12-15-2022

Countering Terrorism on Tomorrow’s Battlefield: Critical Infrastructure Security and Resiliency (NATO COE-DAT Handbook 2)

Lucas M. Cox

Denise Feldner

Trevor P. Helmy

Frank J. Kuzminski

Sarah J. Lohmann

See next page for additional authors

Recommended Citation

Lucas M. Cox, Denise Feldner, Trevor P. Helmy, Frank J. Kuzminski, Sarah J. Lohmann, Marcus Mohlin, Aleksander Olech, Wuraola Oyewusi, Gabriel T. Raicu, Silke Ruhl, Sabrina Schulz, Máté Tóth, and Megan A. Ward, *Countering Terrorism on Tomorrow’s Battlefield: Critical Infrastructure Security and Resiliency (NATO COE-DAT Handbook 2)* (Carlisle, PA: US Army War College Press, 2022), https://press.armywarcollege.edu/monographs/957

Authors

Lucas M. Cox, Denise Feldner, Trevor P. Helmy, Frank J. Kuzminski, Sarah J. Lohmann, Marcus Mohlin, Aleksander Olech, Wuraola Oyewusi, Gabriel T. Raicu, Silke Ruhl, Sabrina Schulz, Máté Tóth, and Megan A. Ward

This book is prepared by the cooperation
between COE-DAT and USAWC SSI

CENTRE OF EXCELLENCE
DEFENCE AGAINST TERRORISM

U.S. ARMY WAR COLLEGE
SSI
STRATEGIC STUDIES INSTITUTE

COUNTERING TERRORISM ON TOMORROW'S BATTLEFIELD:

CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCY HANDBOOK 2

Sarah J. Lohmann
Editor

UNITED STATES
ARMY WAR COLLEGE
PRESS
Carlisle Barracks, PA

STRATEGIC STUDIES INSTITUTE
"The Army's Think Tank"

The Strategic Studies Institute (SSI) is the US Army's institute for geostrategic and national security research and analysis. SSI research and analysis creates and advances knowledge to influence solutions for national security problems facing the Army and the nation.

SSI serves as a valuable source of ideas, criticism, innovative approaches, and independent analyses as well as a venue to expose external audiences to the US Army's contributions to the nation. It acts as a bridge to the broader international community of security scholars and practitioners.

SSI is composed of civilian research professors, uniformed military officers, and a professional support staff, all with extensive credentials and experience. SSI's Strategic Research and Analysis Department focuses on global, transregional, and functional security issues. Its Strategic Engagement Program creates and sustains partnerships with strategic analysts around the world, including the foremost thinkers in the field of security and military strategy. In most years, about half of SSI's publications are written by these external partners.

Research Focus Arenas

Geostrategic net assessment—regional and transregional threat analysis, drivers of adversary conduct, interoperability between partner, allied, IA, commercial, and Joint organizations

Geostrategic forecasting—geopolitics, geoeconomics, technological development, and disruption and innovation

Applied strategic art—warfare and warfighting functions, Joint and multinational campaigning, and spectrum of conflict

Industrial/enterprise management, leadership, and innovation—ethics and the profession, organizational culture and effectiveness, transformational change, talent development and management, and force mobilization and modernization

US Army War College

Countering Terrorism on Tomorrow's Battlefield:
Critical Infrastructure Security and Resiliency
NATO COE-DAT Handbook 2

Sarah J. Lohmann
Editor

Lucas M. Cox, Denise Feldner, Trevor P. Helmy,
Frank J. Kuzminski, Sarah J. Lohmann, Marcus Mohlin,
Aleksander Olech, Wuraola Oyewusi, Gabriel T. Raicu,
Silke Ruhl, Sabrina Schulz, Máté Tóth, Megan A. Ward
Contributors

December 2022

UNITED STATES
ARMY WAR COLLEGE
PRESS
Carlisle Barracks, PA
STRENGTH and WISDOM

Strategic Studies Institute

This is a peer-reviewed publication. The views expressed in this publication do not necessarily reflect the official policy or position of NATO, COE-DAT, NATO member countries, or the institutions with which the lecturers are affiliated. The views expressed in this publication do not necessarily reflect the official policy or position of the Department of the Army, the Department of Defense, or the US government. Authors of Strategic Studies Institute and US Army War College Press publications enjoy full academic freedom, provided they do not disclose classified information, jeopardize operations security, or misrepresent official US policy. Such academic freedom empowers them to offer new and sometimes controversial perspectives in the interest of furthering debate on key issues. This publication is cleared for public release; distribution is unlimited.

******

******

Comments pertaining to this publication are invited and should be forwarded to: Director, Strategic Studies Institute and US Army War College Press, US Army War College, 47 Ashburn Drive, Carlisle, PA 17013-5244.

******

ISBN 1-58487-844-4

Cover Photo Credits

Front Cover

Photo Description: Man in black crew neck shirt
Photo by: Alyona Grishina on Unsplash
Photo Publication Date: April 20, 2020
Website: https://unsplash.com/photos/BBmi4nJjKk8

Back Cover

Background Image Compilation Description: Study the halls of biology
Image by: LiuZiShan on Freepik
Website: https://www.freepik.com/free-photo/study-halls-biology-digital-illustrations_14541125.htm

Table of Contents

Preface

Countering Terrorism on Tomorrow's Battlefield is a handbook on how to strengthen critical infrastructure resilience in an era of emerging threats. Every day malicious actors target new technologies and medical resilience or seek to wreak havoc following disasters brought on by climate change, energy insecurity, and supply-chain disruptions. At the same time, NATO member states are making strides in innovation to protect critical infrastructure. The counterterrorism research produced for this volume aligns with NATO's Warfighting Capstone Concept, which details how NATO Allies can transform and maintain their advantage for the next two decades despite new threats. The topics are rooted in NATO's seven baseline requirements, which set the standard for enhancing resilience in every aspect of critical infrastructure and civil society.

The book is the product of a formal partnership between NATO's Centre of Excellence for the Defence Against Terrorism (COE-DAT) and the US Army War College Strategic Studies Institute. The first handbook on critical infrastructure security resilience published by the US Army War College Press in November 2022 detailed the kinetic, cyber, and hybrid threats to critical infrastructure through diverse lifeline case studies and provided important tools for policymakers and critical infrastructure owners and operators to enhance resiliency. This second volume looks to the future and what innovation is being developed, how terrorists and adversaries are using emerging and disruptive technologies, and how they fill the power vacuum left in the wake of emergencies (such as pandemics and natural disasters) for malicious purposes. Both handbooks evolved from recommendations on how to improve the Critical Infrastructure Protection against Terrorist Attacks course taught at COE-DAT. As such, the handbooks are designed to be used in the classroom to inform NATO allies, partners, policymakers, and private-sector organizations.

This second handbook is divided into three subcategories: countering the terrorist threat to technology; to medical resilience; and to climate change, energy, and the supply chain. For each topic, readers are informed of NATO policies, context and methods of resilience, and evolving terrorist threats and tactics. Each chapter recommends new policies and tools to counter these evolving tactics and poses questions on greater NATO collaboration and interoperability in the fight against terrorism. NATO has new possibilities to cooperate in the joint creation and operation of drone exercises, to cull big-data analytics to stop terrorist attacks before they occur, or to track illnesses through early-warning technology that can help stop the spread of illness before it becomes a pandemic.

We hope this collaboration of authors from the military, academic, and private-sector communities and from across North America, Europe, and Africa provides NATO and its partner nations with actionable information and recommendations to prepare for the battlefield of the future.

Sarah J.M Lohmann

Sarah J. Lohmann
Visiting Professor
Strategic Studies Institute
US Army War College

Acting Assistant Professor
University of Washington

Acknowledgments

The US Army War College Strategic Studies Institute (SSI) is honored to have partnered with the NATO Centre of Excellence for the Defence Against Terrorism (COE-DAT) in this project. The concept for the handbook, crafted under the leadership of SSI Director Dr. Carol Evans and COE-DAT Director Colonel Oğuzhan Pehlivan and Deputy Director Daniel Wayne Stone, was developed to completion through the hard work of the book authors: Lucas Cox and Trevor Helmy, Denise Feldner, Lieutenant Colonel Frank Kuzminski, Sarah Lohmann, Aleksander Olech, Commander Marcus Mohlin and Sabrina Schulz, Lieutenant Colonel Sabine Ruhl and Major Máté Tóth, and Wuraola Oyewusi. Together, they worked across 11 time zones and four workshops to produce this handbook. We were pleased that the NATO Energy Security Centre of Excellence and the NATO Centre of Excellence for Military Medicine provided support for the volume.

Our thanks go to Dr. Lohmann, who edited and led the writing of the volume, shaped the content, and recruited and coordinated with the authors to ensure a diversity of military and academic voices could be represented while staying true to the framework of the NATO Warfighting Capstone Concept. We are also grateful to US Army War College intern Lucas Cox for his editing and layout prowess and for the support of Dr. Lohmann's University of Washington students, who provided the research for the first chapter on mission-critical infrastructure. Our appreciation is owed to Army War College Press Editor in Chief Dr. Antulio J. Echevarria II for his insightful questions and comments during workshops.

Our gratitude goes to Colonel Daniel Wayne Stone for his support for the project and the critical analysis he provided on the chapters. We cannot thank Colonel Attila Csurgo enough for his tireless project coordination and availability around the clock to answer questions. Ms. Selvi Kahraman was crucial to the project with her ability to keep the team connected and workshops flowing. Thanks to the entire COE-DAT staff for hosting SSI during the workshops and for your hospitality, hard work, and preparation. Without the effort of the entire team of both institutions, this book would not have been possible.

Carol V. Evans

Dr. Carol V. Evans
Director, Strategic Studies Institute
and US Army War College Press

Oğuzhan Pehlivan, PhD
Colonel (TUR A)
Director, COE-DAT

Executive Summary

What do election infrastructure, space, drones, and disinformation have to do with each other? How can medical resilience be strengthened, and how are terrorists using broken supply chains, energy security, and climate change to sow chaos and destruction? Malicious actors are laying the groundwork for victory on tomorrow's battlefield by using the same innovation and critical infrastructure democracies are using to save lives. Terrorists, however, are using new technologies to extinguish lives.

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, and asymmetrical warfare. While technological innovation and infrastructure interdependencies heighten the risks of cascading effects, the systems providing 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.

Countering Terrorism on Tomorrow's Battlefield assesses new technologies, civil-military cooperation, interoperability, and a whole-of-government approach as ways to strengthen NATO's resilience. It also examines where innovation needs to be hardened to ensure Alliance security. The same big-data analytics the US military has used to hunt terrorists are being used by the Taliban to target innocents. Space systems provide critical capabilities to enable NATO's core missions of deterrence and defense, including secure communications (SATCOM), positioning, navigation, and timing (PNT), early warning, environmental assessment, and intelligence, surveillance, and reconnaissance (ISR). However, the proliferation of counter-space technologies renders these systems vulnerable to interference and attack by state and non-state actors. Terrorists and adversaries with lower defense budgets and less training are making gains on battlefields due to drones, even as NATO is increasing its counter-unmanned aerial vehicle (UAV) capacities.

The story does not end there. NATO member states are working together to strengthen UAV prowess through joint exercises. Disinformation and hacked election infrastructure are being countered through targeted information campaigns and updated cybersecurity protections. Medical resilience is being strengthened through new pandemic tracking and early-warning systems. Energy security requires a unified political, economic, and military approach of member states that will bring long-term energy independence. In addition, NATO is creating healthier supply chains within the Alliance rather than turning to unreliable outside partners. The impacts of climate change on military preparedness are forcing new methods of preparedness and equipment.

This second handbook on critical infrastructure security and resilience for NATO's Centre of Excellence in the Defence Against Terrorism analyzes today's emerging threats, their trajectory, and how equipped NATO is to handle them. It provides recommendations and suggests new tools for foresight, preparedness, and response to these threats. We hope this research serves as a foundation to strengthen Alliance defenses today—and for decades to come.

— Section 1 —

Countering the Terrorist Threat to Technology

— 1 —

Mission-dependent Critical Infrastructure

Lucas M. Cox and Trevor P. Helmy

Chris Chomyszak, Samuel Jacobson, Sam Lavey,
Martha Lewis, Katherine Lin, Sam Mabe, Alex Olsen, Isobel Williamson,
Sydney Winstead, Abraham Wu
Student Researchers

ABSTRACT: This chapter discusses the vulnerabilities facing NATO critical infrastructure and proposes ways to promote critical infrastructure resilience. After defining key terms, the chapter explores how critical infrastructure has been tested in NATO partner states and out-of-area. Member states' critical infrastructure has inherent vulnerabilities to external threats and internal failure. The authors explore these weaknesses as well as describe areas of civil-military cooperation and partnerships that can promote critical infrastructure security and resilience.

Keywords: critical infrastructure, mission-dependent infrastructure, Kazakhstan, European Union, energy security, cybersecurity, civil-military cooperation

Introduction

This chapter first summarizes NATO's definitions of critical infrastructure categories. Next, it discusses resilience, detailing NATO's seven baseline requirements, explores the January 2022 riots in the wake of gas price hikes in Kazakhstan as a case study 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, including power generation, water supply, communications assets, transportation, and energy distribution.

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 created a plan, NATO can identify critical national infrastructure to ensure essential assets are adequately protected.[3]

NATO defines *mission-vital infrastructure* 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

Note: This chapter appeared in altered form in Sarah Lohmann et al., *Navigating New Threats: NATO's Posture on Emerging Technologies* (Seattle: University of Washington Henry M. Jackson School of International Studies, March 2022), 3–22, https://jsis.washington.edu/wordpress/wp-content/uploads/2022/04/22_TF_JSIS-495H_Lohmann.pdf.

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

[2] NATO, *Infrastructure Assessment*.

[3] NATO, *Infrastructure Assessment*.

a failure.[4] Meanwhile, *key infrastructure* is defined as infrastructure 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 linking the port to inland areas, however, would be considered key infrastructure in this scenario since 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, and adversaries can use hypersonic missiles to launch a devastating first strike. There have been examples of national critical infrastructure being unexpectedly degraded or taken offline at the hands of state actors. Alternatively, a lesser adversary might affect some national critical infrastructure and raise doubts about the allies' ability to defend themselves. Attacks can come from anywhere at any time, and there is no guarantee they will 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

[4] NATO, *Infrastructure Assessment*.

[5] NATO, *Infrastructure Assessment*.

[6] "Resilience, Civil Preparedness and Article 3," NATO (website), March 23, 2021, https://www.nato.int/cps/en/natohq/topics_49158.htm.

[7] "Resilience, Civil Preparedness and Article 3."

of resilience in these areas secure the continuity of government functions and essential services during and after a crisis. Each area 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 a framework to foster innovation against new emerging threats.

NATO and its member states can strengthen resilience through four primary means: building persistence, capacity consideration, education, and training.[8] Building persistence requires a critical, continuous assessment of areas in which member states' baseline resilience plans 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 vital 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. Although 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

[8] NATO Supreme Allied Command Transformation (SACT) and City of Norfolk, *Building Resilience: Collaborative Proposals to Help Nations and Partners* (Norfolk, VA: SACT and City of Norfolk, June 2017), 2, https://www.act.nato.int/images/stories/events/2017/resilience/resilience-wp.pdf.

[9] 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 M. Gohel and Peter K. Forster, eds., *Counter-terrorism Reference Curriculum* (Brussels: NATO Defence Education Enhancement Programme, May 2020), https://www.nato.int/nato_static_fl2014/assets/pdf/2020/6/pdf/200612-DEEP-CTRC.pdf.

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 infrastructure and deterring adversaries from using civil instability to debilitate partner nations. This example 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 2022 Russian invasion of Ukraine.

The January 2022 protests and riots in Kazakhstan resulted from a critical infrastructure failure. On January 1, 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 these 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 the Collective Security Treaty Organization forces to improve the security, 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, caused energy shortages in Europe, and threatened the efficiency of NATO military forces.[15] The Kazakh example illustrates the multifaceted nature of critical infrastructure and how its nonmilitary impacts could affect 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.

