further developing its own autonomous offensive and defensive capabilities, NATO will soon lose its strategic advantage in autonomous technology.

Policy recommendations

We recommend NATO's Science and Technology Organization (STO) and Science for Peace and Security (SPS) Programme promote research into defenses against autonomous weapons to increase security and defend critical infrastructure. Several STO technological projects show promise in the defense against drones. One project, the Allied Future Surveillance and Control initiative, allows NATO to monitor the airspace over allied nations.[118] A second program, the Autonomy for Anti-Submarine Warfare program, creates secure communication between autonomous systems onboard submarines to counter nautical threats.[119] Lastly, UAV radar (SET-245) development aims at upgrading counter UAV radar systems by improving their detection, classification, and identification capabilities.[120] Counter-Rocket, Artillery, and Mortar (C-RAM) systems effectively integrate discrete sensor systems to detect incoming threats.[121]

We recommend NATO establish an early warning system-of-systems against emerging threats, connecting multiple existing autonomous systems. This

[117] Marie Morales, "Electromagnetic Pulse Used in Chinese Weapon Can Take Down Unmanned Aircraft; Field Test Aims to Catch Up With US," *Science Times,* August 27, 2021, https://www.sciencetimes.com/articles/33096/20210827/electromagnetic-pulse-used-chinese-weapon-take-down-unmanned-aircraft-field.htm.
[118] NATO, "NATO Science and Technology Organization [STO]," *NATO Newsroom,* accessed September 21, 2021, https://www.nato.int/cps/en/natohq/topics_88745.htm.
[119] NATO, "NATO STO."
[120] NATO, "NATO STO."
[121] US Army, "Counter-Rocket, Artillery, Mortar."

system-of-systems, much like C-RAM systems, would combine the above technologies to defend against autonomous weapons on a large scale. This system-of-systems would supplant NATO's existing Airborne Warning & Control System fleet and would need to be paired with physical interceptors.[122] The NATO Science for Peace and Security Programme can fund anti-drone technology-specific grants for projects like those described above. With these investments into emerging autonomous weapon technology for offensive and defensive purposes, NATO countries would be able to secure their borders more effectively and protect their critical infrastructure from adversaries.

[122] NATO, "AWACS–NATO's 'eye in the sky,'" *NATO Newsroom*, August 30, 2021, https://www.nato.int/cps/en/natohq/topics_48904.htm.

Selected Bibliography

Airbus. "The Future Combat Air System (FCAS)." Accessed February 9, 2022. https://www.airbus.com/en/products-services/defence/multi-domain-superiority/future-combat-air-system-fcas.

Anderson, James M., Benoit Arbour, Roberta Arnold, Thomas Kadiofsky, Tom Keely, Matthew R. MacLeod, Sean Bourdon, Rebecca Crootof, John Matsumara, Chris Mayer, Mark Roorda, Pertti Saariluoma, Paul Scharre, Brandon Suarez, Christopher Sulzbachner, Erik Theunissen, Andreas Tolk, Andrew Williams, and Christian Zinner. "Autonomous Systems: Issues for Defence Policymakers." Norfolk, VA: NATO Supreme Allied Command Transformation, September 30, 2015. https://apps.dtic.mil/sti/pdfs/AD1010077.pdf.

Antebi, Liran. "Changing Trends in Unmanned Aerial Vehicles: New Challenges for States, Armies and Security Industries." Issue 6, no. 2 (2014).

Barrie, Douglas, Niklas Ebert, Oskar Glaese, and Franz-Stefan Gady. "Armed Uninhabited Aerial Vehicles and the Challenges of Autonomy." International Institute for Strategic Studies, accessed January 12, 2022. https://www.iiss.org/blogs/research-paper/2021/12/armed-uninhabited-aerial-vehicles-and-the-challenges-of-autonomy.

Bendett, Samuel, Stephen Blank, Joe Cheravitch, Michael B. Petersen, and Andreas Turunen. "Improvisation and Adaptability in the Russian Military." Center for Strategic and International Studies, April 2020. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200430_Mankoff_Russian%20Military_web_v3_UPDATED%20FINAL.pdf?w8E_tmNl65QbUPtiv6FomIF5U7yGzqBl.

Eckstein, Megan. "Sonar Equipped Drone Fleets Could Be Key to Future Submarine Warfare." *USNI News* (blog), March 9, 2020. https://news.usni.org/2020/03/09/sonar-equipped-drone-fleets-could-be-key-to-future-submarine-warfare.

Fox, Amos. "The Russian–Ukrainian War: Understanding the Dust Clouds on the Battlefield." Modern War Institute, January 17, 2017. https://mwi.usma.edu/russian-ukrainian-war-understanding-dust-clouds-battlefield/.

Gokhberg, Leonid, Alexander Sokolov, and Alexander Chulok. “Russian S&T Foresight 2030: Identifying New Drivers of Growth.” *Foresight* 19, no. 5 (January 1, 2017): 441–56. https://doi.org/10.1108/FS-07-2017-0029.

Hambling, David. “Russia Reveals New Drone Capabilities, Hinting at What It Could Bring to Bear in Ukraine.” *Forbes*, December 23, 2021. https://www.forbes.com/sites/davidhambling/2021/12/23/russia-reveals-new-drone-precision-bomber-dogfighter-and-more/?sh=7dcb59732252.

Joint Air Power Competence Centre (JAPCC). “A Comprehensive Approach to Countering Unmanned Aircraft Systems.” Kalkar, DE: JAPCC, December 17, 2020. https://www.japcc.org/portfolio/c-uas/.

Kallenborn, Zachary. “Applying Arms-Control Frameworks to Autonomous Weapons.” *Brookings* (blog), October 5, 2021. https://www.brookings.edu/techstream/applying-arms-control-frameworks-to-autonomous-weapons/.

Lavrov, Anton. “The Russian Air Campaign in Syria: A Preliminary Analysis.” Arlington, VA: The Center of Naval Analyses, June 2018. https://apps.dtic.mil/sti/pdfs/AD1057649.pdf.