[12] Valerie Hopkins, "Kazakhstan Declares State of Emergency as Protests over Fuel Prices Spread," *New York Times* (website), 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 (website), 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* (website), 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 (website), March 1, 2022, https://www.reuters.com/markets/europe/global-markets-wrapup-1-2022-03-01/; and Kristian Knus Larsen, *Unfolding Green Defense: Linking Green Technologies and Strategies to Current Security Challenges in NATO and the NATO Member States* (Copenhagen: University of Copenhagen Centre for Military Studies, December 2015), https://cms.polsci.ku.dk/publikationer/unfolding-green-defense/Undfolding_Green_Defense_CMS-rapport.pdf, 3–5.

Testing Resilience

Testing Alliance states' resilience is critical in identifying weaknesses and avenues for improvement. The following exercises 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, assessing resilience across various sectors, and promoting 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 with 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 cybersecurity.[18] The US Army War College Center for Strategic Leadership and Development (CSLD) has led war games, 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,

[16] Alex Beehler and J. E. Jack Surash, "Cutting the Cord to Test Energy Resilience," US Army (website), April 13, 2020, https://www.army.mil/article/234514/cutting_the_cord_to_test_energy_resilience.

[17] Beehler and Surash, "Cutting the Cord."

[18] "Science and Technology: First Responder/Disaster Resilience," US Department of Homeland Security (DHS) (website), last updated on June 8, 2022, accessed on January 20, 2022, https://www.dhs.gov/science-and-technology/first-responder-disaster-resilience.

[19] Cynthia E. Ayers and Kenneth D. 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.

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 Cybersecurity and 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. The 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 to the military and civilians that would be cut off 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 technologies that could serve as back-ups to current infrastructure or help maintain supply chains.[23] This directorate created a strategic plan for artificial intelligence (AI) and machine learning that 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

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

[21] Chris Anderson, *Privacy Impact Assessment for the National Infrastructure Coordinating Center INSight Application* (Washington, DC: DHS, November 23, 2007), https://www.dhs.gov/sites/default/files/publications/privacy_pia_nppd_nicc.pdf, 2–7.

[22] "Emergency Support Function #14 – Cross-Sector Business and Infrastructure" (Washington, DC: US Federal Emergency Management Agency, October 2019), 1, https://www.fema.gov/sites/default/files/2020-07/fema_ESF_14_Business-Infrastructure.pdf.

[23] William N. Bryan, "The Power of Testing Critical Infrastructure in Operational Settings," DHS *Science and Technology* (blog), November 19, 2018, https://www.dhs.gov/science-and-technology/blog/2018/11/19/power-testing-critical-infrastructure-operational-settings.

[24] "Critical Infrastructure Vulnerability Assessments," US Cybersecurity and Infrastructure Security Agency (CISA) (website), n.d., accessed January 20, 2022, https://www.cisa.gov/critical-infrastructure-vulnerability-assessments.

[25] DHS, "First Responder/Disaster Resilience."

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 a nation-state, a non-state actor, or the environment. For example, increased disinformation campaigns delivered through cyberspace and traditional media have added to the spread of disinformation and damaged election integrity.[26] These attacks disturb the continuity of government by sowing distrust 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 threaten access to these vital resources. The COVID-19 pandemic and resulting mass casualties overextended many states' health-care systems to the point of near collapse.[28]

NATO critical infrastructure systems also have multiple inherent vulnerabilities that leave dependent populations at risk. One 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

[26] Jamie Shea, "Resilience: A Core Element of Collective Defence," NATO Review (website), March 30, 2016, https://www.nato.int/docu/review/articles/2016/03/30/resilience-a-core-element-of-collective-defence/index.html.

[27] "Energy Security," NATO (website), 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 U.S. Critical Infrastructure Entities: Guidelines from an Intelligence Perspective* (Washington, DC: NCSC, 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.

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 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 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 vulnerabilities.

In some instances, the 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 some states purposely ignored phone calls from the Department of Homeland Security. They stated they could not comply with the DHS security standards because of existing burdens, poor technology, and their own cost-benefit calculations. Some states also noted they lacked the expertise to create disaster scenarios and prepare as the Department of Homeland Security wanted.[36]

Given the high degree of infrastructural interdependence, a critical infrastructure failure in one state can lead to cascading cross-border

[30] NCSC, "Insider Threat Mitigation."

[31] SACT and City of Norfolk, *Building Resilience*, 2.

[32] Humphreys, *Critical Infrastructure*, 20.

[33] DHS and Department of State (DOS) CISA, *A Guide to Critical Infrastructure Security and Resilience* (Washington, DC: DHS and DOS CISA, November 2019), 12, https://www.cisa.gov/sites/default/files/publications/Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf.

[34] Humphreys, *Critical Infrastructure*, 20.

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

[36] Humphreys, *Critical Infrastructure*, 7.

failures.[37] 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.[38] 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 critical point in its existence, needing to determine the extent to which, if any, 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.[39] 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.[40] 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.[41] Each of these assets is highly vulnerable, and the prevalence of civilian

[37] Gohel and Forster, *Counter-terrorism Reference Curriculum*, 95.

[38] SACT and City of Norfolk, *Building Resilience*, 1.

[39] "Resilience, Civil Preparedness and Article 3."

[40] "Resilience, Civil Preparedness and Article 3."

[41] "Resilience, Civil Preparedness and Article 3."

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.[42] 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.[43] 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.[44]

Second, civil-military cooperation in the construction of nongovernment-owned infrastructure "can accelerate the technological process" by which new technologies are researched, developed, and put into use.[45] 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.[46] 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 technology by "pointing to specific university

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

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

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

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

[46] "Hypersonics Force Multiplier."

research that will contribute to closing those gaps."[47] 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."[48]

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 Department of Defense and with industry partners, including nontraditional military partners. In an important example of civil-military cooperation, the Department of Defense 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.[49]

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 over European cooperation with Russian- and China-owned companies, arguing that some countries are putting "economic benefits above the objectives of the European Union and broader geopolitical concerns."[50] 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.[51] Other European investors such as Engie from France, Shell, a British and Dutch company, and OMW of Austria financially supported the pipeline.[52] If the pipeline had become operational, Russia, through Gazprom, would have become a more dominant supplier of European

[47] "Hypersonics Force Multiplier."

[48] "Hypersonics Force Multiplier."

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

[50] Moniek 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 2021): 495–510, https://doi.org/10.1080/07036337.2020.1800680.

[51] "Resilience, Civil Preparedness and Article 3"; and Andrew A. 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/.

[52] Michta, "Three Seas Initiative."

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.[53] Until Olaf Scholz's government canceled the pipeline's certification after Russia's invasion of Ukraine, many feared Germany's hands-off, pro-commerce attitude on the pipeline was creating vulnerabilities in European critical infrastructure.[54] Indeed, much of the damage had already been done.

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 September 11 attacks facilitated NATO's efforts in improving civil-military coordination of air traffic control.[55]

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.[56]

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.[57] Military sectors can rely on advanced equipment

[53] de Jong and Van de Graaf, "Lost in Regulation."

[54] Melissa Eddy, "Germany Puts a Stop to Nord Stream 2, a Key Russian Natural Gas Pipeline," *New York Times* (website), February 22, 2022, https://www.nytimes.com/2022/02/22/business/nord-stream-pipeline-germany-russia.html?smid=url-share.

[55] "Countering Terrorism," NATO (website), September 14, 2021, https://www.nato.int/cps/en/natohq/topics_77646.htm.

[56] Kevin M. Camp et al., "Monthly Labor Review: From the Barrel to the Pump: The Impact of the COVID-19 Pandemic on Prices for Petroleum Products," US Bureau of Labor Statistics (website), October 2020, https://doi.org/10.21916/mlr.2020.24.

[57] Constantine Samaras, William J. Nuttall, 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.

to assess the destruction rapidly and send out response teams when responding to natural disasters.[58] For example, partnership between NATO members through the NATO Innovation Fund can foster close research relationships between the government and private firms.[59] Nations can use their NATO connections to strengthen a 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 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 toward a near-limitless technological frontier of opportunities and threats, NATO members can leverage this advantage and collaborate to enhance their cybersecurity and technological security standards and 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 a shared interest in maintaining Euro-Atlantic security. There is significant potential to meet mutual needs and increase resilience between these two organizations. There have already been significant security partnerships between the EU and NATO, for example, the European Centre of Excellence for Countering Hybrid Threats (Hybrid COE), which became operational in April 2017. Since this program's inception, the EU and NATO staff have participated in joint workshops on how hybrid threats can disrupt security.[60] 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.[61] Joint training operations between the EU and NATO, the United States

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

[59] "Emerging and Disruptive Technologies," NATO (website), October 22, 2021, https://www.nato.int/cps/en/natohq/topics_184303.htm.

[60] Sonia Krimi, *2020 – Report – The NATO-EU Partnership in a Changing Global Context* (Brussels: 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.

[61] "Brussels Summit Communiqué: Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Brussels, 14 June 2021," NATO (website), last updated July 1, 2022, https://www.nato.int/cps/en/natohq/news_185000.htm.

and NATO, and the EU and the United States—particularly those relating to hybrid warfare and emerging technologies—will foster further cooperation and increase the Alliance's counterterrorism capacity and collective security.[62]

NATO can play an important role in ensuring the security of privately owned critical infrastructure, specifically in the foreign acquisition process. Certain EU 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.[63] For example, Italy has given conditional approval for Huawei, a corporation with links to Chinese security services, to develop 5G infrastructure across the country.[64] 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.

The EU and NATO also encourage civil-military cooperation on emerging technologies to promote critical infrastructure resilience. For example, 34 NATO and EU members and more than 30 private-sector partners 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."[65] 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."[66]

[62] Michael Rühle and Clare Roberts, "Enlarging NATO's Toolbox to Counter Hybrid Threats," NATO (website), March 19, 2021, https://www.nato.int/docu/review/articles/2021/03/19/enlarging-natos-toolbox-to-counter-hybrid-threats/index.html.

[63] Sarah Erickson, "Recent Developments in EU Foreign Investment Screening," CSIS *Strategic Technologies Blog*, April 19, 2021, https://www.csis.org/blogs/strategic-technologies-blog/recent-developments-eu-foreign-investment-screening.

[64] Elvira Pollina and Giuseppe Fonte, "Italy Gives Vodafone 5G Deal with Huawei Conditional Approval – Sources," Reuters (website), May 31, 2021, https://www.reuters.com/technology/italy-gives-vodafone-5g-deal-with-huawei-conditional-approval-sources-2021-05-31/.

[65] SACT and City of Norfolk, *Building Resilience*.

[66] Karlijn Jans and Lauren M. Speranza, "Bridging the Gap: Time for an EU-NATO Strategic Dialogue on Defensive Tech," University of Leiden *Blog Post*, 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.

In the future, standardizing technological procedures across NATO and the EU will be essential to minimize redundancy between allies.[67]

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 euros' worth 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.[68] The EU is also responding to the crisis's humanitarian consequences by granting temporary residency to Ukrainian refugees.[69] 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.[70]

There are still impediments to NATO-EU cooperation, including the global rise of isolationist movements.[71] Furthermore, only 55 percent of European citizens "totally" or "somewhat" support the creation of a "European army."[72] Nevertheless, as the response to Russia's invasion of Ukraine shows, partnership between the EU and NATO is essential to transatlantic security and the resilience of member states' critical infrastructure.

Conclusion

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

[67] Giovanna De Maio, *Opportunities to Deepen NATO-EU Cooperation* (Washington, DC: Brookings Institution, December 2021), https://www.brookings.edu/wp-content/uploads/2021/12/FP_20211203_nato_eu_cooperation_demaio.pdf.

[68] John Chalmers, "Dramatic Zelenskiy Call Prompted EU Move to Provide Arms," Reuters (website), March 2, 2022, https://www.reuters.com/world/europe/dramatic-call-with-ukraine-leader-prompted-historic-eu-move-provide-arms-2022-03-02/.

[69] Philip Blenkinsop and Gergely Szakacs, "EU Backs Move to Give Ukraine Refugees Temporary Residency," Reuters (website), March 3, 2022, https://www.reuters.com/world/europe/eu-prepares-millions-refugees-ukraine-2022-03-03/.

[70] Humeyra Pamuk, "EU Chief Says Bloc Wants Ukraine as Member," Reuters (website), February 27, 2022, https://www.reuters.com/world/europe/eu-chief-says-bloc-wants-ukraine-member-they-are-one-us-2022-02-28/.

[71] 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/.

[72] Krimi, *NATO-EU Partnership*, 12.

armed attack."[73] 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 absent of a posture of resilience, NATO diminishes its deterrence potential and decreases the security of its members' critical infrastructure. Deterrence, which NATO defines as the "threat of force in order to discourage" actors from harming one another, no longer adequately protects the Alliance.[74] Facing unpredictable, unanticipated, and inevitable threats, NATO can ensure the resilience of its members' critical infrastructure.

Understanding 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, a holistic approach to capacity consideration, and informing policymakers and the public of the importance of resilience. Infrastructure systems must be resilient to 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 promotes civil-military cooperation and collaboration between member states. This 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 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.

[73] "North Atlantic Treaty," *International Journal* 4, no. 2 (1949): 156–58, https://doi.org/10.1177/002070204900400206.

[74] Michael Rühle, "Deterrence: What It Can (and Cannot) Do," NATO (website), April 20, 2015, https://www.nato.int/docu/review/articles/2015/04/20/deterrence-what-it-can-and-cannot-do/.

Ensuring the resilience of NATO member states is vital to the success of NATO missions and the integrity of the Alliance. Without resilience, the Alliance and its member states' critical infrastructure systems are vulnerable to various threats, including terrorist attacks, hybrid attacks, asymmetrical warfare, and CBRN strikes. While technological innovation and compounding infrastructure interdependencies heighten the risks of cascading effects, the systems providing 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 must work together to strengthen their collective resilience against known and emerging threats, building a future of robust security for the transatlantic region.

Select Bibliography

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

de Jong, Moniek, 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 2021). https://doi.org/10.1080/07036337.2020.1800680.

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

Hodicky, Jan et al. “Dynamic Modeling for Resilience Measurement: NATO Resilience Decision Support Model.” *Applied Sciences* 10, no. 8 (2020). 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.

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

US National Counterintelligence and Security Center (NCSC). *Insider Threat Mitigation for U.S. 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 Congres*s. Congressional Research Service (CRS) Report RL32115. Washington, DC: CRS, January 29, 2008. https://www.everycrsreport.com/reports/RL32114.html.

— 2 —

Emerging and Disruptive Technologies Used in Counterterrorism: The Future of Big Data, Drones, and Hypersonic Weapons

Sarah J. Lohmann

ABSTRACT: NATO has prioritized areas of cooperation for innovation and defense as it pertains to emerging and disruptive technologies (EDTs). This chapter looks at three of them: autonomous weapons such as drones, technologies using big data, and hypersonic weapons. There will be analysis of how each technology has been used by terrorists or state actors to threaten security and leave critical infrastructure vulnerable. The text will analyze how NATO is repositioning itself to create a coordinated response to these threats and what remains to be done.

Keywords: drones, big-data analytics, counterterrorism, hypersonic weapons, critical infrastructure, NATO, future of war, emerging and disruptive technologies

> Future conflicts will be fought not just with bullets and bombs, but also with bytes and big data. We see authoritarian regimes racing to develop new technologies, from artificial intelligence to autonomous systems. So we are taking further steps to future-proof the alliance.[1]
>
> —NATO Secretary General Jens Stoltenberg,
> October 20, 2021

[1] Florian Eder and Laurenz Gehrke, "German Defense Minister Warns Europeans: Don't Detach from NATO," *Politico* (website), October 21, 2021, https://www.politico.eu/article/germany-defense-minister-annegret-kramp-karrenbauer-eu-nato/.

Introduction

NATO's defense methods are being drastically changed by the emerging technologies used to threaten its member states and allies across the globe. For the first time, hypersonics has been used as a weapon of war on the battlefield in Ukraine. Drones have given a once-small terrorist resistance force in Yemen firepower, and the Taliban have harnessed big data intended for counterterrorism purposes to carry out their terror. At the same time, critical infrastructure connected to emerging technology is creating new vulnerabilities and national security concerns.