Morales, Marie. “Electromagnetic Pulse Used in Chinese Weapon Can Take Down Unmanned Aircraft; Field Test Aims to Catch Up With US.” *Science Times,* August 27, 2021. https://www.sciencetimes.com/articles/33096/20210827/electromagnetic-pulse-used-chinese-weapon-take-down-unmanned-aircraft-field.htm.

NATO. “NATO Science and Technology Organization [STO],” *NATO Newsroom*, accessed September 21, 2021. https://www.nato.int/cps/en/natohq/topics_88745.htm.

NATO. “Autonomous Military Drones: No Longer Science Fiction.” *NATO Review*, July 28, 2017. https://www.nato.int/docu/review/articles/2017/07/28/autonomous-military-drones-no-longer-science-fiction/index.html.

NATO. “DEEP - Counter-Terrorism Reference Curriculum.” *NATO Newsroom*, September 30, 2020. https://www.nato.int/cps/en/natohq/topics_176310.htm.

NATO. "AWACS–NATO's 'eye in the sky.'" *NATO Newsroom*, August 30, 2021. https://www.nato.int/cps/en/natohq/topics_48904.htm.

NATO. "Countering Terrorism." *NATO Newsroom*, September 14, 2021. https://www.nato.int/cps/en/natohq/topics_77646.htm.

NATO. "The Partnership Action Plan against Terrorism (PAP-T) (Archived)." April 13, 2021. https://www.nato.int/cps/en/natohq/topics_50084.htm.

Oh, Donggeun, and Junghee Han. "Smart Search System of Autonomous Flight UAVs for Disaster Rescue." *Sensors* 21, no. 20 (October 15, 2021): 6810–6810. https://doi.org/10.3390/s21206810.

Reding, D.F., and J. Eaton. *Science & Technology Trends 2020-2040*. Brussels, BE: NATO Science & Technology Organization, March 2020.

Romasheva, Natalia, and Diana Dmitrieva. "Energy Resources Exploitation in the Russian Arctic: Challenges and Prospects for the Sustainable Development of the Ecosystem." *Energies* 14, no. 24 (December 15, 2021): 8300. https://doi.org/10.3390/en14248300.

Siebold, Sabine, and Philip Blenkinsop. "EU Tightens Russian Sanctions and Buys Weapons for Ukraine." *Reuters*, February 27, 2022. https://www.reuters.com/world/europe/eu-close-airspace-russia-curb-media-target-belarus-2022-02-27/.

Tian, Nan and Su, Fei. "An Estimate of China's Military Expenditure." *SIPRI*. January 2021. https://www.sipri.org/sites/default/files/2021-01/2101_sipri_report_a_new_estimate_of_chinas_military_expenditure.pdf.

US Army. "Counter-Rocket, Artillery, Mortar (C-RAM) Intercept Land-Based Phalanx Weapon System (LPWS)." *US Army Acquisition Center* (blog), accessed February 24, 2022. https://asc.army.mil/web/portfolio-item/ms-c-ram_lpws/.

US Department of Defense. "DOD Releases Fiscal Year 2021 Budget Proposal." Accessed February 13, 2022. https://www.defense.gov/News/Releases/Release/Article/2079489/dod-releases-fiscal-year-2021-budget-proposal/.

Valasek, Tomas. “What Does the War in Georgia Mean for EU Foreign Policy?” Center for European Reform, 2008. https://www.cer.org.uk/publications/archive/briefing-note/2008/what-does-war-georgia-mean-eu-foreign-policy.

Zegart, Amy. “Cheap Fights, Credible Threats: The Future of Armed Drones and Coercion.” *Journal of Strategic Studies* 43, no. 1 (January 2, 2020): 6–46. https://doi.org/10.1080/01402390.2018.1439747.

Chapter 5: Hypersonic Weapons

By: Lucas Cox, Samuel Lavey, Sydney Winstead, and Yanchen Wu

The development of hypersonic technologies has brought threats and opportunities to NATO. Russia and China both developed hypersonic strike capabilities that can avoid the Alliance's north-facing defense systems. With the potential of inflicting severe damage to NATO allies' critical infrastructure, these hypersonic weapons are significantly shifting the security landscape in Eurasia and Asia-Pacific toward NATO adversaries' advantages. Therefore, it is important that NATO partner states increase hypersonic technology funding to develop robust offensive and defensive capabilities.

The state of hypersonic weapons

Hypersonic weapons are missiles, vehicles, and aircraft that are highly maneuverable systems and can travel faster than Mach 5—five times the speed of sound.[1] The emergence of hypersonic weapons creates opportunities for NATO military expansion while also presenting immense vulnerabilities and implications for international security. Nevertheless, there is no Alliance-wide NATO posture on hypersonic weapons, their development, or unified defense against hypersonic threats.

Notably, hypersonic weapons pose a considerable risk to NATO critical infrastructure. Critical infrastructure such as missile silos, naval fleets, defense systems, and civil infrastructure is more vulnerable to an inexorable hypersonic strike than a traditional Intercontinental Ballistic Missile (ICBM). Their speed, detection evasion, and kinetic power make hypersonic weapons difficult to intercept with current technology. Although critical infrastructure protection is not the primary purpose of hypersonic weapons development, hypersonic missiles could be used for defense purposes such as intercepting high-value or high threat time-critical targets.[2]

NATO allies are trailing Russia and China in the development of hypersonic capabilities.[3] Russia's development and deployment of hypersonic weapons threaten NATO on a level not seen since the Cold War. Russia's development of hypersonic weapons, both conventional and nuclear, serves its long-standing geopolitical goal of deterring the West, considering NATO's robust missile defense

[1] D.F. Reding and J. Eaton, *Science & Technology Trends 2020-2040* (Brussels, BE: NATO Science & Technology Organization, March 2020), 86-87.
[2] Reding and Eaton, *Science & Technology Trends*, 90.
[3] Jessica Cox, "Nuclear Deterrence Today," *NATO Review*, June 08, 2020, https://www.nato.int/docu/review/articles/2020/06/08/nuclear-deterrence-today/index.html.