NATO's Science for Peace and Security Programme defines *emerging and disruptive technologies* (EDTs) as "technologies that undergo rapid development and can be disruptive to existing systems such as critical infrastructure, supply chains, data networks."[2] NATO has identified seven key areas for cooperation on innovation and defense within the Alliance regarding EDTs: artificial intelligence, data and computing, autonomous weapons, quantum-enabled technologies, biotechnology and human enhancements, hypersonic technologies, and space.[3] This study will examine three of these technologies and how they are being used or have been used to counter terrorism: autonomous weapons such as drones, technologies using big data, and hypersonic weapons. Likewise, there will be an analysis of how terrorists or state actors have used each technology to threaten security and often leave critical infrastructure vulnerable.

The autonomous weapons section will examine the danger posed by drones used by terrorists, nation-states, and non-state actors and analyze current counter-UAV efforts within NATO nations. How drones are changing the battlefield will be analyzed in case studies such as the Houthi attack on the United Arab Emirates critical infrastructure in 2022 and Azerbaijan's use of drones in the Nagorno-Karabakh War in 2020.

The real-time big-data analytics section will discuss big-data technology's value in counterterrorism missions. Here, there will be a discussion of how the Taliban captured US biometric devices and ways to secure the technology so it cannot be used if it falls into the hands of bad actors.

[2] "NATO News: Changing Lives and the Security Landscape – How NATO and Partner Countries Are Cooperating on Advanced Technologies," NATO (website), June 11, 2021, https://www.nato.int/cps/en/natohq/news_184899.htm?selectedLocale=en.

[3] "NATO News: Emerging and Disruptive Technologies," NATO (website), last updated on December 8, 2022, accessed on October 22, 2021, https://www.nato.int/cps/en/natohq/topics_184303.htm.

Finally, the hypersonics section will examine NATO's changing posture as it faces gains made by China, Russia, and North Korea and how it harnesses hypersonic technology for deterrence in this adversarial environment.

NATO Context

In December 2019, NATO leaders agreed on an Emerging and Disruptive Technology Implementation Roadmap, which helped the Alliance coordinate its work around emerging technology in defense, deterrence, and capabilities.[4] Emerging technologies were increasingly impacting NATO's task of defending its member states while also creating new challenges from adversaries. By July 2020, NATO Secretary General Jens Stoltenberg had created an Advisory Group on Emerging and Disruptive Technologies of a dozen private-sector and academic experts who provided NATO with advice on adopting EDT in its mission. By September 2020, these experts had provided NATO with recommendations for technologies on which to focus, and by March 2021, their first annual report.

In February 2021, Defense Ministers endorsed a strategy focusing on military and civilian dual-use technology that can improve NATO's defense advantage while creating a forum for best practices. These goals were made tangible through the establishment of a NATO Innovation Fund at the 2021 Brussels Summit in June to support the development of and guidance on such technology. Real-time data analytics and autonomous weapons have a history of dual use.[5] This capability can create greater competition for the creation of quality defense products and greater risk when the technology is available to adversaries of democratic states. As the example of the capture of biometric devices in Afghanistan shows, the technology used by the military must be hardened to ensure that dual-use technology vital to the mission does not become compromised.

Thus, this chapter will explore how member states future-proof the way they develop emerging technology used for NATO missions. Using the NATO Science and Technology Organization's "Science and Technology Trends: 2020–2040" as a framework, reports of technical developments and

[4] "Emerging and Disruptive Technologies."

[5] Jayshree Pandya, "The Dual-use Dilemma of Artificial Intelligence," *Forbes* (website), January 7, 2019, https://www.forbes.com/sites/cognitiveworld/2019/01/07/the-dual-use-dilemma-of-artificial-intelligence/?sh=60031226cf02; and Peter Novitzky, Ben Kokkeler, and Peter-Paul Verbeek, "The Dual-use of Drones," *Tijdschrift voor Veiligheid* 17, no. 1-2 (July 2018): 79–95, https://www.researchgate.net/profile/Peter-Novitzky/publication/326591084_The_Dual-use_of_Drones/links/5bbf2bb692851c4efd569d38/The-Dual-use-of-Drones.pdf.

challenges will be assessed. NATO's guidelines on emerging and disruptive technologies and dual-use EDTs and military and academic literature will support this assessment. As critical national infrastructure is shaped or challenged by innovators or malicious actors using emerging technology, NATO is repositioning itself to create a coordinated response. The analysis will document this journey and identify areas under development.

Autonomous Weapons

Nation-states and terrorists use autonomous weapons (such as drones) in warfare and armed combat. NATO defines *autonomy* as: "A system's ability to function, within parameters established by programming and without outside intervention, in accordance with desired goals, based on acquired knowledge and an evolving situational awareness."[6] An unmanned aerial vehicle (UAV), often referred to as a drone, is an aircraft without a pilot or human life onboard, remotely piloted by unmanned aircraft systems (UAS), including the controller, support equipment, data links, weapons systems platform, display, payload, and the communications system.[7]

While international law prevents the use of fully autonomous drones, NATO's Science and Technology Organization (STO) predicts that "semi-autonomous systems will have more impact on operations" for the Alliance in the near term.[8] There, the warfighter remains the final decisionmaker, while artificial intelligence and other emerging technologies allow the drone to respond to numbers of adversaries or new obstacles autonomously while seeking out preprogrammed targets.[9] Autonomous systems are changing how war is conducted on NATO's doorstep. Ukraine has publicized its possession of drones that are playing a key role on the battlefield in the conflict

[6] NATO, *NATO Glossary of Terms and Definitions*, AAP-06 (Brussels: NATO Standardization Office, 2019), https://www.jcs.mil/Portals/36/Documents/Doctrine/Other_Pubs/aap6.pdf.

[7] Junyan Hu and Alexander Lanzon, "An Innovative Tri-rotor Drone and Associated Distributed Aerial Drone Swarm Control," *Robotics and Autonomous Systems* 103 (January 2018): 162–74, https://www.researchgate.net/profile/Junyan-Hu-3/publication/324868897_An_innovative_tri-rotor_drone_and_associated_distributed_aerial_drone_swarm_control/links/5fb6365f458515b79750f6a8/An-innovative-tri-rotor-drone-and-associated-distributed-aerial-drone-swarm-control.pdf; and see also US Army, *U.S. Army Roadmap for UAS 2010–2035: Eyes of the Army* (Fort Rucker, AL: Unmanned Aircraft Systems Center of Excellence, 2010), https://apps.dtic.mil/sti/pdfs/ADA518437.pdf.

[8] D. F. Reding and J. Eaton, *NATO Science & Technology Trends 2020–2040*: *Exploring the S&T Edge* (Brussels: NATO Science & Technology Organization, 2020), https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf.

[9] Reding and Eaton, *NATO Science & Technology Trends 2020–2040*.

with Russia.[10] Azerbaijan used drones in the Nagorno-Karabakh war in 2020 to carry laser-guided missiles, successfully attacking Armenian tanks.[11] Russia's swarming drone capacity has strategic and tactical implications for how NATO defends its backyard going forward.[12]

Drones are changing warfare, causing destabilizing effects across regions, escalating conflicts, and putting increased killing capacity in the hands of terrorists and non-state actors. Take the Houthis, for example. In what they dubbed "Operation Hurricane Yemen," the Houthis used drones and five ballistic missiles to target civilians and critical infrastructure, including the Dubai and Abu Dhabi airports and the Musaffah oil refinery, exploding three petroleum tankers near the Abu Dhabi National Oil Company fuel facilities.[13]

The Houthis took responsibility for the drone attacks that killed at least three people and caused explosions across Abu Dhabi on January 18, 2022. The Houthis had previously been designated a terrorist organization, and following the attacks, the United Arab Emirates asked the United States to designate the Houthis as a terrorist organization again.[14] The Saudi-led coalition, including the United Arab Emirates, responded immediately with airstrikes against the Yemeni capital, Sana'a.[15] These drone attacks were the most recent in a multiyear war the Houthis have been waging in the region against challengers to their power. Their use of unmanned technology against Saudi Arabia contributed significantly to a doubling of Houthi-led attacks against Saudi Arabia in 2021.[16]

[10] Aaron Stein, "From Ankara with Implications: Turkish Drones and Alliance Entrapment," War on the Rocks (website), December 15, 2021, https://warontherocks.com/2021/12/from-ankara-with-implications-turkish-drones-and-alliance-entrapment/.

[11] Shaan Shaikh and Wes Rumbaugh, "The Air and Missile War in Nagorno-Karabakh: Lessons for the Future of Strike and Defense," Center for Strategic and International Studies (CSIS) (website), December 8, 2020, https://www.csis.org/analysis/air-and-missile-war-nagorno-karabakh-lessons-future-strike-and-defense.

[12] Samuel Bendett, "Strength in Numbers: Russia and the Future of Drone Swarms," Modern War Institute at West Point (website), April 20, 2021, https://mwi.usma.edu/strength-in-numbers-russia-and-the-future-of-drone-swarms/.

[13] Charbel Mallo et al., "Saudi-led Coalition Launches Airstrikes on Yemeni Capital after Deadly Houthi Drone Strike in Abu Dhabi," *CNN* (website), January 18, 2022, https://www.cnn.com/2022/01/17/middleeast/uae-abu-dhabi-explosion-drone-houthi-intl/index.html.

[14] Lucy van der Kroft, "Yemen's Houthis and the Terrorist Designation System," International Centre for Counter-terrorism – The Hague (website), June 10, 2021, https://icct.nl/app/uploads/2021/06/Houthi-Terrorist-Designation-Policy-Brief.pdf.

[15] van der Kroft, "Yemen's Houthis."

[16] Seth G. Jones et al., "The Iranian and Houthi War against Saudi Arabia," CSIS (website), December 21, 2021, https://www.csis.org/analysis/iranian-and-houthi-war-against-saudi-arabia.

While not in NATO's usual battleground, the Houthi attrition of their Saudi Arabian–led coalition capacities using unmanned aerial vehicles and unmanned vehicle attacks can provide lessons learned as NATO considers the changing nature of warfare and threats from non-state actors.[17] When the rebel group stormed Yemen's capital in September 2014, most would not have predicted that they would have kept the Saudi Arabian–led coalition—backed by the United Arab Emirates, the United States, the United Kingdom, and France—at bay and involved in a drawn-out war since Saudi Arabia began armed interventions in March 2015. Drone warfare has contributed significantly to the rebels' success; access and the number of troops were not obstacles as in traditional warfare.[18] In addition, the rebels did not use internationally recognized norms of limiting targets to military assets but targeted critical infrastructure and civilian targets. This use highlights the need for investing in counter-UAV technology since terrorists and non-state actors increasingly use drones to compensate for the lack of manpower and authorized use of airspace or critical infrastructure.

Closer to NATO's backyard, the air and missile war in Nagorno-Karabakh has provided lessons to be learned on the strengths and weaknesses of using drones in warfare and the changing nature of war. In the conflict between Armenia and Azerbaijan over the disputed Nagorno-Karabakh region, missiles and unmanned aerial vehicles were used. While Azerbaijan modernized its armed forces through new drones from foreign nation-states, Armenia relied on Russian and indigenously produced UAVs for reconnaissance. Azerbaijan took a strategic advantage by using UAVs with light munitions and long endurance (capable of flying for up to 24 hours). It also had a robust fleet of loitering munitions, also called suicide drones, which can hover in an area for a period of time looking for a target.[19]

Ultimately, all sides considered Azerbaijan to have "won" the war due to the strategic advantage provided by drones that had better tracking, targeting, and neutralizing power far beyond the front lines.[20] The diversity of Azerbaijan's air defense shows how crucial having sophisticated UAVs has become in conflict. Passive defense was shown to be a challenge on both sides, as soldiers did not adequately hide their digital or thermal presence and

[17] van der Kroft, "Yemen's Houthis."

[18] van der Kroft, "Yemen's Houthis."

[19] Shaikh and Rumbaugh, "War in Nagorno-Karabakh"; and see also Stefano D'Urso, "Let's Talk about the Israel Air Industries Loitering Munitions and What They're Capable of," Aviationist (website), January 7, 2022, https://theaviationist.com/2022/01/07/iai-loitering-munitions/.

[20] Shaikh and Rumbaugh, "War in Nagorno-Karabakh."

could thus be tracked for targeting.[21] This war offers insight for NATO and its partners to train their forces to camouflage digitally for longer periods and diversify and synchronize a broad array of UAV capabilities during an attack.

Russian takeaways from the 44-day war reflected in Russian military venues such as the *Army Standard* or *Military Review* are slightly more nuanced. While praising the technological strides made by Azerbaijan, they were not convinced the success was due to technology only. Their analyses shed light on a young, inexperienced, and primarily volunteer Armenian army compared to an older, experienced force in Azerbaijan. In addition, they gave credit to the focus and funding of Azerbaijan, which was singularly dedicated to reclaiming the Nagorno-Karabakh region with popular national support.[22] Their lessons learned call for taking into account the whole battlefield, training the force, and looking for one's vulnerabilities or tendency to believe exaggerated nationalist propaganda. Their perspectives may provide NATO with helpful insights into Russia's tactics and motivations as it engages in the conflict with Ukraine.

So far, Ukrainian drones have flown close to Russian vehicles without the expected counter-drone or electronic warfare.[23] Ukrainians have been able to destroy almost half of Russia's surface-to-air missiles with drones, which have aided in information operations and reconnaissance. More recently, field reports have indicated that China has provided Russia with the means to track some of the Chinese-made DJI drones Ukraine has used through Auroscope tracking software and has started to attack the drones and their operators.[24]

It is not yet clear how crucial autonomous weapons have been in helping Ukraine overall in its battleground advances. What is clear is that drones have provided Ukraine with low-cost defense and intelligence, have been intensively used, and, due to a number of factors, a country that ranks 40th in defense spending has been able to have initial successes against a country that ranks fourth.[25]

[21] Shaikh and Rumbaugh, "War in Nagorno-Karabakh."

[22] Alexander Stronell, "Learning the Lesson of Nagorno-Karabakh the Russian Way," International Institute for Strategic Studies (IISS) *Analysis* (blog), March 10, 2021, https://www.iiss.org/blogs/analysis/2021/03/lessons-of-nagorno-karabakh.

[23] Zachary Kallenborn, "Seven (Initial) Drone Warfare Lessons from Ukraine," Modern War Institute at West Point (website), May 12, 2022, https://mwi.usma.edu/seven-initial-drone-warfare-lessons-from-ukraine/.

[24] "'Young Nerds': Ukrainians Use Drones to Kill Russian Soldiers," *CNN* (website), May 13, 2022, https://edition.cnn.com/videos/world/2022/05/13/ukrainian-drones-combat-russian-forces-burnett-dnt-ebof-vpx.cnn.

[25] "Ukrainians Use Drones."

Moving forward, NATO STO predicts that the use of autonomous systems will be critical for operational success in the land, air, and space domain, particularly when it comes to swarming systems.[26] Nuclear powers such as the United States, the United Kingdom, and Russia all have a drone-swarming capacity that they can use in combat for a number of purposes—from precision-guided weapons to remote communications jamming capabilities.[27] Drone swarms are small UAVs that can self-organize and work together to complete multiple tasks.[28] They are often the weapon of choice because their low-cost use translates into fewer soldier casualties, shorter training times, increased targeting efficiency, and durability of expensive weapons systems.[29] Future warfare could escalate quickly as nuclear-armed powers use drone-swarming tactics. With UAVs using artificial intelligence to increase the element of surprise as their capabilities advance in speed, range, and accuracy, escalation of conflict between nuclear powers looms large.[30] So too, do the dangers of using UAVs if employed by non-state actors and terrorists.

So, what can be done? NATO has several goals in its counter-UAS strategy. First, it aims to: integrate multiple solutions technically into a larger defense context; second, to create systems that counter drone threats without collateral damage; third, to integrate counter-UAS across multiple operations; and fourth, to have the same standards across diverse government ministries and public agencies.[31] To make these goals more practical, NATO has created a counter-UAS working group since 2019 with experts from across NATO. The group of experts collaborates on operational and technical interoperability of counter-UAS systems NATO can use and performs trials and exercises together (most recently in September 2022).[32]

[26] Reding and Eaton, *NATO Science & Technology Trends 2020–2040*, 61–63.