and conventional superiority. To keep up with changing security dynamics and adapt to technological developments, the Russian Federation has heavily modernized both its conventional and nuclear forces to "dissuade [the US] from pursuing comprehensive missile defense systems by developing weapons that could puncture those defenses."[4]

China's pursuit of hypersonic weapons has also become a NATO concern, as it might shift the security landscape that the United States, NATO's leading power, faces in the Asia-Pacific. By developing hypersonic vehicles equipped with nuclear warheads, Beijing seeks to deter the United States from interfering in portions of the Eastern Pacific that it sees as a privileged sphere of influence.[5]

Russia, China, and Western allies are currently developing two types of hypersonics: hypersonic glide vehicles (HGV) and hypersonic cruise missiles (HCM). HGVs are launched briefly into orbit by existing missile technology and glide toward their target at hypersonic speeds. HCMs fly at lower altitudes and reach hypersonic speed with an airbreathing jet engine or scramjet. HGVs are mostly being considered in a strategic context, with most states arming them with nuclear warheads. Unlike current strategic missiles, HGVs are highly maneuverable in all stages of flight. In combination with their speed, this trait allows them to evade detection and engagement by missile defense systems.[6]

These weapons play an important role in NATO's strategic narrative of allies' critical infrastructure. Both Chinese and Russian HGVs carry nuclear payloads or conventional payloads indistinguishable from nuclear warheads.[7] Strategic hypersonic weapons could cause mass casualties and disrupt the continuity of government if NATO lacked defense capabilities. Not only do HGVs require a much shorter defensive response time due to their speed, but they are maneuverable once detached from their first stage. These factors render much of NATO's early warning, tracking, and missile defense systems impotent. HGVs also fly at higher altitudes, making them harder to detect with existing radar. There is also the possibility of HGV traveling over the South Pole, completely dodging NATO North Pole missile defense.[8]

Hypersonic cruise missiles are more likely to be used in sub-strategic arsenals. These missiles exploit critical infrastructure vulnerabilities, as HCMs are

---

[4] Edward Geist and Dara Massicot, "Understanding Putin's Nuclear 'Superweapons,'" *The SAIS Review of International Affairs* 39, no. 2 (2019): 103-17.

[5] Alan Cummings, "Hypersonic Weapons: Tactical Uses and Strategic-Goals," War on the Rocks, November 12, 2019, https://warontherocks.com/2019/11/hypersonic-weapons-tactical-uses-and-strategic-goals/.

[6] Reding and Eaton, *Science & Technology Trends,* 87.

[7] Alan Cummings, "Hypersonic Weapons."

[8] Jeffrey Smith, "Hypersonic Missiles Are Unstoppable. And They're Starting a New Global Arms Race," *New York Times*, October 27, 2021, https://www.nytimes.com/2019/06/19/magazine/hypersonic-missiles.html.

more tactically available than HGVs. The missiles' kinetic energy causes more serious damage without being nuclear, lowering the threshold of a hypersonic strike.[9] Their hypersonic speed makes them more effective at penetrating targets, and they are more maneuverable at high speeds in all stages of flight. This capability makes HCMs more effective, harder to track, and nearly impossible to intercept compared to currently deployed cruise missiles such as the Tomahawk.[10] Hypersonic cruise missiles can destroy mission-vital infrastructure (including missile defenses and forward-deployed weapons) and critical national infrastructure (including energy, transportation, and communications networks).

The development of hypersonic weapons varies greatly in different countries. The projects of hypersonic development are rooted largely in the historical desire for full security from adversarial world powers. The Russian Federation claims to have created hypersonic weapons to gain the upper hand in deterring NATO and the United States' strategic capabilities, while China claims it built hypersonic missiles to counter Western threats to its sphere of influence.[11] The United States and other allied nuclear powers allies have mainly focused on hypersonics in research, commercial, and civilian contexts. This focus has allowed Russia and China to gain the upper hand in offensive weapons technologies.[12] Additionally, treaties put in place before the development of these weapons, the New START particularly, had loopholes that allowed for the uncontrolled development and deployment of hypersonic weapons. The emergence of hypersonic weapons creates opportunities for enhancing NATO resilience while also presenting immense vulnerabilities and implications for international security. The opportunities of hypersonic created include the development of more resilient missile defense systems, more adaptable weapons systems, and dual-use applications that may aid in manned missions to Mars and beyond. The principal vulnerability presented is shifting the paradigm of nuclear deterrence, as Russian and Chinese hypersonic weapons can circumvent current Allied missile detection and defense systems through speed, maneuverability, and endurance. With this is mind, this Task Force finds it important to analyze current hypersonic Russian and Chinese hypersonic capabilities.

The Russian Avangard HGV was designed for long-range strategic nuclear purpose. Avangard, carried into orbit by an ICBM, was deployed and is operational

---

[9] Kelley M. Sayler, *Hypersonic Weapons: Background and Issues for Congress*, Congressional Research Service (CRS) Report R45811 (Washington, DC: CRS, October 19, 2021), 3, https://sgp.fas.org/crs/weapons/R45811.pdf

[10] Sayler, *Hypersonic Weapons*, 17.

[11] John Borrie, Amy Dowler, and Pavel Podvig, "Hypersonic Weapons: A Challenge and Opportunity for Strategic Arms Control," UN Institute for Disarmament Research, February 14, 2019, 16, https://unidir.org/publication/hypersonic-weapons-challenge-and-opportunity-strategic-arms-control.