[27] Cholpon Abdyraeva, "Drone Swarms – A Future Threat to Armed Forces?," Finabel – European Army Interoperability Centre (website), December 2, 2020, https://finabel.org/drone-swarms-a-future-threat-to-armed-forces/.

[28] Keirin Joyce, "Swarm Robotics: What Will It Look Like?," Defense Info (website), May 20, 2020, https://defense.info/williams-foundation/2020/05/swarm-robotics-what-will-it-look-like/.

[29] Abdyraeva, "Drone Swarms."

[30] James Johnson, "Artificial Intelligence, Drone Swarming and Escalation Risks in Future Warfare," *RUSI Journal* 165, no. 2 (2020): 26–36, https://doi.org/10.1080/03071847.2020.1752026.

[31] Claudio Palestini, "Countering Drones: Looking for the Silver Bullet," NATO Review: Opinion, Analysis, and Debate on Security Issues (website), December 16, 2020, https://www.nato.int/docu/review/articles/2020/12/16/countering-drones-looking-for-the-silver-bullet/index.html.

[32] Rojoef Manuel, "NATO, Netherlands Conduct Counter-Drone Live-testing Exercise," Defense Post (website), October 3, 2022, https://www.thedefensepost.com/2022/10/03/nato-counter-drone-exercise-netherlands/.

The graph in figure 2-1, developed by Lieutenant Colonel Andre Haider of the Joint Air Power Competence Centre, illustrates the comprehensive, multi-domain effort NATO is aiming for as it considers countermeasures it should use depending on the spatial distance between the UAS component and NATO forces. Here, one can view in one graph all the factors that must be considered in counter-UAS measures. In the yellow box, force protection (FP) is vital because it is easy for terrorists and non-state actors to possess and modify commercial off-the-shelf low, slow, and small (LSS) unmanned aerial systems for malicious purposes. Notice that intelligence, surveillance, and reconnaissance (ISR) is the first step in the defense of critical infrastructure here.[33]

[33] Andre Haider, "A Comprehensive Approach to Countering Unmanned Aircraft Systems: And Why Current Initiatives Fall Short," Joint Air Power Competence Centre (website), August 2019, https://www.japcc.org/flyers/a-comprehensive-approach-to-countering-unmanned-aircraft-systems/.

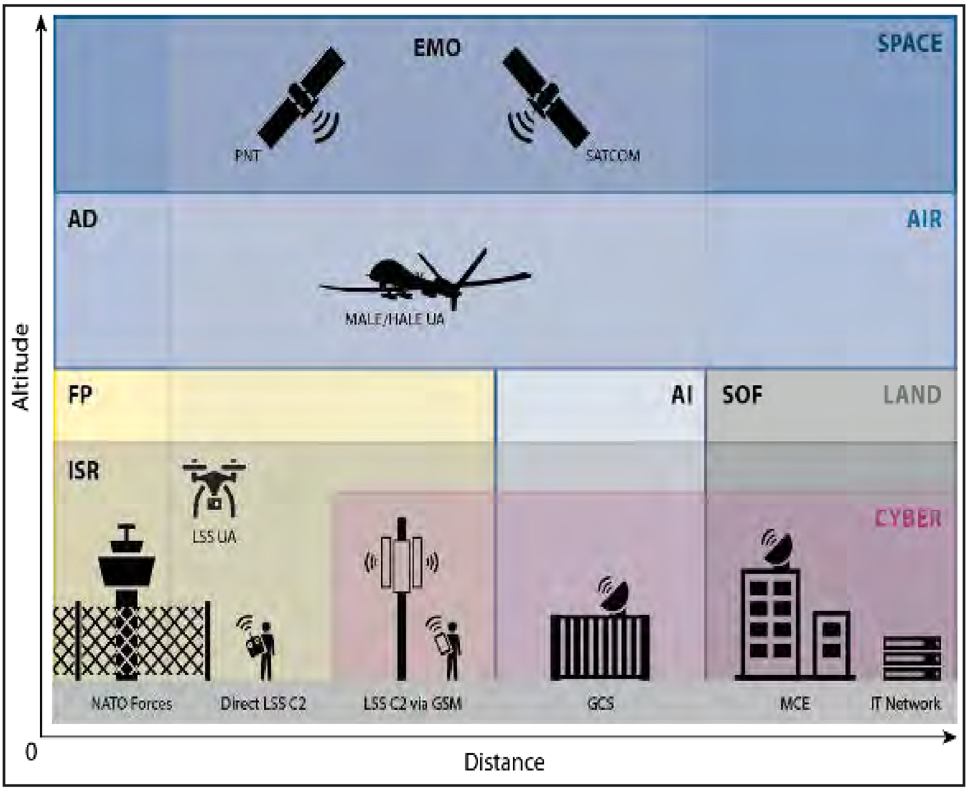


Figure 2-1. A multi-domain effort
(Image used with permission of Lieutenant Colonel Andre Haider)

Moving further away in distance (pink box), the ground control station is crucial for the launch and recovery element (LRE) of larger UAS. As such, the LRE is a critical infrastructure that must be protected through air interdiction (AI) in real time. If the LRE is destroyed, UAS will no longer be able to function.[34] Air defense (AD) in the blue box is likewise important for protection against swarming drones via short-wave air defense and anti-aircraft artillery. Cybersecurity is a crucial layer. Without it, swarming drones' control stations can be knocked offline. The dark blue box shows countermeasures against space-based communications via satellites or position, navigation, and timing signals that can be used against adversary's swarming drones.[35] This comprehensive approach, offered by interoperability operations and defense systems from different NATO members, provides a practical application of NATO's countermeasures.

[34] Haider, "Countering Unmanned Aircraft Systems."

[35] Haider, "Countering Unmanned Aircraft Systems."

Real-time Big-data Analytics

Real-time big-data analytics can be used for predicting terrorist incidents. However, terrorists can also employ this information to target innocents.[36] The Taliban captured US military biometric devices in August 2021 to track and kill those who cooperated with US forces. Biometric systems are big-data systems that work with large volumes of data and analytics to verify and identify a person based on physiological or behavioral characteristics.[37] US forces used these systems in Afghanistan to track terrorists and vet local Afghans assisting US forces in diplomatic talks, defending embassies, serving as translators, or providing other support activities. There is concern that the Taliban could use these biometric systems to target US-friendly Afghans, putting lives at risk.

In addition, the Taliban has taken over the Afghan Interior Ministry's automated biometric identification system and the country's voting record digital identity systems and biometric ID card system, putting additional populations (like women, journalists, and human rights defenders) at risk.[38] Tech companies and nongovernmental organizations are being warned to secure any databases storing this information.

US forces initiated the biometric program in 2007 to track the true identities of persons in Afghanistan regardless of alias, as aliases in the country were common. At the time of the system's creation, there was no single reliable system for national IDs. Over time, however, the Afghan government adopted the system for use in courts or passport applications. By 2011, the Department of Defense had 4.8 million biometric records of people in Afghanistan and Iraq. Once the democratically elected government of Afghanistan fell, the data housed in the biometric device servers became the property of the Taliban.[39] Reports of the Taliban conducting door-to-door searches with biometric devices targeting those with connections

[36] Ibrahim Toure and Aryya Gangopadhyay, "Real Time Big Data Analytics for Predicting Terrorist Incidents," in *Proceedings of 2016 Institute of Electrical and Electronics Engineers (IEEE) Symposium on Technologies for Homeland Security* (Walham, MA: IEEE, May 2016), https://ieeexplore.ieee.org/document/7568906.

[37] Ken Klippenstein and Sara Sirota, "The Taliban Have Seized U.S. Military Biometrics Devices," Intercept (website), August 17, 2021, https://theintercept.com/2021/08/17/afghanistan-taliban-military-biometrics/.

[38] "New Evidence that Biometric Data Systems Imperil Afghans: Taliban Now Control Systems with Sensitive Personal Information," Human Rights Watch (website), March 30, 2022, https://www.hrw.org/news/2022/03/30/new-evidence-biometric-data-systems-imperil-afghans.

[39] Margaret Hu, "The Taliban Reportedly Have Control of US Biometric Devices – A Lesson in Life-and-Death Consequences of Data Privacy," Conversation (website), August 31, 2021, https://theconversation.com/the-taliban-reportedly-have-control-of-us-biometric-devices-a-lesson-in-life-and-death-consequences-of-data-privacy-166465.

to the former Afghan government, journalists, and foreign nonprofits highlight the quandary created by not correctly storing this sensitive big data.[40]

There were three problems with how the United States accessed and stored biometric data. First, the server was built in Afghanistan and fell under its jurisdiction. This issue caused a legal quandary, as the United States would need to enter negotiations with the Taliban—which is holding the data and many of the people connected to it captive—to shut down or limit access to the data.

Second, the United States now had an access issue. When the server became the property of the Taliban, they denied the United States access. The United States could no longer exfiltrate anyone in the system who worked with US forces unless they were documented separately somewhere else.[41] Thus, the United States could not verify whether a person was a former contractor who still needed airlifting out of Afghanistan or if they were in the system due to their terrorist crimes.

Third, US-built federal-use data sources are subject to federal law even when overseas. Ultimately, National Institute of Standards and Technology (NIST) standards should have been applied to the US biometric system. What began as sensitive personally identifiable information (PII) for US military use only was disseminated to the Afghan government without a backup plan if the Afghan government could not be trusted to protect the sensitive data.[42]

There are several solutions NATO can use to save big-data storage and ensure the sensitive data it collects is not compromised.

- NIST-compliant cloud storage for government use.[43] The access nation-states have to the data for each perspective country would need to be clarified in advance but is technically possible.

[40] Rina Chandran, "Afghans Scramble to Delete Digital History, Evade Biometrics," Reuters (website), August 17, 2021, https://www.reuters.com/article/afghanistan-tech-conflict-idUSL8N2PO1FH.

[41] Hu, "Taliban Control of US Biometric Device."

[42] Author interviews with a biometric system creator and law enforcement agent.

[43] John R. Hoehn, *Joint All-domain Command and Control: Background and Issues for Congress*, Congressional Research Service (CRS) Report R46725 (Washington, DC: CRS, March 18, 2021), https://crsreports.congress.gov/product/pdf/R/R46725/2.

- Layered security architecture. Instead of having one employee or login that can provide access to all data, credentials locked in various forms of encryption can hide different elements of critical infrastructure.[44]

Beyond ensuring secure big-data storage, NATO can use big-data analytics to prepare for potential challenges to NATO operations—from terrorism to armed conflict to cyberattacks.[45] In March 2022, the Allied Command Transformation Innovation Hub delivered the Resilience Data Analytics Tool. With Baseline Requirements of Resilience topics and a keywords dashboard, the tool can search through massive amounts of open-source and media reports in 44 languages. The tool incorporates big-data analytics with machine learning to establish patterns and then provides end users with data visualization on where threats to resilience exist across NATO nations.[46]

As a proof of concept, the tool has already assessed the Baltic States and Poland for how they meet the seven baseline requirements of resilience. NATO used the tool in its September 2022 Dynamic Messenger exercise, a large-scale test to demonstrate unmanned systems capabilities in the maritime environment.[47] NATO has the potential to predict future crises and strengthen resilience by refining this big-data analytics tool, feeding it with real-time data, and allowing it to be used more frequently throughout NATO commands to build accuracy. Such collaborative, open-source tools also foster information sharing among allies in the unclassified realm and security within member states.

With the proper national security firewalls, NATO members can combine big data from national databases to track terrorist operations

[44] Jeff Pracht, "A Layered Security Architecture Offers the Strongest Protection from Cyber Threats," Mainstream Technologies (website), November 30, 2021, https://www.mainstream-tech.com/layered-security-architecture/.

[45] Sarah Lohmann and Tim Tepel, "Will the Real Security Foresight Expert Please Stand Up?," *European Journal of Futures Research* 2, no. 37 (March 2014), https://doi.org/10.1007/s40309-014-0037-6; and see also Sarah Lohmann, "Weiterentwicklung der Methoden der Zukunftsanalyse," Institut für Politikwissenschaft/Universität der Bundeswehr, 2014, https://www.unibw.de/politikwissenschaft/professuren/lehrstuhl-ip/projekte/weiterentwicklung-der-methoden-der-zukunftsanalyse.

[46] "A New Resilience Data Analytics Tool." NATO Allied Command Transformation (website), March 24, 2022, https://www.act.nato.int/articles/new-resilience-data-analytics-tool.

[47] "New Resilience Data Analytics Tool"; and see also *12th NATO Maritime Interdiction Operational Training Centre (NMIOTC) Annual Conference Speakers' Inputs* (Crete: NMIOTC, June 1, 2021), https://nmiotc.nato.int/wp-content/uploads/2021/08/12th-Annual-Conference-FFT.pdf.

better across borders.[48] While NATO is already using big data and data sharing to respond to terrorist attacks, it can also exploit advanced data analytics with big-data sources (like social media feeds and sensor and log information) to warn of terrorist attacks down to the neighborhood level and provide foresight into the timing and placement of malicious intrusions on critical infrastructure.[49] While access and coordination would need to be handled delicately, this big-data innovation would take cooperative NATO counterterrorism and promotion of critical infrastructure resilience to the next level.

Hypersonic Technologies

In 2018, Michael Griffin, the Pentagon's new undersecretary for defense for research and engineering, made his first public statements at a Credit Suisse conference about his highest research priority:

> I'm sorry for everybody out there who champions some other high priority, some technical thing; it's not that I disagree with those. But there has to be a first, and hypersonics is my first. . . . When the Chinese can deploy [a] tactical or regional hypersonic system, they hold at risk our carrier battle groups. They hold our entire surface fleet at risk. They hold at risk our forward-deployed forces and land-based forces. Without our ability to defend and without at least an equal response capability on the offensive side, then what we have done is we have allowed a situation to exist where our deployed forces are held at risk, and we cannot do the same for them.[50]

In the three years since then, the public message has been that hypersonic research and development continues to focus on defensive and space purposes. However, current technical developments from NATO adversaries have forced the Alliance to rethink its posture. The Pentagon's fiscal year 2022 budget

[48] Sarah Lohmann et al., *Navigating New Threats: NATO's Posture on Emerging Technologies* (Seattle: University of Washington Henry M. Jackson School of International Studies, March 2022), 23, https://jsis.washington.edu/wordpress/wp-content/uploads/2022/04/22_TF_JSIS-495H_Lohmann.pdf.

[49] Reding and Eaton, *NATO Science & Technology Trends 2020–2040*, 46; and see also Lohmann et al., *Navigating New Threats*, 23.

[50] Aaron Mehta, "Hypersonics 'Highest Technical Priority' for Pentagon R&D Head," Defense News (website), March 16, 2018, https://www.defensenews.com/pentagon/2018/03/06/hypersonics-highest-technical-priority-for-pentagon-rd-head/.

request for hypersonic research is $3.8 billion—up from $3.2 billion last year.[51] The Department of Defense is prioritizing offensive programs, requesting $3.8 billion for hypersonic weapons programs and $247.9 million for hypersonic defense programs for fiscal year 2022.[52] Principal Director for Hypersonics Mike White explained that the United States was still trying to find "the path forward to get a robust defensive strategy" and focusing on offensive programs.[53]

Hypersonic capabilities—which allow propulsion at Mach 5 or above—have been applied to advanced defense systems and can provide access to space.[54] After the September 11 attacks, the counterterrorism value of hypersonic long-range conventional capabilities (to interrupt a meeting of terrorist leaders, for example) was considered.[55] However, over the last decade, hypersonic defense technology has changed focus from counterterrorism uses to interstate warfare.[56] Until now, the United States and NATO have not considered developing hypersonic weapons for use with nuclear warheads but have focused on the technology for short- and intermediate-range conventional precision strikes.[57] Now, technological developments from Russia and China have caused the Alliance to start considering otherwise since the summer of 2021.

Russia's Tsirkon missile system is operational, and the anti-ship hypersonic cruise missile has been reported to have a speed of Mach 9, or roughly 11,000 kilometers per hour.[58] Russia tested the missile system in July 2021, reportedly for the 10th time, launching the Tsirkon missile from the *Admiral Groshkov*

[51] Kelley M. Sayler, *Hypersonic Weapons: Background and Issues for Congress*, CRS Report R45811 (Washington, DC: CRS, October 19, 2021), https://crsreports.congress.gov/product/pdf/R/R45811/22.