[12] Sayler, *Hypersonic Weapons*, 1.

as of 2020. The Avangard HGV can attack targets over 6,000 km away with either a nuclear or conventional payload. The glide vehicle detaches from the rocket upon reaching its highest point (roughly 100 km), thereafter cruising down towards its target through the atmosphere.[13] Reports indicate that Avangard is deployed on the SS-19 Stiletto ICBM, though Russia plans to deploy the vehicle atop the Sarmat ICBM. Kinzhal, which can carry conventional or nuclear warheads, was designed to destroy NATO missile defense systems and warships in the opening salvoes of a large-scale conflict. The 3M22 Zircon HCM is predicted to be in service before 2025, is highly maneuverable, and can reportedly use plasma stealth and sea-skimming to evade interception. Zircon can strike both ground and naval targets at a range of 250 to 600 miles in a matter of minutes.[14]

For instance, while at sea, any of Russia's 15 Buyan-class corvettes will be able to carry up to 25 Tsirkon hypersonic missiles. Even a few of these missiles could sink advanced American aircraft carriers.[15] Also, if launched from the Gulf of Finland, an air-launched Kinzhal HGV can travel at Mach 10 and hit Sofia within 11 minutes. It could reach London, Paris, or Rome in comparable time. Put differently, a target 1,200 miles away from a hypersonic weapon would be warned of an incoming hypersonic missile at the same time as a "target within roughly 100 miles of a subsonic cruise missile."[16]

China has similarly deployed its DF-ZF HGV for long-range use with a nuclear warhead. This hypersonic capability affords Beijing more options for simultaneously striking ships at sea, forces ashore, and command functions using a deceptively routine force posture. China's system is believed to be more advanced than its Russian counterpart, and its most recent test included a Fractional Orbital Bombardment System (FOBS). China's HGV program includes the DF-17, a medium-range ballistic missile specifically designed to launch the DF-ZF HGV. This strategic deployment concerns NATO, as NATO recently declared China a global security problem that is important to address.[17] In a recent test, a DF-ZF hypersonic glide vehicle operating at Mach 15 reportedly hit its target at 1,500 miles under 9 minutes. This test indicates that Chinese forces could position their launchers to target anywhere in the Pacific region with near-instantaneous strikes.

---

[13] Center for Strategic and International Studies Missile Defense Project (CSIS MDP), "Avangard," *Missile Threat*, January 3, 2019, https://missilethreat.csis.org/missile/avangard/.
[14] Sayler, *Hypersonic Weapons*, 12-13.
[15] Prakash Nanda, "BrahMos-II Missile Program to Greatly Benefit from The Successful Test of Russian Zircon Hypersonic Missile," *EurAsian Times*, July 22, 2021, https://eurasiantimes.com/category/expert-reviews/.
[16] Alan Cummings, "Hypersonic Weapons."
[17] Stephen Erianger and Michael D. Shear, "Shifting Focus, NATO Views China as a Global Security Challenge," *New York Times*, June 14, 2021, https://www.nytimes.com/2021/06/14/world/europe/biden-nato-china-russia.html.

China's goal in testing these new weapons is to demonstrate the risk to the United States of interfering with its regional interests.[18]

Beyond missiles, long-range intelligence, surveillance, and reconnaissance (ISR) are other potential applications of hypersonic technologies. Yet, no country currently has programs of human-crewed hypersonic reconnaissance aircraft. On the other hand, hypersonic unmanned aerial vehicles (UAVs) are capable of weapon delivery in addition to long-range ISR. Hypersonic UAVs allow the mission to be more flexible than reconnaissance satellites.[19]

The United States has shifted its focus to defensive uses of hypersonic weapons. There is still the concern, however, that current US and NATO systems cannot engage effectively with hypersonic threats. To date, the United States has heavily invested in defenses against conventional missiles. For example, the United States can shoot down ICBM threats with its Terminal High Altitude Area Defense system (THAAD). This system can intercept missiles at almost any altitude due to its transportability and rapid deployment.[20] Another component of American missile defense is the Aegis Missile System. This system is deployed on US destroyers around the globe. This versatile sea-based can shoot down short to medium-range missiles.[21] Russia's hypersonic missile development directly responds to these American missile defense systems. Importantly, hypersonic weapons render these current missile defense systems obsolete.[22] This inability to effectively detect and engage a hypersonic threat from Russia constitutes a great security vulnerability to NATO, its warfighting ability, and allied critical infrastructure.

Hypersonics and arms control treaties

International arms agreements have historically impacted the use and development of hypersonic technologies. Russia and the United States have been part of several such agreements that have severely limited strategic capabilities. These treaties include the Intermediate Nuclear Forces Treaty (INF), the Anti-Ballistic Missile Treaty (ABM), and the New START Treaty. The ABM Treaty prohibited missiles whose ranges exceeded 3,500 kilometers and velocities

[18] Alan Cummings, "Hypersonic Weapons."
[19] Reding and Eaton, *Science & Technology Trends,* 90.
[20] Michael Tuttle, "DLA Fuels THAAD Deployment to Romania, Helps Maintain Missile Defense," *US Defense Logistics Agency,* October 15, 2019, https://www.dla.mil/AboutDLA/News/NewsArticleView/Article/1989005/dla-fuels-thaad-deployment-to-romania-helps-maintain-missile-defense/.
[21] Tuttle, "DLA Fuels THAAD."
[22] Zachary Keck, "Will Hypersonic Capabilities Render Missile Defense Obsolete?," *The Diplomat,* February 07, 2014, https://thediplomat.com/2014/02/will-hypersonic-capabilities-render-missile-defense-obsolete/.

exceeded five kilometers per second. The ABM Treaty also aimed to put restrictions on missile defense systems, bringing an end to the Cold War-era arms race by preventing defense strategies that would render offensive nuclear capabilities ineffective. [23]

Without an international ruling body, arms control agreements and treaties can be hard to enforce and keep participating states accountable. Signatories have the unilateral ability to withdraw from treaties, as seen with the exit of the U.S. from the ABM Treaty. This action furthered the US's goal of developing a national nuclear defense system, which the ABM prohibited.[24] Since withdrawing, the United States has spent billions of dollars on systems that can detect, track, and shoot down an incoming ICBM in thirty minutes or less.[25] These multicomponent systems could theoretically shoot down any ICBM in the world.