[52] Sayler, *Hypersonic Weapons*, 19.

[53] Aaron Mehta, "Is the Pentagon Moving Quickly Enough on Hypersonic Defense?," Defense News (website), March 21, 2019, https://www.defensenews.com/pentagon/2019/03/21/is-the-pentagon-moving-quickly-enough-on-hypersonic-defense/.

[54] "Aeronautics Research: Hypersonic Technology (HT) Project," NASA (website), April 22, 2021, https://www.nasa.gov/aeroresearch/programs/aavp/ht.

[55] James M. Acton, "Silver Bullet? Asking the Right Questions about Conventional Prompt Global Strike," Carnegie Endowment for International Peace (website), 2013, https://carnegieendowment.org/2013/09/03/silver-bullet-asking-right-questions-about-conventional-prompt-global-strike-pub-52778.

[56] Acton, "Silver Bullet?"

[57] Susan Davis, "Hypersonic Weapons – A Technological Challenge for Allied Nations and NATO?" (Brussels: NATO Parliamentary Assembly Science and Technology Committee, 2020), https://www.nato-pa.int/download-file?filename=sites/default/files/2020-07/039%20STC%2020%20E%20-%20HYPERSONIC%20WEAPONS.pdf.

[58] Mark Episkopos, "Bad News, NATO: Russia's Tsirkon Hypersonic Cruise Missile Is Operational," *National Interest* (blog), August 16, 2021, https://nationalinterest.org/blog/reboot/bad-news-nato-russia%E2%80%99s-tsirkon-hypersonic-cruise-missile-operational-191751.

frigate in the White Sea at Mach 7 and hitting a target on the coast of the Barents Sea 350 kilometers away.[59] While NATO responded with a statement that the "hypersonic missiles are highly destabilizing and pose significant risks to security and stability across the Euro-Atlantic area," it vowed to "maintain credible deterrence and defense, to protect our nations."[60] Since then, the US Air Force, in partnership with DARPA, successfully tested its own Hypersonic Air-breathing Weapon Concept (HAWC), flying at a speed greater than Mach 5, on September 27, 2021.[61] It also successfully tested the boost-glide AGM-183A Rapid Response Weapon (ARRW) on May 14, 2022.[62] Russia responded to the fall 2021 test with more hypersonic weapons tests. Furthermore, in a move that surprised US intelligence agencies, China tested its hypersonic missile in August 2021.[63]

As hypersonic missiles' speed does not allow reaction time for defense and provides near-assured destruction of its target, NATO is rethinking its posture, especially considering the danger hypersonic missiles pose to Europe. In fact, for the first time in history, hypersonic weapons are being used in combat by Russia against Ukraine, according to US Joint Chiefs Chairman General Mark Milley. Between 10 and 12 hypersonic weapons (all without nuclear warheads) have been launched against Ukraine at the time of this writing.[64] Three Kinzhal hypersonic missiles hit "tourist infrastructure," with a barrage of Russian missiles striking a shopping mall and two hotels in Odesa, causing civilian casualties.[65] Russia's use of hypersonic missiles

[59] Hercules Reyes, "Russia's Tsirkon Hypersonic Missile Completes Ship Tests," Defense Post (website), September 29, 2021, https://www.thedefensepost.com/2021/09/29/tsirkon-hypersonic-missile-tests/.

[60] "Russia Tests Hypersonic Tsirkon Missile, Leaving NATO Concerned about Potential Escalation," *ABC News* (website), July 20, 2021, https://www.abc.net.au/news/2021-07-20/russia-conducts-missile-test-hypersonic-euro-atlantic-tsirkon/100308688.

[61] "DARPA's Hypersonic Air-breathing Weapon Concept Achieves Successful Flight," DARPA, *Seapower Magazine* (website), September 27, 2021, https://seapowermagazine.org/darpas-hypersonic-air-breathing-weapon-concept-achieves-successful-flight/.

[62] Secretary of the Air Force Public Affairs, "Air Force Conducts Successful Hypersonic Weapon Test," Air Force (website), May 16, 2022, https://www.af.mil/News/Article-Display/Article/3033416/air-force-conducts-successful-hypersonic-weapon-test/.

[63] Demetri Sevastopulo and Kathrin Hille, "China Tests New Space Capability with Hypersonic Missile," *Financial Times* (website), October 16, 2021, https://www.ft.com/content/ba0a3cde-719b-4040-93cb-a486e1f843fb.

[64] Michael Conte, "Russian Use of Hypersonic Weapons in Ukraine Is Not 'Game-changing,' Top US General Says," *CNN* (website), May 11, 2022, https://edition.cnn.com/europe/live-news/russia-ukraine-war-news-05-11-22/h_72ad8e80af76a73251fa61fb6ff61efc.

[65] Paul P. Murphy, "Ukraine Says Second Hotel, Shopping Mall Hit as Russia Fires Hypersonic Missiles at Odesa," *CNN* (website), May 9, 2022, https://www.cnn.com/europe/live-news/russia-ukraine-war-news-05-09-22/h_30902995486238c6d046d1186d9979c5.

against civilian targets underscores a pattern of attacking civilians, resulting in the NATO Parliamentary Assembly deeming Russia a "terrorist state."[66]

Considering those new threats, this section will examine the Alliance's changing posture and how NATO is considering using hypersonic technology for deterrence in this adversarial environment.

The Players

China, the United States, and Russia have had hypersonic capabilities since the early 2000s. While these superpowers use the weapons as a form of deterrence and to shift the global balance of power, less predictable regional players, such as North Korea, have had them for years. West Coast air traffic was stopped at several airports on January 11, 2022, during North Korea's hypersonic weapon test. While early-warning systems provided initial telemetry readings that indicated the launched North Korean missile could hit the Aleutian Islands or the California coast, US Northern Command quickly determined the hypersonic weapon could not harm the United States, and air traffic was restarted within 15 minutes.[67]

North Korea's test also used an HGV, though one with a more limited range of maneuverability than the one used by China. North Korea's test of two hypersonic weapons and 15 other ballistic missiles in 2022—violate United Nations Security Council resolutions banning the use of ballistic missiles.[68] Two successful tests were of missiles to be used with tactical nuclear weapons.[69] The hypersonic tests were alarming because North Korea's hypersonic missile is hard to track. It can change course mid-flight, leaving South Korea vulnerable. Because South Korea lacks the necessary defenses against this maneuverability, it is concerned its only defense could be a preemptive strike, which could cause a quick escalation of conflict.[70]

[66] Sarthak Gupta, "NATO Deems Russia as a 'Terrorist State,' Calls for Support for Ukraine," Jurist (website), November 21, 2022, https://www.jurist.org/news/2022/11/nato-deems-russia-as-terrorist-state-calls-for-support-for-ukraine/.

[67] Katie Bo Lillis, Barbara Starr, and Oren Liebermann, "Early Warning Systems First Suggested North Korean Missile Could Hit US, Causing Temporary Scramble," *CNN* (website), January 13, 2022, https://edition.cnn.com/2022/01/13/politics/north-korean-missile-faa-grounded-planes/index.html.

[68] Lillis, Starr, and Liebermann, "Early Warning Systems."

[69] "North Korea Fires 3 Suspected Ballistic Missiles as U.S. Pushes U.N. for More Sanctions against Kim Regime" *CBS News* (website), May 12, 2022, https://www.cbsnews.com/news/north-korea-ballistic-missile-test-launch-covid-cases-us-sanctions-un/.

[70] Sungwon Baik and Cristy Lee, "Analysis: Why North Korea's Hypersonic Missile Test Is Troubling," Voice of America (website), January 19, 2022, https://www.voanews.com/a/analysis-why-north-korea-s-hypersonic-missile-test-is-troubling/6404637.html.

Once perfected, the Chinese hypersonic capability could send its nuclear warheads over the South Pole and get around the US defense system.[71] In the August 2021 test, China's nuclear-capable hypersonic glide vehicle circled the globe and missed its target by just 24 miles. This capability is new because other hypersonic capabilities from NATO's adversaries can be defended against if they fly in a high arc over the North Pole as conventional ballistic missiles do. This fractional orbital bombardment system flies in a low orbit over the Earth and can get around the north-facing defense system.[72] The United States is considering using directed-energy systems to disrupt the missile flight paths.[73] Those developments will take time to develop.

The Objective

The technology is being developed to use against high-value or high-threat targets where time is vital. Because of the high speed and vast distance that hypersonic weapons can cover, they can be launched outside of conflict areas. For the United States and other NATO members, territory that has been difficult to reach due to China's and Russia's increased anti-access and area denial capabilities—which deny freedom of action and access in areas under friendly control—could be penetrated from a safe, distant perimeter if successfully developed.[74] However, Russia and China already possess these high-speed, long-distance capabilities, and the extreme speed of hypersonic weapons makes interception difficult.

Russia's current goal is assured destruction of its targets in Ukraine and deterrence of NATO and the West. China's objective is neutralizing the United States and maintaining control of the Pacific. The US Naval Institute released photos in May 2022—ranging from US warships in the Pacific to naval bases in Korea and Guam—that provide insight into China's hypersonic missile targets.[75]

[71] Aleks Phillips, "China's Orbiting Hypersonic Missile Could 'Neutralize US Defenses,'" *Express* (website), October 19, 2021, https://www.express.co.uk/news/world/1508211/china-missile-orbiting-hypersonic-weapon-us-defences-concerns.

[72] Reuters Staff, "China's Hypersonic Missile Test Takes US by Surprise," Reuters (website), October 17, 2021, https://www.haaretz.com/world-news/asia-and-australia/2021-10-17/ty-article/chinas-hypersonic-missile-test-takes-u-s-by-surprise/0000017f-f734-d460-afff-ff767e0b0000.

[73] Jack Detsch, "The Pentagon Wants to Ruin China's 'Sputnik Moment,'" *Foreign Policy* (website), February 7, 2022, https://foreignpolicy.com/2022/02/07/us-china-russia-biden-hypersonic-missile-defense-pentagon/.

[74] Reding and Eaton, *NATO Science & Technology Trends 2020–2040*, 90.

[75] Gabriel Honrada, "US, China Locked in a Hypersonic Tit for Tat," *Asia Times* (website), May 13, 2022, https://asiatimes.com/2022/05/us-china-locked-in-a-hypersonic-tit-for-tat/.

The Problem

Until now, NATO has focused on protecting mainland Europe from an intercontinental ballistic missile (ICBM) strike from Russia. A defense posture focused on only one kind of hypersonic weapon and adversary has left NATO at a disadvantage. As successful tests from the summer of 2021 show, China and Russia have pulled ahead of the United States in their hypersonic capabilities. Part of the main problem is the quicker-than-expected successful development of the hypersonic glide vehicle as the delivery mechanism.

The difference between hypersonic glide vehicles and hypersonic ICBMs, which the US has focused on in the past, is that hypersonic ICBMs are powered by rockets, arc high above the Earth, and then return to Earth to strike targets on a preplanned path. The hypersonic glide vehicle uses its momentum, flies low in the Earth's orbit, and upon return to Earth can maneuver off a charted path without being tracked.[76] While eyes were focused on Russia's anti-ship hypersonic cruise missile and its potential impact on Europe in the summer of 2021, China launched a hypersonic missile with the potential for far more devastating damage to the Alliance.

In March 2018, China conducted 20 times as many hypersonic tests as the United States.[77] When the Chinese military tested its hypersonic glide vehicle (HGV) in August 2021, US defense and intelligence officials were alarmed for two reasons. First, as previously mentioned, the hypersonic missile cannot be stopped by NATO's north-facing defenses in Europe, as China's missiles can avoid them by flying over the South Pole. Second, China's hypersonic capability can be much more devastating to the Alliance because its maneuverability makes it extremely hard to track. Unlike a US hypersonic ICBM that flies in a high arc above the North Pole on a fixed path, China's hypersonic glide vehicle flew through low-orbit space propelled by its momentum before it maneuvered toward its target.[78] The United States will not have defensive capabilities against this new weapon until the mid-2020s (at the earliest), leaving a three-year gap with no protection.[79]

[76] Andrew Thornebrooke, "Explainer: What Are Hypersonic Weapons and Why Do They Matter?," October 19, 2021, https://www.theepochtimes.com/mkt_breakingnews/explainer-what-are-hypersonic-weapons-and-why-do-they-matter_4056767.html.

[77] Sayler, *Hypersonic Weapons*, 16.

[78] Sevastopulo and Hille, "China Tests New Space Capability."

[79] "Transcript: Media Availability with Deputy Secretary Shanahan and Under Secretary of Defense Griffin at NDIA Hypersonics Senior Executive Series," US Department of Defense (website), December 13, 2018, https://www.defense.gov/News/Transcripts/Transcript/Article/1713396/media-availability-with-deputy-secretary-shanahan-and-under-secretary-of-defens/.

The United States had not been using or developing hypersonic technology for nuclear weapons due to its New START Treaty with Russia, which bans offensive arms. Russia, however, found a loophole. The treaty does not cover weapons that fly on a ballistic trajectory for less than 50 percent of the flight, as with hypersonic glide and hypersonic cruise missiles.

In concert with NATO, the United States must decide whether to respond by developing its offensive weapons or amping up its defense of the new hypersonic weapons. In the interim, the United States has activated its deterrence initiative to protect NATO member states. In November 2021, it reactivated a nuclear unit at the 56th Artillery Command in Mainz-Kastel, Germany, with the "Dark Eagle," a long-range hypersonic missile that could be in service next year, travel at Mach 17, and reach Moscow in just over 21 minutes.[80]

A third option is the renegotiation of the New Start Treaty, set to expire in 2026 "when a Party believes that a new kind of strategic offensive arm is emerging, that Party shall have the right to raise the question of such a strategic offensive arm for consideration in the Bilateral Consultative Commission."[81] As the treaty has not contained Russia's development in the past, a US priority should be the Mach-speed development of immediate and long-term defenses and early-warning systems for adversary HGVs—whether through laser weapons, radio-frequency jammers, or microwave weapons—to counter the hypersonic missiles.[82]

Conclusion and Final Recommendations

As NATO prepares for the emerging technology challenges to critical infrastructure resilience for the next two decades, its member states must be prepared to counter EDTs on two fronts. While traditional adversaries are making strides in their development, terrorists are also gaining ground in using EDTs in peer-to-peer conflicts.

While NATO has made initial strides in expanding innovation and joint defense in this rapidly changing environment, there is much room for improvement. In the area of autonomous weapons, NATO is already

[80] Niamh Cavanagh, "Dark Eagle Has Landed: US to Arm Nuclear Unit in Germany with 4,000 mph 'Dark Eagle' Hypersonic Missiles to 'Blitz Moscow in 21 Mins,'" *Sun* (website), November 11, 2021, https://www.thesun.co.uk/news/16695568/us-nuclear-germany-eagle-hypersonic-missiles-moscow/.

[81] Sayler, *Hypersonic Weapon*s, 22.

[82] Honrada, "US, China Locked."

developing countermeasures and innovation in a coordinated way by incorporating exercises, a whole-of-government approach, and interoperability to operations and technology across the Alliance to hold terrorists and rogue actors at bay. As NATO nations continue to work together to develop and improve the performance of autonomous weapons and counter-UAV technology for the battlefield, they will be able to protect better the critical infrastructure and national security of member states.

The collection of big data and the process that makes it useful—big-data analytics—is changing NATO's preparedness and the way it protects critical infrastructure. Analytics helps to target terrorists and receive early warning of armed conflict, transportation or communication vulnerabilities, nuclear threats, or pandemics more accurately. NATO is in the nascent stages of fully harnessing the advantages of this data and exploring how to share it with nation-states within the Alliance in a secure manner that does not harm national security or civil liberties. While proposals exist for more effective implementation, creating common standards across the Alliance for secure storage, jurisdiction, access, and cybersecurity will remain an important strategic task for nation-states in the future. In addition, NATO nation-states should continue to develop and invest in early-warning systems and use big-data analytics and machine learning to receive foresight on where and when terrorists and malicious actors could escalate armed violence or threaten critical infrastructure.