The New START agreement was the latest attempt to address growing concerns between the United States and Russia. New START effectively replaced older strategic arms control agreements between the United States and Russia. Within the treaty, both countries agree to limit the number of deployed nuclear warheads, nuclear-capable bombers, ICBMs, and Submarine-Launched Ballistic Missiles (SLBM).[26] Each country is allowed eighteen inspections at the other countries' nuclear devices and facilities as stated within the treaty.[27] Nevertheless, the parties omitted hypersonic weapons from the New START negotiations, partially due to a lack of testing and respective national interests in developing hypersonic technology.[28] It remains uncertain whether the New START Treaty will be renewed and address hypersonic capabilities.

Conclusions

The development of hypersonic technologies presents threats and opportunities to NATO allies. Both Russia and China have successfully advanced their hypersonic weapon projects. With the potential of inflicting serious damage to NATO allies' critical infrastructure, these weapons serve Russia's and China's long-term goal of shifting the security landscape. Russia's development of hypersonic weapons is an important part of a greater strategy of shifting the balance

[23] "Treaty Between the United States of America and the Union of Soviet Socialist Republics on The Limitation of Anti-Ballistic Missile Systems (ABM Treaty)," signed May 26, 1972, https://2009-2017.state.gov/t/avc/trty/101888.html.
[24] "ABM Treaty."
[25] Jon A. Hill and Michelle C. Atkinson, "Department of Defense Press Briefing on the President's Fiscal Year 2022 Defense Budget for the Missile Defense Agency," Transcript, US Department of Defense, May 28, 2021; "ABM Treaty."
[26] US Department of State (DOS), "New START Treaty," www.state.gov/new-start/.
[27] US DOS, "New START Treaty."
[28] US DOS, "New START Treaty."

of the deterrence regime developed in the context of the Cold War. Russia now sees its superior strategic capabilities as the ultimate deterrent to both its assured destruction in the event of a large-scale nuclear conflict, as well as its ability to freely intervene military in the affairs of its neighbors without interference. In his speech outlining the Russian invasion of Ukraine, President Vladimir V. Putin touted the Russian Federation's "modern nuclear force components" to dissuade the NATO from intervening in the conflict.[29] By comparison, China prioritizes the development of HGVs to deter the United States from interfering in portions of the Western Pacific that it sees as within its sphere of influence.

NATO has a prominent role to play in addressing significant vulnerabilities to match its would-be adversaries' abilities safely and effectively. Possession of advanced hypersonic weapons across nuclear states leads experts to believe that leaders could more seamlessly and brazenly escalate conflict following a crisis.[30] Warhead ambiguity, a major concern in the deployment of hypersonic glide vehicles, is also a large risk.

Thus, surges in emerging technology undoubtedly provide ground for nuclear allied states to build and research in line with one another while allowing smaller, non-nuclear states to aid in research and technology.[31] Current challenges include reducing R&D costs, developing and refining satellite networks for detecting incoming hypersonic threats, and missile defense capable of engaging them. Producing hypersonic defenses also helps NATO allies understand how to counter the technology itself. While the decision to move forward in hypersonic weapon development is controversial, the need for a "resilient and persistent space sensor layer capable of observing, classifying, and tracking missile threats of all types, azimuths, and trajectories" should remain central to NATOs position, creating a foundational base of security.[32]

In an increasingly disruptive security environment, we recommend NATO have a unified and comprehensive strategy to address all hypersonic threats to transatlantic. It would benefit the Alliance to develop a top-down strategy on how hypersonics are to be used in conflict, by whom, and for what explicit purposes. Additionally, NATO has unique opportunities to establish an alliance-wide hypersonic strategy that emphasizes civil-military cooperation.

The emergence of hypersonic missiles also raises new opportunities for NATO members and nuclear adversaries to formulate and sign a new treaty

---

[29] Sarah Starkey, "Putin reminds everyone that Ukraine joining NATO could lead to nuclear war," *Bulletin of the Atomic Scientists*, February 11, 2002, https://thebulletin.org/2022/02/putin-says-ukraine-membership-in-nato-would-make-nuclear-war-more-likely/.

[30] Erianger and Shear, "Shifting Focus."

[31] Vivienne Machi, "Where Does NATO Fit in the Global Hypersonic Contest?," *Defense News*, March 15, 2021, https://www.defensenews.com/global/europe/2021/03/15/where-does-nato-fit-into-the-global-hypersonic-contest/.

[32] Borrie, Dowler and Podvig, "Hypersonic Weapons," 3.

prohibiting the use and escalation of hypersonics. If NATO aims to maintain its long-standing posture of deterrence, possessing both offensive hypersonic capabilities and successful countermeasures is imperative.

Policy recommendations

As Russia and China develop increasingly advanced hypersonic weaponry, We recommend NATO make significant technological improvements to support operational coordination. Considering Chinese and Russian hypersonic capabilities and the United States' funding of a multi-billion-dollar research and development program in the offensive realm, NATO has a gap to fill in the development of defensive capabilities. *We therefore recommend NATO develop a doctrine for the deployment and development of hypersonic weaponry.* The United States, France, and Britain are deploying new hypersonic weapons, but these weapons are largely ungoverned.[33] Under this doctrine, NATO would also update its IAMD program, allowing it to detect and engage with hypersonic threats simultaneously.[34] Additionally, we recommend NATO refocus its IAMD system around the interception of incoming weapons at longer distances to protect against hypersonic missiles.

Under this doctrine, NATO would use the NATO Innovation Fund to fund a European Consortium on Hypersonics that includes national militaries, research universities, and industry partners. Creating a partnership to agree on the distribution of funding and responsibilities among member states would greatly reduce R&D costs, improve information sharing, and accelerate technological development in an area vital to resilience. Research would also allow non-nuclear allied states to contribute knowledge and could advance other technologies.[35] The development of hypersonic weapons also relies on cross-disciplinary efforts, and this can be reflected in the development of any new defensive or offensive capabilities. Importantly, the advancement of hypersonic technologies is inextricably linked to artificial intelligence (AI). For instance, while testing the hypersonic vehicle, AI could rapidly generate a hypersonic flight plan for human review and approval, significantly improving experiments' effectiveness.[36]

---

[33] Machi, "Where Does NATO Fit?"
[34] Richard Weitz, *Managing Multi-Domain and Hypersonic Threats to NATO* (Estonia: International Centre for Defense and Security, 2020), https://icds.ee/en/managing-multi-domain-and-hypersonic-threats-to-nato/.
[35] Sally Cole, "Hypersonic Missile Detection and Countermeasures Depend on Persistent Sensing," *Military Embedded Systems*, February 07, 2022, https://militaryembedded.com/radar-ew/sensors/hypersonic-missile-detection-and-countermeasures-depend-on-persistent-sensing.
[36] Sandia National Laboratories, "Future Hypersonics Could Be Artificially Intelligent," *Design World*, April 22, 2019, https://www.designworldonline.com/future-hypersonics-could-be-artificially-intelligent/.

Artificial intelligence is essential to defensive methods against incoming hypersonic strikes. Due to hypersonic weapons' high airspeed, interception requires AI-powered optical sensing.[37] While member states promote various AI and hypersonic projects, NATO plays an essential role in coordinating these efforts.[38] An effective NATO hypersonic weapons doctrine would therefore promote the advancement of foundational emerging technologies.

[37] Raymond S. Swanson and Kent R. Engebretson, "Artificial Intelligence and Hypersonic Weapons Drive Sensing, Fusion Research," *Aerospace America*, December 2019, https://aerospaceamerica.aiaa.org/year-in-review/artificial-intelligence-and-hypersonic-weapons-drive-sensing-fusion-research/.
[38] Machi, "Where does NATO fit?" March 15, 2021

Selected Bibliography

Borrie, John, Amy Dowler, and Pavel Podvig. “Hypersonic Weapons: A Challenge and Opportunity for Strategic Arms Control.” UN Institute for Disarmament Research, February 14, 2019. https://unidir.org/publication/hypersonic-weapons-challenge-and-opportunity-strategic-arms-control.

Center for Strategic and International Studies Missile Defense Project (CSIS MDP). "Avangard.” *Missile Threat*, January 3, 2019. https://missilethreat.csis.org/missile/avangard/.

Cox, Jessica. “Nuclear Deterrence Today.” *NATO Review,* June 08, 2020. https://www.nato.int/docu/review/articles/2020/06/08/nuclear-deterrence-today/index.html.

Erianger, Stephen, and Michael D. Shear. “Shifting Focus, NATO Views China as a Global Security Challenge.” *New York Times,* June 14, 2021. https://www.nytimes.com/2021/06/14/world/europe/biden-nato-china-russia.html.

Geist, Edward, and Dara Massicot. "Understanding Putin's Nuclear ‘Superweapons.’" *The SAIS Review of International Affairs* 39, no. 2 (2019): 103-17.

Hill, Jon A., and Michelle C. Atkinson. “Department of Defense Press Briefing on the President's Fiscal Year 2022 Defense Budget for the Missile Defense Agency.” Transcript, US Department of Defense, May 28, 2021.

Keck, Zachary. “Will Hypersonic Capabilities Render Missile Defense Obsolete?” *The Diplomat,* February 07, 2014. https://thediplomat.com/2014/02/will-hypersonic-capabilities-render-missile-defense-obsolete/.

Machi, Vivienne. “Where Does NATO Fit in the Global Hypersonic Contest?” *Defense News,* March 15, 2021. https://www.defensenews.com/global/europe/2021/03/15/where-does-nato-fit-into-the-global-hypersonic-contest/.

Nanda, Prakash. “BrahMos-II Missile Program to Greatly Benefit from The Successful Test of Russian Zircon Hypersonic Missile.” *EurAsian Times*, July 22, 2021. https://eurasiantimes.com/category/expert-reviews/.

Reding, D.F., and J. Eaton. *Science & Technology Trends 2020-2040.* Brussels, BE: NATO Science & Technology Organization, March 2020.

Sandia National Laboratories. “Future Hypersonics Could Be Artificially Intelligent.” *Design World*, April 22, 2019. https://www.designworldonline.com/future-hypersonics-could-be-artificially-intelligent/.

Sayler, Kelley M. *Hypersonic Weapons: Background and Issues for Congress*. Congressional Research Service (CRS) Report R45811. Washington, DC: CRS, October 19, 2021. https://sgp.fas.org/crs/weapons/R45811.pdf

Smith, Jeffrey. “Hypersonic Missiles Are Unstoppable. And They’re Starting a New Global Arms Race.” *New York Times*, October 27, 2021. https://www.nytimes.com/2019/06/19/magazine/hypersonic-missiles.html.

Simon, Steven. “Hypersonic Missiles Are a Game Changer.” *New York Times*, January 2, 2020. www.nytimes.com/2020/01/02/opinion/hypersonic-missiles.html.

Starkey, Sarah. “Putin reminds everyone that Ukraine joining NATO could lead to nuclear war.” *Bulletin of the Atomic Scientists*, February 11, 2002. https://thebulletin.org/2022/02/putin-says-ukraine-membership-in-nato-would-make-nuclear-war-more-likely/.

Tuttle, Michael. “DLA Fuels THAAD Deployment to Romania, Helps Maintain Missile Defense.” *US Defense Logistics Agency,* October 15, 2019. https://www.dla.mil/AboutDLA/News/NewsArticleView/Article/1989005/dla-fuels-thaad-deployment-to-romania-helps-maintain-missile-defense/.

“Treaty Between the United States of America and the Union of Soviet Socialist Republics on The Limitation of Anti-Ballistic Missile Systems (ABM Treaty).” Signed May 26, 1972, https://2009-2017.state.gov/t/avc/trty/101888.html.

US Department of Defense. “US to Deploy THAAD Missile Battery to South Korea.” *DoD News,* July 8, 2016. https://www.defense.gov/News/News-

Stories/Article/Article/831630/us-to-deploy-thaad-missile-battery-to-south-korea/.

US Department of State. *n.d.* "New START Treaty," www.state.gov/new-start/.

Weitz, Richard. *Managing Multi-Domain and Hypersonic Threats to NATO*. Estonia: International Centre for Defense and Security. https://icds.ee/en/managing-multi-domain-and-hypersonic-threats-to-nato/.