Finally, as NATO considers its new posture in the hypersonic arms race, it will need to make a strategic decision about the most effective deterrence methods. NATO must determine whether its nation-states should invest in offensive or defensive weapons and identify how to best counter an adversary's new hypersonic technology. Nuclear powers must use a coordinated approach and ensure civil-military cooperation on hypersonic development and countermeasures. This approach will ensure NATO can defend its nation-states in a way that maximizes innovation while considering escalation impacts.

Select Bibliography

Cholpon, Abdyraeva. “Drone Swarms – A Future Threat to Armed Forces?” Finabel – European Army Interoperability Centre (website). December 2, 2020. https://finabel.org/drone-swarms-a-future-threat-to-armed-forces/.

Hoehn, John R. *Joint All-Domain Command and Control: Background and Issues for Congress*. Congressional Research Service (CRS) Report R46725. Washington, DC: CRS, March 18, 2021. https://crsreports.congress.gov/product/pdf/R/R46725/2.

Hu, Junyan, and Alexander Lanzon. “An Innovative Tri-rotor Drone and Associated Distributed Aerial Drone Swarm Control.” *Robotics and Autonomous Systems* 103 (January 2018). https://www.researchgate.net/profile/Junyan-Hu-3/publication/324868897_An_innovative_tri-rotor_drone_and_associated_distributed_aerial_drone_swarm_control/links/5fb6365f458515b79750f6a8/An-innovative-tri-rotor-drone-and-associated-distributed-aerial-drone-swarm-control.pdf.

Johnson, James. “Artificial Intelligence, Drone Swarming and Escalation Risks in Future Warfare.” *RUSI Journal* 165, no.2. https://doi.org/10.1080/03071847.2020.1752026.

Lohmann, Sarah et al. *Navigating New Threats: NATO’s Posture on Emerging Technologies*. Seattle: University of Washington, Henry M. Jackson School of International Studies. March 2022. https://jsis.washington.edu/wordpress/wp-content/uploads/2022/04/22_TF_JSIS-495H_Lohmann.pdf.

Reding, D. F., and J. Eaton. *NATO Science & Technology Trends 2020–2040: Exploring the S&T Edge*. Brussels: NATO Science & Technology Organization, 2020. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf.

Sayler, Kelley M. *Hypersonic Weapons: Background and Issues for Congress*. Congressional Research Service (CRS) Report R45811. Washington, DC: CRS, October 19, 2021. https://crsreports.congress.gov/product/pdf/R/R45811/22.

Shaikh, Shaan, and Wes Rumbaugh. “The Air and Missile War in Nagorno-Karabakh: Lessons for the Future of Strike and Defense.” Center for Strategic and International Studies (website). December 8, 2020. https://www.csis.org/analysis/air-and-missile-war-nagorno-karabakh-lessons-future-strike-and-defense.

— 3 —

NATO Space Critical Infrastructure

Frank J. Kuzminski

ABSTRACT: Space systems provide critical capabilities to enable NATO's core missions of deterrence and defense, including secure satellite communications (SATCOM), positioning, navigation, and timing (PNT), early warning, environmental assessment, and intelligence, surveillance, and reconnaissance (ISR). However, the proliferation of counter-space technologies renders these systems vulnerable to interference and attack. NATO Members must harden their space systems from attacks by state and non-state actors to ensure the resilience of NATO operations in the era of strategic competition.

Keywords: satellites, space, ASAT, ISR, cyber

In December 2019, NATO declared space as the fifth operational domain—alongside land, maritime, air, and cyber—and adopted a space policy recognizing the domain's importance to Alliance operations.[1] Jens Stoltenberg, the NATO Secretary General, remarked "space is extremely important for all civilian and military activities . . . so of course, space and satellites are of great importance for all NATO Allies."[2]

Space technologies and orbital platforms (such as satellites) provide core capabilities to enable NATO's core missions of deterrence and defense. The five core capabilities include secure communications, positioning, navigation, timing (PNT), and velocity; integrated tactical warning and threat

[1] "NATO's Approach to Space," NATO (website), last updated October 6, 2022, https://www.nato.int/cps/en/natohq/topics_175419.htm.

[2] Jens Stoltenberg, "Doorstep Statement by NATO Secretary General Jens Stoltenberg Ahead of the Meeting of NATO Ministers of Foreign Affairs," NATO (website), November 20, 2019, http://www.nato.int/cps/en/natohq/opinions_171016.htm.

assessment; environmental monitoring; communications; and intelligence, surveillance, and reconnaissance (ISR).[3]

Space capabilities enable command and control of NATO forces, provide early warning of potential threats, indicate whether threats are terrorist or nation-based, and improve the amount and quality of information available to Alliance leaders for decision making.[4] NATO's core space capabilities also provide a strategic advantage for Alliance operations worldwide. NATO depends on various national and commercial launch capabilities, platforms, sensors, and space operations that are resilient to environmental and man-made hazards.[5] This chapter will analyze terrorist threats to space assets coming from direct attacks, man-portable air defense systems, electronic warfare, and cyberattacks.

Space technologies, however, are increasingly vulnerable to interference and attack from ground-based orbital threats, including direct-ascent anti-satellite (ASAT) weapons (such as the one China used to destroy a derelict weather satellite in 2007). Cyber or physical attacks can also disrupt tracking stations or control centers. Orbital threats include kinetic counter-space weapons and satellites, which are inherently dual-use technologies.

To fulfill its basic deterrence and mutual defense functions, NATO needs assured and secure access to space. Adversaries could intercept satellites using rendezvous and proximity operations (RPO) to disable, spy on, or neutralize Alliance satellites. In 2018, France accused Russia of using its satellite *Luch* (aka Olymp-K) to attempt an unfriendly espionage act through RPO with the French-Italian communications satellite, *Athéna-Fidus*.[6] Additionally, orbital debris from decades of human space activity will continue to pose collision risks to all objects occupying Earth's low-, medium- and geosynchronous orbital regimes.

Space is a domain in which state actors exert influence and power to pursue interests on Earth and in outer space. As of 2022, there were 12 NATO members operating military or dual-purpose satellites that provide

[3] D. F. Reding and J. Eaton, *Science & Technology Trends 2020–2040: Exploring the S&T Edge* (Brussels: NATO Science & Technology Organization, March 2020), 75–76, https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf.

[4] Kestutis Paulauskas, "Space: NATO's Latest Frontier," NATO (website), March 13, 2020, https://www.nato.int/docu/review/articles/2020/03/13/space-natos-latest-frontier/index.html.

[5] Reding and Eaton, "*Science & Technology Trends 2020–2040*," 76.

[6] "France Accuses Russia of Trying to Spy on Franco-Italian Military Satellite," *France 24* (website), last updated August 9, 2018, https://www.france24.com/en/20180907-france-accuses-russia-trying-spy-franco-italian-military-satellite-espionage-athena-fidus.

space functions for defense purposes. However, only three possess the domestic ability to place satellites into orbit: the United States, France, and the United Kingdom. However, the emergence of commercial operators providing launch services has lowered the threshold of space access for various state and non-state actors. Once the exclusive purview of the superpowers, space and Earth's orbital regimes are increasingly congested, competitive, and contested given the proliferation of spaceflight and orbital capabilities.

The following section covers the four segments of space-critical infrastructure and reviews the space capabilities upon which NATO operations depend. The next section covers the threats facing space-critical infrastructure and reviews the attendant risks and actors that possess the necessary capabilities. The case study looks at threatening Russian behavior in space and against space critical infrastructure. The chapter concludes with recommendations based on NATO's recently published space policy.

Space Critical Infrastructure Overview

Space operations rely on critical infrastructure consisting of four discrete segments: space, user, link, and ground segments.[7] Doctrinally, NATO combines the link segment as part of the other three. This chapter treats the link segment separately, which is useful for analyzing threats against the functions of the link segment. The following section describes each segment in greater detail.

Space Segment

The space segment consists of spacecraft, payloads, and satellite constellations across the various orbital regimes that provide the space-based capabilities upon which NATO forces rely. Examples include the Global Positioning Satellite (GPS) constellation, which consists of 29 satellites operated by the US Space Force in medium-Earth orbit, and the German SAR-Lupe satellite reconnaissance system, among others.[8]

[7] The US Space Force aggregates the ground and link segments into the "control" segment. Separating these segments is useful for threat analysis purposes and is used here. See Brandon Bailey et al., *Defending Spacecraft in the Cyber Domain* (El Segundo, CA: Aerospace Corporation Center for Space Policy and Strategy, November 2019, https://csps.aerospace.org/sites/default/files/2021-08/Bailey_DefendingSpacecraft_11052019.pdf.

[8] "Space Segment," GPS (website), n.d., accessed January 5, 2022, https://www.gps.gov/systems/gps/space/.

User Segment

The user segment refers to any terrestrial device, vehicle, person, or organization with receiver equipment for satellite signals, including positioning, navigation, timing (PNT), and imagery. Examples include automobile navigation systems, smartphones, Internet connections, ATMs, and others. NATO military forces operate in the land, maritime, and air domains, which all comprise the user segment. However, readers should note that large swaths of modern society are part of the user segment, and national economies and industries worldwide depend on space capabilities to function.

Ground Segment

The ground segment incorporates all Earth-based elements of the space architecture and includes space support facilities, launch facilities, mission control centers, and ground stations. The ground segment encompasses the physical infrastructure of NATO space systems and is present in most member states in some fashion. Examples include the European Space Operations Center in Darmstadt, Germany; the Guiana Space Center in Kourou, French Guiana; ground stations located around the world that provide radio links and data storage; and the entire network infrastructure connecting these elements. Ground stations support military operations, day-to-day commercial functions, and space-based science and research initiatives.

Link Segment

Information transmission architecture that connects the ground and space segments comprises the link segment. The architecture includes uplink and downlink data streams, security protocols, and the data that is transmitted. This data includes telemetry and guidance and content for the user segment. For example, communications, PNT data, and imagery are delivered to the user segment via the link segment.

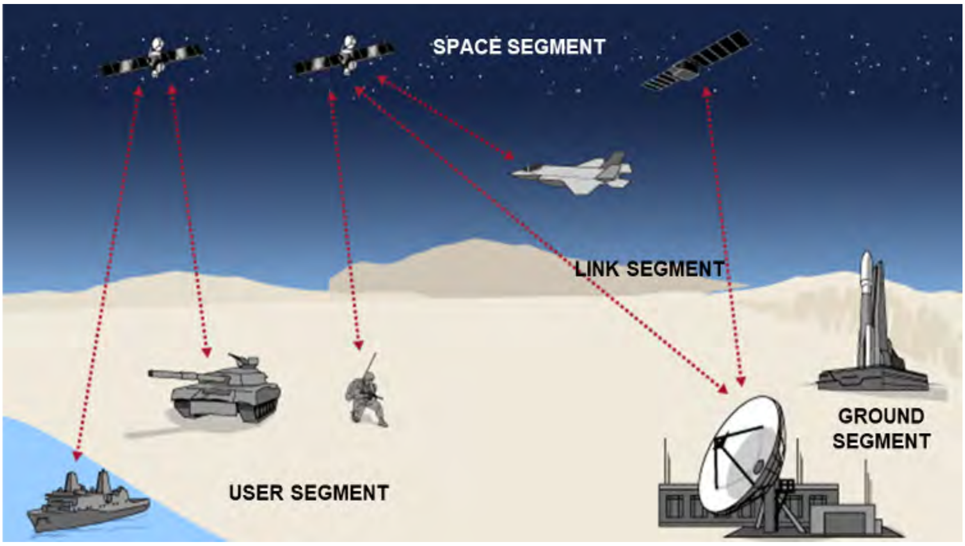


Figure 3-1. Space system and critical infrastructure diagram
Source: US Government Accountability Office (GAO), *Space Acquisitions: Changing Environment Presents Continuing Challenges and Opportunities for DOD,* GAO-22-105900 (Washington, DC: GAO, 2022), https://www.gao.gov/products/gao-22-105900.

Space Support Functions and Capabilities

Space is a resource and technology-intensive domain, and several NATO member states operate advanced space systems across the four segments. The United States is the world's most prolific space power and operates the greatest number of military satellites.[9] The space domain allows Alliance forces to anticipate threats and respond to crises quickly.[10] The space capabilities detailed below build on those outlined in NATO's 2022 Space Policy and the US Department of Defense Joint Publication 3-14 *Space Operations*.[11]

[9] "Satellite Database," Union of Concerned Scientists (website), May 1, 2021, https://www.ucsusa.org/resources/satellite-database.

[10] "NATO's Overarching Space Policy," NATO (website), January 17, 2022, https://www.nato.int/cps/en/natohq/official_texts_190862.htm.

[11] Joint Chiefs of Staff (JCS), *Space Operations*, Joint Publication (JP) 3-14, change 1 (Washington, DC: JCS, October 26, 2020), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_14Ch1.pdf.

Positioning, Navigation, and Timing (PNT) and Velocity

PNT is a mission-essential service provided by Alliance and non-NATO services to the entire user segment. The uses and effects of PNT include precision strike, personnel recovery, combat search and rescue, and digital network timing. The NATO forces in the user segment rely on global navigation satellite systems (GNSS) for precise, accurate, and near-instantaneous geographic location, navigation, and time-reference services during all types of missions.

Integrated Tactical Warning and Threat Assessment

NATO's deterrence and defense missions rely on early warning of missile events to provide decision space for Alliance leaders while enabling effective response measures. Tactical warning is a vital function of NATO's space -critical infrastructure, and the Alliance must maintain access to clear and timely warning information. Persistent overhead monitoring satellites form the backbone of NATO's missile-warning system and provide coverage over key areas and territories. Additionally, ground-based radars in the ground segment help confirm strategic attacks and ballistic trajectories.

Environmental Monitoring

Space systems help planners predict the impact of atmospheric and oceanic effects on NATO operations in the land, sea, and air domains. Accurate weather forecasting and understanding maritime conditions mitigate air and maritime operations risk while enabling flight planning for patrols over NATO airspace. Weather forecasting also supports threat assessments and munitions selection.

Satellite Communications (SATCOM)

Satellite communication is vital for effective command and control at the tactical, operational, and strategic levels, supporting forces operating in remote areas. Satellite communication enables over-the-horizon and beyond line-of-sight voice and data communication for NATO forces. Satellite communication also enables unmanned aerial system (UAS) operations supporting NATO missions. As part of recent investments to improve SATCOM capabilities, the NATO Communications and Information (NCI) Agency has partnered with France, Italy, the United Kingdom, and the United States, for SATCOM services under NATO SATCOM Services Sixth Generation (NSS6G) Project.

Satellite communication is also where the space and cyber domains intersect across the four space segments. The data transmission networks that enable ground stations to command-and-control satellites in orbit and enable forces in the user segment to utilize satellite capabilities exist in the cyber domain. The medium over which data transmission occurs in the link segment relies on communication protocols derived from the cyber domain.

Intelligence, Surveillance, Reconnaissance (ISR)

Alliance military operations rely heavily on space-based services for ISR. Operational and tactical planning requires accurate satellite imagery to understand the effects of terrain on land-based operations. Sophisticated orbital capabilities like synthetic aperture radar and remote sensing enable decision making at the strategic level with timely and accurate information that reduces uncertainty and risk during crises.

Space Situational Awareness (SSA)

The importance of the space domain to Alliance operations and daily life demands that NATO maintain continuous situational awareness of objects, activities, and actors across the orbital regimes to anticipate and identify risks. Spatial situational awareness is an emerging capability in response to the proliferation of actors and threats in the space domain. Spatial situational awareness enables effective command and control in support of Alliance operations while providing a timely understanding of the space environment.

NATO forces have access to the most advanced space infrastructure in the world. However, this access is not assured, and planners and policymakers cannot assume space will remain an uncontested domain. Moreover, technological advances have democratized the benefits of space to a wide range of actors. Commercially available drones with onboard satellite navigation and mapping can be improvised into precision-guided explosives. In contrast, commercial mapping services such as Google Maps can provide detailed satellite images of potential targets for terrorist attacks within member states. Criminal organizations, violent extremist organizations (VEO), and adversary states can also utilize the space capabilities detailed above, thanks to the ubiquity of smart devices and satellite imagery on the Internet. The next section, however, will focus on the main threats facing NATO space critical infrastructure.

Threats and Vulnerabilities

The growing ubiquity of commercial and national space technologies suggests potential threat actors will seek to leverage space for the same advantages as NATO.[12] There are generally five categories of space threat actors, plus the space environment itself, which is hazardous to Alliance space capabilities. This discussion will focus on threat actors, including insider threats, criminal gangs, terrorists/VEOs, non-state actors, and state actors. In terms of technical complexity, each type of threat actor is capable of low-threshold threats, while only state actors with advanced space programs are capable of high-end threats.

The threats affecting NATO's space capabilities exist on Earth and in orbit and range from crude attacks resulting in physical destruction to space support facilities on Earth, sophisticated counter-space weapons deployed on orbital platforms, and the growing orbital debris problem. Lower threshold threats may cause temporary disruptions to Alliance space functions and local operations, while higher threshold threats could render catastrophic consequences to the security of NATO members. Generally, terrorist actors possess the ability to cause temporary disruptions to space infrastructure. However, the most significant threats are the most technically complex and thus will likely remain exclusive to advanced state actors (see figure 3-1).

The following threats have a lower technical and resource threshold and are available to various actors seeking to disrupt critical space infrastructure. Attacks can still cause much damage and impair vital functions but are generally reversible in terms of NATO's ability to continue to access space and space support functions.

Direct Attack

NATO's orbital capabilities depend on the space support functions provided by various military and civilian organizations with facilities located around the globe. Some facilities (such as France's Guyana Space Center or the United States' Kennedy Space Center) host vital space launch and space support facilities located on military installations or supported by the host nation's military forces. They are, therefore, relatively secure from direct attacks. For example, in French Guyana, France's 3rd Regiment

[12] Reding and Eaton, "*Science & Technology Trends 2020–2040*," 82.

of the Foreign Legion is tasked with defending the facility from direct attack by terrorists or VEOs.[13]

Other facilities, however, including the ESA's European Space Operations Centre (ESOC), located in Darmstadt, Germany, are primarily civilian. They are often situated in congested metropolitan areas and easily accessible by public transportation. The ESOC and other civilian facilities perform vital space support functions and operate many satellites that NATO relies upon to conduct its missions.[14] Nevertheless, despite local security, they could remain particularly vulnerable to terrorist attacks, including car/truck bombings, mass shootings, or suicide attacks.

A terrorist attack, such as the 2015 Paris shootings, against a key element of the ground segment could result in catastrophic physical destruction to vital space support facilities and the loss of life among space professionals, technicians, and engineers who operate Alliance satellites. While such damage and loss of life would be devastating, the impact on NATO's ability to use satellites and perform its core missions would likely be relatively low. There is sufficient redundancy in satellite operation and tracking or launch services. For example, isolated direct attacks against these facilities would not meaningfully disrupt NATO's ability to obtain PNT data from the GPS constellation or for intelligence organizations to utilize satellite imagery for reconnaissance purposes. In other words, an isolated terrorist attack against the ground segment, while devastating, would have a limited impact on NATO's overall space critical infrastructure.

Man-portable Air Defense Systems (MANPADS)

MANPADS are lightweight air defense systems designed to protect ground-based forces from air attacks. Widely distributed during the Cold War, terrorist organizations and insurgent groups throughout Africa, the Middle East, and Central Asia have acquired MANPADS through theft, illicit arms transfers, black market sales, and capture due to loss of inventory control. Prolific examples include the US-made FIM-92 Stinger and the Soviet/Russian-made 9K32 Strela-2 (NATO designation SA-7 Grail). Additionally, there have been several documented events of terrorist actors firing MANPADS against military and civilian aircraft. For example, in November 2002, al-Qaeda–affiliated terrorists fired two Strela-2 missiles

[13] "3rd Foreign Infantry Regiment," French Foreign Legion (website), 2022, https://foreignlegion.info/units/3rd-foreign-infantry-regiment/.

[14] "Where Missions Come Alive," European Space Agency (website), n.d., https://www.esa.int/About_Us/ESOC/Where_missions_come_alive.

at an Israeli civilian Boeing 737 airliner departing from Mombasa, Kenya.[15] Additionally, in March 2020, the US Federal Aviation Administration issued a notice to airmen (NOTAM) warning civilian aircraft of the surface-to-air missile threat near Kabul, Afghanistan. The NOTAM was issued because Taliban insurgents had acquired MANPADS and fired them against NATO aircraft taking off from Bagram airfield.[16]

Terrorist organizations could conceivably target a space launch in a manner similar to attacks against civilian and military aircraft taking off from airports around the world. Due to their widespread availability, MANPADS are an attractive choice for terrorists seeking to attack a symbolic target such as an airliner or rocket. Unlike military aircraft, which carry effective countermeasures against surface-to-air threats, rockets are unarmed and highly vulnerable to MANPADS. While highly symbolic and devastating in its immediate impact, a successful terrorist attack against a space vehicle launch would likely not disrupt NATO's overall space infrastructure or ability to exploit space support functions for routine operations.

Electronic Warfare (EW)

Satellites beam signals to Earth and transmit their data to end users via a defined set of radio frequencies across the electromagnetic spectrum. Spectrum and signal interference, or jamming, using radio emissions from adjacent spectrum bands, deliberately or accidentally, can degrade vital space functions, including PNT and communications.[17]

The International Telecommunications Union (ITU) and the United Nations agency regulate and coordinate global radio frequency (RF) spectrum allocations. Positioning, navigation, and timing signals from GPS or GNSS satellites operate along a segment of the RF spectrum known as the L-Band, with a frequency range between 1 to 2 gigahertz, with satellites specifically operating between 1525 to 1660.5 megahertz.[18]

[15] Martin Landauer, "The Threat from MANPADS," Royal United Services Institute (website), November 14, 2007, https://rusi.org/publication/threat-manpads.

[16] "FAA Background Information Regarding U.S. Civil Aviation in the Kabul Flight Information Region (OAKX)," Federal Aviation Administration (website), March 28, 2021, https://www.faa.gov/air_traffic/publications/us_restrictions/media/Afghanistan-Background_Notice-28_MAR_2021.pdf.

[17] "GPS Spectrum and Interference Issues," GPS (website), accessed September 29, 2021, https://www.gps.gov/spectrum/.

[18] Radio signals in the L-Band are ideal for PNT and communications use because these waves can travel long distances and penetrate Earth's weather and vegetation. Jill C. Gallagher, Alyssa K. King, and Clare Y. Cho, "Spectrum Interference Issues: Ligado, the L-Band, and GPS," Congressional Research Service (CRS) Report IF11558 (Washington, DC: CRS, May 28, 2020), https://crsreports.congress.gov/product/pdf/IF/IF11558/2.

Jamming RF signals in the L-Band is relatively easy and cheap, requiring powerful broadcast equipment to transmit interference signals in the appropriate frequency range. Although illegal in many countries, GPS signal jammers can be purchased or manufactured with readily available electronic equipment.

For criminal and terrorist actors, satellite signal jamming is most effective in a localized and targeted manner. Commercially available "privacy-seeking" jammers are difficult to detect while far less capable than military EW capabilities. Criminals and terrorists could disrupt financial services and trading at stock exchanges, which rely on precise timing for financial transactions.[19] For example, actors seeking to disrupt Alliance military forces operating in remote areas, could also easily jam GPS and communications signals as part of a broader complex attack against NATO forces. However, on a larger-scale, state actors, including Iran and Russia, possess the technical ability to jam GPS signals across a large area.

Cyber Threats and Effects

In recent years, the proliferation of cyber threats and cyber-capable actors has posed many threats to Alliance's critical infrastructure, including in space. Satellites and their services are vulnerable to cyber threats because they often operate and rely on a digital network to communicate with operators and users on the ground. Additionally, much of the equipment across the four space segments linking space critical infrastructure to users on Earth employs commercial hardware, firmware, and software. There is an inescapable interdependence between the space and cyber domains. Since these systems contain known and unknown vulnerabilities affecting cyber and space domains, all segments of the space system depend on updates and patching from manufacturers. Space systems and cybersecurity are inherently linked.

Cyber threats, including malware, hacking, spoofing, and denial of service, can affect NATO's space infrastructure: space segment, user segment, link segment, and ground segment. Depending on the intent, attackers can achieve command and control system intrusions to affect satellite orbits, payload disruption, signal disruption, or data skimming, among other risks.[20] Motivated attackers can also use sophisticated cyber techniques

[19] Tegg Westbrook, "The Global Positioning System and Military Jamming: Geographies of Electronic Warfare," *Journal of Strategic Security* 12, no. 2 (2019): 9.

[20] Bailey et al., *Defending Spacecraft*, 3.

for denial-of-service attacks against space infrastructure across all segments of the space system, resulting in loss of services and capabilities. At worst, sophisticated attackers could hijack NATO satellites and disrupt their orbits or compromise sensitive payloads.[21]

Cyber threats against space systems offer advantages to would-be attackers due to the relatively low cost and potential for high-impact disruptions to NATO operations and the attribution challenge which can obfuscate the responsible party.[22] As a result, cyber threats against NATO space critical infrastructure are an attractive option for the determined and well-resourced threat actors. While non-state actors, including criminal and terrorist organizations may lack the skill set and resources to target and strike specific targets through the cyber domain, they may occasionally achieve some success, given the unpredictable and uncertain nature of cyberspace vulnerabilities.

The following higher consequence threats to NATO space critical infrastructure may cause irreversible damage to space systems and support functions. Due to their technical complexity, they are generally within the capability scope of advanced state actors.

Direct Ascent Anti-Satellite Weapon (ASAT)

Ground-launched anti-satellite weapons, known as ASATs, are a significant threat to satellites. They allow threat actors to destroy a satellite with a kinetic kill vehicle launched atop a missile from an Earth-based platform. The kinetic destruction produces a debris field that remains in Earth's orbit and poses collision risks to other satellites.

In January 2007, China successfully tested an ASAT in a show of force when it destroyed a derelict weather satellite known as Fengyun using a medium-range ballistic missile.[23] The act, widely condemned by other countries and proponents of civilian space flight, generated a persistent debris cloud and demonstrated China's ability to target an adversary's space-based infrastructure in a potential future conflict. Up to that point, only the United States and Russia demonstrated such a capability.

India has also demonstrated an ASAT capability. The country shot down one of its satellites using a modified ballistic missile defense

[21] Joan Johnson-Freese, *Space Warfare in the 21st Century: Arming the Heavens* (New York: Routledge, 2017), 97.

[22] Johnson-Freese, *Space Warfare*, 43.

[23] William J. Broad and David E. Sanger, "China Tests Anti-Satellite Weapon, Unnerving U.S.," *New York Times* (website), January 18, 2007, https://www.nytimes.com/2007/01/18/world/asia/18cnd-china.html.

interceptor in March 2017 in a show of force mission called Shakti.[24] In November 2021, Russia destroyed a derelict satellite weighing over 2,000 kilograms.[25] The event drew swift condemnation from NATO and other space actors and created a sizable debris field that threatened the International Space Station (ISS).[26] NASA had to alert the ISS crew to evacuate into their escape capsule until the threat diminished. While no country has ever shot down an adversary's satellite during a conflict, NATO must remain vigilant of the growing risks to its space critical infrastructure with the proliferation of ASAT capabilities and the debris any kinetic attack in orbit will create.

Rendezvous and Proximity Operation (RPO) and Intercept

Advanced satellite operators can maneuver and alter satellite orbits to rendezvous with other orbital platforms. Known as rendezvous and proximity operations (RPO), these maneuvers are often benign and deliberate, such as a manned capsule docking with the International Space Station. This ability suggests operators can intercept satellites situated in predictable orbits, especially in low-Earth orbit (LEO), for nefarious purposes. Malign actions include satellite capture, signal intercept for espionage purposes, or ramming one satellite into another in a kinetically destructive maneuver (in extreme circumstances).[27]

Rendezvous and proximity operation capability primarily rests within the purview of state actors. However, legitimate business and commercial interests exist in pursuing RPO and satellite-capture technologies. Several aerospace firms and startup companies are developing

[24] Jeff Foust, "India Tests Anti-Satellite Weapon," SpaceNews (website), March 27, 2019, https://spacenews.com/india-tests-anti-satellite-weapon/.

[25] Jeff Foust, "Russia Destroys Satellite in ASAT Test," SpaceNews (website), November 15, 2021, https://spacenews.com/russia-destroys-satellite-in-asat-test/.

[26] "Statement by the North Atlantic Council on the Recent Anti-Satellite Missile Test Conducted by the Russian Federation," NATO (website), November 19, 2021, https://www.nato.int/cps/en/natohq/news_188780.htm. Regarding the International Space Station astronauts seeking shelter, see also Joey Roulette, "Debris from Test of Russian Antisatellite Weapon Forces Astronauts to Shelter," *New York Times* (website), November 16, 2021, https://www.nytimes.com/2021/11/15/science/russia-anti-satellite-missile-test-debris.html.

[27] Johnson-Freese, *Space Warfare*, 143.

maintenance satellites to repair and refuel existing satellite constellations.[28] Space infrastructure servicing, including satellite refueling and debris mitigation, is a developing and ostensibly beneficial capability that can extend the service life of orbital payloads and declutter Earth's orbital regimes. Satellite servicing is promising for improving the resilience of space systems. However, from a security perspective, the same spacecraft used to repair or refuel a satellite can also be used to intercept signals, damage, or deliberately deorbit an adversary's satellites.[29] Absent operating standards and security norms, the proliferation of RPO capability to commercial entities and non-state actors for space servicing exposes another vector that can be exploited through cyber or other means to threaten Alliance satellites.[30]

Orbital Counter-Space Weapon (Directed Energy and Kinetic)

With perhaps the highest level of technical complexity, orbital counter-space weapons also pose the highest risk of irreversible and catastrophic damage to NATO's space critical infrastructure. These weapon systems include directed energy (such as laser) and kinetic weapons (such as swarms of nanosatellites) that can disable satellites from orbit. Several states, including France and the United States, have announced plans to deploy or study such capabilities in the future to defend their national space systems. France described nanosatellites as "key areas of defense" and announced plans to deploy "active defense measures" in space in its 2019 space defense strategy, while the US has explored the potential of nanosatellites for defensive purposes.[31] Additionally, General John W. Raymond, the US chief of space operations, testified before Congress on June 16, 2021, that directed energy is one of "several of the emerging technologies that are necessary to integrate

[28] Examples include Northrop Grumman's successful test of its Mission Extension Vehicle-1 (MEV-1) in February 2020, and the Ukrainian startup Krus Orbital, which plans to launch a service satellite in 2023. Caleb Henry, "Northrop Grumman's MEV-1 Servicer Docks with Intelsat Satellite," SpaceNews (website), February 26, 2020, https://spacenews.com/northrop-grummans-mev-1-servicer-docks-with-intelsat-satellite/; and Sandra Erwin, "Startup Using Soviet-Era Technology to Build Satellite Servicing Vehicle," SpaceNews, (website) March 10, 2021, https://spacenews.com/space-startup-using-soviet-era-technology-to-build-satellite-servicing-vehicle/.

[29] Saadia M. Pekkanen, "Neoclassical Realism in Japan's Space Security," in *The Oxford Handbook of Japanese Politics*, ed. Robert J. Pekkanen and Saadia M. Pekkanen (Oxford, UK: Oxford University Press, 2021), 775.

[30] Hussain Bokhari, "NSR Insight: In-orbit Servicing: Stepping Up to the Challenge?," satnews (website), February 17, 2021, https://news.satnews.com/2021/02/17/nsr-insight-in-orbit-servicing-stepping-up-to-the-challenge/.