Stanley-Lockman, Zoe, and Edward Hunter Christie. "An Artificial Intelligence Strategy for NATO." *NATO Review*, October 25, 2021. https://www.nato.int/docu/review/articles/2021/10/25/an-artificial-intelligence-strategy-for-nato/index.html.

UN Office of Counter-Terrorism and UN Interregional Crime and Justice Research Institute. "Countering Terrorism Online with AI - an Overview for Law Enforcement." July 28, 2021. https://issuu.com/unicri/docs/countering_terrorism_online_with_artificial_intell.

US Army. "Strong Europe Tank Challenge." *7th Army Training Command*. https://www.7atc.army.mil/TankChallenge/.

US Cybersecurity Infrastructure and Security Agency. "ICS Alert (IR-Alert-H-16-056-01)." February 25, 2016. https://www.cisa.gov/uscert/ics/alerts/IR-ALERT-H-16-056-01.

US National Security Commission on Artificial Intelligence (NSCAI). "Final Report." Washington, DC: 2021. https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.

USAF College of Aerospace Doctrine, Research and Education (CADRE). "Three Levels of War," *Air and Space Power Mentoring Guide* 1. Maxwell AFB, AL: CADRE, 1997.

Weinstein, Emily. "China's Use of AI in its COVID-19 Response." CSET Data Brief, *CSET*, August 2020. https://cset.georgetown.edu/publication/chinas-use-of-ai-in-its-covid-19-response/.

Yang, Xiaozhe. “Accelerated Move for AI Education in China.” *ECNU Review of Education 2*, no. 3 (September 2019): 347–52. https://doi.org/10.1177/2096531119878590.

Zouave, Erik, Marc Bruce, Kajsa Colde, Margarita Jaitner, Ioana Rodhe, and Tommy Gustafsson. *Artificially Intelligent Cyberattacks*, Totalförsvarets forskningsinstitut (FOI) Report FOI-R--4947—SE. Stockholm, SE: FOI, March 2020. https://www.statsvet.uu.se/digitalAssets/769/c_769530-l_3-k_rapport-foi-vt20.pdf.

Conclusions and Cross-Discipline Policy Recommendations

Big data, artificial intelligence, autonomous weapons, and hypersonic weapons present NATO with opportunities and expose new vulnerabilities. These new threats are inevitable, constantly evolving, and unpredictable. Critical infrastructure is already vulnerable to a wide variety of threats, and potential adversaries' technological advances force NATO to shift its infrastructure protection priorities from prevention to resilience. Big data and AI, two foundational technologies, can revolutionize adversaries' intelligence operations and power advanced weaponry. China and Russia already have advanced autonomous weapons, but NATO defense systems are insufficiently integrated and unprepared for autonomous threats. Hypersonic weapons that can follow previously impossible trajectories similarly challenge traditional defense systems. Cultural attitudes, research and development funding, training, and regulation all impact the development and deployment of these technologies. Protecting critical infrastructure from these threats and enhancing NATO's own offensive capabilities requires an array of cross-discipline policy changes.

To rectify the growing threat of advanced cyberattacks on NATO critical infrastructure—including AI-enabled attacks, quantum decryption, and EMP attacks—we recommend that NATO develop redundant analog systems to support mission-vital infrastructure. As of 2019, one-third of businesses have experienced severe cyberattacks costing over $575 billion annually, illustrating the danger such an attack poses to NATO.[1] The threat of advanced cyberattacks will only continue to grow. It is vital that critical infrastructure therefore be able to operate independently of fragile networked systems.

NATO plays only a secondary role in protecting most critical infrastructure; the implementation of critical infrastructure resilience primarily falls on member states. NATO can nevertheless advocate for new redundancy standards by educating member states about the dangers of cyberattacks on critical infrastructure and the cost savings of protecting against a certain threat. NATO also has some more direct tools at its disposal, including the Industry Cyber Partnership, which promotes cybersecurity within private firms.[2] We recommend the NATO

[1] Piotr Lis and Jacob Mendel, "Cyberattacks on Critical Infrastructure: An Economic Perspective," *Economics and Business Review* 5, no. 2, (2019): 24-27, https://sciendo.com/pdf/10.18559/ebr.2019.2.2.
[2] NATO, "Cyber Defense," *NATO Newsroom*, July 2, 2021, https://www.nato.int/cps/en/natohq/topics_78170.htm.

Standardization Office also implement standards that promote analog backup systems for infrastructure crucial to NATO operations.[3]

This shift toward analog backups requires a comprehensive overview of critical infrastructure by NATO member states to ensure the operational integrity of critical infrastructure organizations. Current European infrastructure suffers from structural vulnerabilities that put the security of NATO partner states at risk. NATO allies, especially those in Europe, have no common standard for protecting critical national, mission-vital, and key infrastructure. Therefore, there are different levels of readiness and resilience across the Alliance, particularly relating to emergent threats. Furthermore, the private sector controls much of NATO's critical infrastructure, undermining resilience.

We therefore recommend NATO conduct annual security reviews of all allied mission-vital and key infrastructure, determine vulnerabilities, and mandate standards for individual partner states. Most importantly, this process would involve in-depth analysis of civilian and privately controlled infrastructure. We also recommend that NATO require member states to define their critical national infrastructure and conduct similar, more granular audits. This process would further clarify NATO's vulnerabilities and generate solutions to strengthen resilience against terrorism and peer adversaries. NATO can use the NATO Defense Planning Process (NDPP) to conduct these assessments, which would require funding increases.[4]

NATO does not have the legislative or legal means to mandate overarching standards for resilience; it can nevertheless play a leading role in advising EU legal standards on critical infrastructure resilience.[5] A joint process would mandate common NATO-EU standards for privately controlled critical infrastructure. Particularly, this could take the form of NATO performing a coordination role in data and cybersecurity programs, particularly in supervising foreign direct investment in critical infrastructure. NATO members are currently implementing unified standards to protect critical infrastructure, especially cybersecurity, from foreign interference. NATO can lead this process by integrating the methodologies, guidelines, committees, and planning groups under its Civil-Military Planning and Support Program and expanding its Euro-Atlantic Disaster Response Coordination Centre. Including the European Union and its legal frameworks—including the European Programme for Critical Infrastructure Protection (EPCIP)—would

[3] NATO, "NATO Standardization Office," *NATO Newsroom,* June 9, 2017, https://www.nato.int/cps/en/natohq/topics_124879.htm.

[4] Franklin D. Kramer, Lauren Speranza, and Conor Rodihan, "NATO Needs Continuous Responses in Cyberspace," *New Atlanticist,* Atlantic Council, December 9, 2020, https://www.atlanticcouncil.org/blogs/new-atlanticist/nato-needs-continuous-responses-in-cyberspace/.

[5] Luukas K. Ilves et al., "European Union and NATO Global Cybersecurity Challenges," *Prism* 6, no. 2 (2016): 126–141.

institutionalize and expand upon the sectoral approach already in place by NATO's Defense against Terrorism Programme of Work and Civil Emergency Planning Committee.[6]

Therefore, we recommend these processes take the form of European Union (EU) legislation coordinated with the legislation of non-EU NATO partner nations. We strongly encourage NATO to increase its cooperative role with the EU within the framework of the NDPP to:

- define and delineate all critical infrastructure within the European bloc
- require the NDPP and the EPCIP to jointly determine vulnerabilities on the Continent, with a focus on private sector-controlled CI
- develop unified standards for critical infrastructure resilience, namely securing networks from cyberattack and establishing backup and failsafe mechanisms
- establish a security review process for foreign acquisitions that brings both NATO and EPCIP standards and experts to a prominent role in approving new projects

We also recommend NATO encourage more member states to participate in the NATO Innovation Fund and expand the Innovation Fund's endowment. Only 17 member states currently contribute to the NATO Innovation Fund, and the fund has a budget of only €1 billion.[7] For comparison, while NATO operations consume only €2.5 billion in funding, the Alliance's total defense expenditure amounts to nearly €1.1 trillion.[8] The Innovation Fund is nevertheless an ideal platform for ensuring significant investment in emerging technologies. While NATO advises its member states to devote a share of 0.4% of GDP to research and development (R&D) of military equipment, there is great disparity between member states' R&D investments.[9] Considering the interconnectedness of critical infrastructure and cyber networks, this national R&D disparity is a significant gap in NATO's security. Participation and additional funding from the United States, France, and other member states that have not yet signed on would only improve the Fund's potential. These funds could be distributed to universities, state research programs,

---

[6] Maciej Klósak, Leopold Kruszka, and Pawel Muzolf, "Critical Infrastructure Protection: Best Practices and Innovative Methods of Protection," (Amsterdam, NL: IOS Press, 2019), 12; European Commission, "Communication from the Commission: on a European Programme for Critical Infrastructure Protection," December 12, 2006, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF.

[7] NATO, "NATO Allies Take the Lead on the Development of NATO's Innovation Fund," October 22, 2021, https://www.nato.int/cps/en/natohq/news_187607.htm.

[8] NATO Public Diplomacy Division, "Defence Expenditure of NATO Countries (2014-2021)," Communique PR/CP(2021)094, June 11, 2021, 7, https://www.nato.int/nato_static_fl2014/assets/pdf/2021/6/pdf/210611-pr-2021-094-en.pdf.

[9] NATO Public Diplomacy Division, "Defence Expenditure of NATO Countries."

and the private sector. An increase in Alliance-level funding for R&D of emerging technologies with security applications would help NATO match Russian and Chinese advances in autonomous and hypersonic weapons, revolutionize its operations with big data and artificial intelligence, and prepare for the diverse challenges of the coming decades.

Note: **The views expressed are those of the University of Washington students and do not necessarily reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government. Students had no access to special. The students had no special access to intelligence or any operational matters that are not otherwise available to the general public.**

Selected Bibliography

European Commission. "Communication from the Commission: on a European Programme for Critical Infrastructure Protection." December 12, 2006. https://eur-ex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF.

Ilves, Luukas K., Timothy J. Evans, Frank J. Cilluffo, and Alec A. Nadeau. "European Union and NATO Global Cybersecurity Challenges," *Prism* 6, no. 2 (2016): 126–141. http://cco.ndu.edu/PRISM/PRISM-Volume-6-no-2/Article/840755/european-union-and-nato-global-cybersecurity-challenges-a-way-forward/.

Klósak, Maciej, Leopold Kruszka, and Pawel Muzolf. "Critical Infrastructure Protection: Best Practices and Innovative Methods of Protection." Amsterdam, NL: IOS Press, 2019.

Kramer, Franklin D., Lauren Speranza, and Conor Rodihan. "NATO Needs Continuous Responses in Cyberspace." *New Atlanticist,* Atlantic Council, December 9, 2020. https://www.atlanticcouncil.org/blogs/new-atlanticist/nato-needs-continuous-responses-in-cyberspace/.

Lis, Piotr, and Jacob Mendel."Cyberattacks on Critical Infrastructure: An Economic Perspective." *Economics and Business Review* 5, no. 2, (2019): 24-27. https://sciendo.com/pdf/10.18559/ebr.2019.2.2.

NATO. "Cyber Defense." *NATO Newsroom,* July 2, 2021. https://www.nato.int/cps/en/natohq/topics_78170.htm.

NATO. "NATO Allies Take the Lead on the Development of NATO's Innovation Fund." October 22, 2021. https://www.nato.int/cps/en/natohq/news_187607.htm.

NATO. "NATO Standardization Office." *NATO Newsroom,* June 9, 2017. https://www.nato.int/cps/en/natohq/topics_124879.htm.

NATO. “Press Conference by NATO Secretary General Jens Stoltenberg Following the Second Day of the Meeting of NATO Ministers of Defence.” *NATO Newsroom*, October 22, 2021. https://www.nato.int/cps/en/natohq/opinions_187634.htm.