[31] *Stratégie spatiale de Défense: Rapport du Groupe de Travail "Espace"* (Paris: Ministère des Armées, July 2019), 32, https://www.vie-publique.fr/sites/default/files/rapport/pdf/194000642.pdf.

into the Space Force architectures to stay ahead of potential adversaries.[32] Notwithstanding the high debris-generating potential of such weapons, a shooting war involving NATO extending to space poses catastrophic risks to the Alliance's space-critical infrastructure and humanity's long-term access to space.[33]

Orbital Debris

This chapter mentions orbital debris, a pernicious problem to space infrastructure that will only worsen as humans continue to place more objects in space. Orbital debris is an objective hazard endemic to the orbital regimes which NATO's space infrastructure occupies.[34] Thanks to orbital mechanics, space junk usually remains in orbit rather than decay into the Earth's atmosphere, posing a persistent risk to space flight. In this view, orbital debris presents a space safety challenge to be mitigated through norms and behaviors. While not a military or security problem, NATO's ability to utilize space reliably for its core missions necessitates a cooperative approach with all space-faring nations to reduce the dangers of orbital debris.

Case Study – Russia as a Threat Actor in the Space Domain

Russia inherited the Soviet space program after the fall of communism and the end of the Cold War. While the Russian space program withered during the 1990s, the country has devoted considerable time and resources during the last 20 years to building its space program, especially its coercive space capabilities. The following case study examines Russia's threatening behavior in the space domain. Specifically, the case study considers four categories of space domain threats: rendezvous and proximity operations (RPO), electronic warfare and jamming, direct-ascent anti-satellite weapons (DA-ASAT), and cyber disruption.

[32] David Vergun, "Nanosatellites Could Play Pivotal Role in Defense against Enemy Missiles," DOD News (website), July 12, 2021, https://www.defense.gov/News/News-Stories/Article/Article/2685840/nanosatellites-could-play-pivotal-role-in-defense-against-enemy-missiles/. See also *Department of the Air Force Posture Statement: Fiscal Year 2023 before the House Armed Services Committee* (statements of Frank Kendall, secretary of the Air Force, General Robert W. Raymond, chief of space operations, US Space Force, and General Charles Q. Brown Jr., chief of staff, US Air Force, June 16, 2021), https://www.af.mil/Portals/1/documents/2022SAF/FY23_DAF_Posture_Statement.pdf.

[33] Rob Waugh, "France to Launch 'Fearsome' Satellites 'Armed with Powerful Lasers' into Space," Yahoo! Finance (website), July 30, 2019, https://finance.yahoo.com/news/france-to-launch-fearsome-satellites-armed-with-powerful-lasers-into-space-193707222.html.

[34] "What is Orbital Debris?" NASA (website), https://www.nasa.gov/audience/forstudents/5-8/features/nasa-knows/what-is-orbital-debris-58.html.

Rendezvous and Proximity Operations – 2015 through 2019

As early as 2015, the Russian satellite *Luch* (aka *Olymp-K*) conducted additional orbital maneuvers after entering the geosynchronous orbital regime (GEO). By 2019, *Luch* occupied at least 16 distinct orbital positions, which is unusual because most satellites maintain a stationary position relative to the Earth once in GEO.[35] Several commercial and state-level satellite operators criticized the Russians for what they viewed as inappropriate and concerning behavior in the fragile orbital regime, which extends over 35,000 kilometers (22,000 miles) above the Earth. Intelsat, a commercial satellite services provider, reported that *Luch* occupied a position between two operational Intelsat satellites for nearly three months.[36] In 2018, France's Armed Forces Minister Florence Parly accused Russia of maneuvering *Luch* dangerously close to the French-Italian military communications satellite *Athéna-Fidus*. Parly called this maneuver an "unfriendly act" of espionage.[37] Later in 2019, *Luch* approached *Intelsat 36* in GEO and closed to a distance less than 1.8 kilometers.[38] By comparison, the average distance between satellites occupying stationary positions in GEO is 207 kilometers.[39]

The *Luch* satellite maneuvers are perhaps the most prolific example of provocative RPO by Russia. However, Russia appears to have been refining its RPO capabilities since at least 2013, when it launched several military satellites that conducted RPO with other Russian satellites. The military utility of *Luch* and Russia's other RPO-capable satellites appears to be surveillance, co-orbital inspection, and intelligence gathering.[40] Rendezvous and proximity operations capability could also support targeting and tracking other counter-space attacks, including direct-ascent ASAT.

Russian satellite maneuvers (such as those described above) are not illegal by international standards. Evidence suggests, however, that Russia's behavior

[35] Thomas G. Roberts, "Unusual Behavior in GEO: *Luch* (*Olymp-K*)," Aerospace Security: A Project of the Center for Strategic and International Studies (website), last updated September 1, 2022, https://aerospace.csis.org/data/unusual-behavior-in-geo-olymp-k/.

[36] Brian Weeden, "Dancing in the Dark Redux: Recent Russian Rendezvous and Proximity Operations in Space," Space Review (website), October 5, 2021, https://www.thespacereview.com/article/2839/1.

[37] "France Accuses Russia of Trying to Spy on Franco-Italian Military Satellite," *France24* (website), September 7, 2018, https://www.france24.com/en/20180907-france-accuses-russia-trying-spy-franco-italian-military-satellite-espionage-athena-fidus.

[38] Colin Clark, "US, China, Russia Test New Space War Tactics: Sats Buzzing, Spoofing, Spying," Breaking Defense (website), October 28, 2021, https://breakingdefense.sites.breakingmedia.com/2021/10/us-china-russia-test-new-space-war-tactics-sats-buzzing-spoofing-spying/.

[39] Roberts, "Unusual Behavior."

[40] Brian Weeden and Victoria Samson, *Global Counterspace Capabilities: An Open Source Assessment* (Washington, DC: Secure World Foundation, April 2021), 2–13.

relative to other satellites increased the risk of collision. It also demonstrates sophisticated and precise space situational awareness capability, enabling the Russian satellite to loiter for extended periods and collect uplink data from Alliance ground stations.[41] The *Luch* incidents exposed the vulnerability of civilian and NATO space infrastructure to RPO, which is inherently a dual-use capability that could be used in a counter-space capacity in the future. These developments suggest additional measures, including transparency, monitoring, and norms, may be necessary to mitigate the risks of such acts in the future.

Jamming – 2017 and 2018

In 2017, civilians and commercial airliners in Scandinavia reported GPS signal disruption and degraded PNT data during periods corresponding with military exercises in the region.[42] Norway reported the signal disruptions during Russia's Zapad-17 exercise in conjunction with NATO's Trident Juncture exercise in 2018 and the United Kingdom's Clockwork exercise in 2019.[43] On more than one occasion, Norway's Civil Aviation Authority issued a notice to airmen (NOTAM) about the GPS signal disruptions in the vicinity of the Arctic Circle.[44] The signal disruptions affected GPS, the PNT satellite constellation owned and operated by the US Space Force. The specific nature of the disruptions suggests Russia used electronic warfare assets to jam the GPS signals in a target fashion.

Electronic warfare, which includes jamming and spoofing, is not new to conflict. Jamming is the deliberate transmission of signal noise across one or more targeted frequencies to corrupt data transmissions or overload transceiver circuits.[45] Spoofing differs from jamming in that it introduces false or misleading data to compromise the signal's integrity and allows an adversary to gain control of a system.[46] The implications of jamming and spoofing for NATO forces that rely on reliable PNT data are serious. PNT signal jamming or spoofing can lead forces astray during complicated maneuvers along international boundaries or compromise targeting data used

[41] Clark, "US, China, Russia Test."

[42] Alexandra Coultrup, "GPS Jamming in the Arctic Circle," Aerospace Security: A Project of the Center for Strategic and International Studies (website), March 31, 2020, https://aerospace.csis.org/data/gps-jamming-in-the-arctic-circle/.

[43] Coultrup, "GPS Jamming."

[44] Coultrup, "GPS Jamming."

[45] Westbrook, "Global Positioning System," 2.

[46] Westbrook, "Global Positioning System," 3.

by precision-guided munitions during crises. Under extreme circumstances, these events can create a pretext for an adversary to escalate a crisis.

During Zapad-17, Norway's Foreign Ministry confronted Russian authorities about jammed GPS signals affecting commercial airline traffic near the Finnmark region in northern Norway.[47] The exercise involved thousands of Russian troops near the Arctic Circle, with troops maneuvering to within 10 kilometers of the Russian-Norwegian border.[48] Similarly, during Trident Juncture the following year, NATO and Norway's Defense Ministry accused Russia of jamming GPS signals from the country's Kola Peninsula. NATO Secretary General Stoltenberg noted that the Alliance has seen "that cyber, electronic warfare, [and] electronic means are used more frequent[ly] in different operations."[49] Defense analysts believe the EW capabilities deployed during Trident Juncture are the same ones Russia tested during Zapad-17 the previous year, suggesting jamming will become a regular part of Russian military activity.[50]

Direct Ascent Anti-Satellite (DA-ASAT) Weapon Test – 2021

Russia possesses one of the world's most prolific direct-ascent ASAT (DA-ASAT) capabilities, which it began testing in the Soviet era during the Cold War. As of 2021, Russia possessed three primary DA-ASAT systems: PL-19 Nudol, a ground-launched ballistic missile capable of intercepting targets in low-earth orbit (LEO); Burevestnik, an air-launched DA-ASAT that can reach LEO to intercept targets or possibly deploy a hypersonic missile; and S-500, a ballistic missile with a next-generation exo-atmospheric kill vehicle that is still in development.[51] In November 2021, Russia successfully demonstrated the operational capability of its PL-19 Nudol DA-ASAT when it destroyed the Cosmos-1408 satellite in LEO at an altitude of approximately 485 kilometers.[52]

According to the US Space Command (USSPACECOM), the Russian test produced over 1,500 pieces of trackable space debris and posed

[47] Westbrook, "Global Positioning System," 7.

[48] Westbrook, "Global Positioning System," 7.

[49] Brooks Tigner, "Electronic Jamming between Russia and NATO Is Par for the Course in the Future, but It Has Its Risky Limits," *New Atlanticist* (blog), November 15, 2018, https://www.atlanticcouncil.org/blogs/new-atlanticist/electronic-jamming-between-russia-and-nato-is-par-for-the-course-in-the-future-but-it-has-its-risky-limits/.

[50] Tigner, "Electronic Jamming."

[51] Weeden and Samson, *Global Counterspace Capabilities*.

[52] Foust, "Russia Destroys Satellite."

an immediate risk to the astronauts aboard the International Space Station, including two Russian cosmonauts.[53] Shortly after *Cosmos-1408* broke apart, NASA ground control notified the crew to take emergency safety procedures when it became apparent the space station would pass "through or near the vicinity of the debris cloud."[54] World leaders widely condemned the event, while Russia denied the test posed any risk to the International Space Station or other space activities.[55] The intensity of worldwide condemnation was similar to the criticism against China after its 2007 DA-ASAT test, which also produced large amounts of space debris.[56]

Russia launched the Nudol interceptor from the Plesetsk Cosmodrome, located about 800 kilometers north of Moscow.[57] Analysis of the PL-19 Nudol missile suggests Russia possesses an operational DA-ASAT capability to threaten credibly any satellite or spacecraft in LEO.[58] The worldwide condemnation following the event suggests Russia was willing to bear reputational and material costs to signal the credibility of its coercive capacity in LEO.

When viewed as a coercive tool, Russia's DA-ASAT capability is another point of leverage to threaten objects of significant value to its adversaries. Russia knows that NATO forces depend on space-based capabilities for missions and operations. Possessing a credible capability to threaten satellites in LEO, Russia has armed itself with another tool to reinforce its bargaining power vis-à-vis NATO and the United States.[59] Given the peculiarities of the space environment and orbital mechanics, all space-faring actors share common interests in maintaining stable and safe access to space. Uncertainty surrounding Russia's interests and intentions in space complicates the overall bargaining situation and

[53] Theresa Hitchens, "Russian Suspected Ground-Launched ASAT Test Scatters Dangerous Debris through LEO," Breaking Defense (website), November 15, 2021, https://breakingdefense.sites.breakingmedia.com/2021/11/suspected-russian-ground-launched-asat-test-scatters-dangerous-debris-through-leo/.

[54] Bill Nelson, "NASA Administrator Statement on Russian ASAT Test," NASA (website), November 15, 2021, https://www.nasa.gov/press-release/nasa-administrator-statement-on-russian-asat-test.

[55] "Военные РФ подтвердили, что сбили советский спутник в ходе испытаний," Interfax (website), November 16, 2021, https://www.interfax.ru/russia/803293.

[56] Broad and Sanger, "China Tests Anti-Satellite Weapon."

[57] Hitchens, "Test Scatters Dangerous Debris."

[58] Todd Harrison et al., *Space Threat Assessment 2022* (Washington, DC: Aerospace Security Project/Center for Strategic and International Studies, 2022), https://www.csis.org/analysis/space-threat-assessment-2022.

[59] For a discussion on coercion and credible threats as instruments of bargaining, see Thomas C. Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 1966), 2–8.

reinforces the need for NATO to maintain its credible deterrent and coercive capabilities.

Disruption of Ukrainian Satellite Communications – 2022

When Russia invaded Ukraine on February 24, 2022, Russian forces attacked along multiple axes to seize key terrain. Shortly before the invasion began, Russian hackers targeted the Viasat KA-SAT commercial satellite communications network by attacking modems and routers in the user segment with malware.[60] The malware attack disabled thousands of systems by erasing all data using "wiper" malware called AcidRain.[61] This attack was significant because the Viasat provides high-bandwidth Internet and satellite communications to the Ukrainian government and military, civilian, and commercial customers. While the attack targeted Ukrainian users, thousands of civilian customers across the European Union were also affected, including NATO members. According to US Secretary of State Antony Blinken, the attack was meant "to disrupt Ukrainian command and control during the invasion" and to provide Russian forces a tactical advantage.[62] Cybersecurity analysts in several NATO and EU countries also attributed the attack to the Russian military.[63]

As Russian forces descended on Kyiv and surrounding areas during the early days of the invasion, Ukraine's command-and-control network had been disabled. With military communications "completely paralyzed," commanders had to move physically to unit locations to assess the situation

[60] Schelling, *Arms and Influence*, 2–8.

[61] Patrick Howell O'Neill, "Russia Hacked an American Satellite Company One Hour before the Ukraine Invasion," *MIT Technology Review* (website), May 10, 2022, https://www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine-invasion/.

[62] James Pearson, "Russia Downed Satellite Internet in Ukraine – Western Officials," Reuters (website), May 10, 2022, https://www.reuters.com/world/europe/russia-behind-cyberattack-against-satellite-internet-modems-ukraine-eu-2022-05-10/.

[63] "Russia behind Cyberattack with Europe-Wide Impact an Hour before Ukraine Invasion," National Cyber Security Centre (website), May 10, 2022, https://www.ncsc.gov.uk/news/russia-behind-cyber-attack-with-europe-wide-impact-hour-before-ukraine-invasion#:~:text=Russia%20has%20been%20behind%20a,its%20major%20invasion%20of%20Ukraine; and Colin Demarest, "US and Allies Blame Russia for Viasat Hack Ahead of Ukraine Invasion," C4ISRNet (website), May 11, 2022, https://www.c4isrnet.com/smr/geoint/2022/05/11/us-and-allies-blame-russia-for-viasat-hack-ahead-of-ukraine-invasion/.

and issue orders.[64] For its part, Viasat required weeks to ship replacement units to customers in Ukraine and elsewhere in Europe to restore SATCOM.

The attack demonstrates how multi-domain effects in space and cyber critical infrastructure can have persistent effects during a conflict and are an enduring feature of the modern battlefield. The attack also reveals the interdependence between space critical infrastructure and cyberspace and illustrates the effects adversaries can deliver against NATO's space critical infrastructure by exploiting cyberspace vulnerabilities. While Ukraine is not a NATO member, Viasat is an American commercial telecommunications firm providing vital SATCOM to Ukrainian government and military users. In this respect, the Viasat SATCOM network comprises Ukraine's space critical infrastructure because of the degree to which Ukraine's ability to defend against Russian aggression depends on commercial SATCOM.

Recommendations

NATO faces serious challenges in the space domain. Technology proliferation and the importance of space capabilities for nearly all modern society functions demonstrate the critical vulnerabilities of NATO space systems. The following recommendations build on existing efforts to instill norms and best practices in space by all actors while hedging against the increasing likelihood that adversaries may target NATO space systems in a future crisis.

Promote Norms for Responsible Behavior in Space by All Actors

The best way to mitigate security risks in the space domain, especially from debris-generating events like kinetic ASAT weapon strikes, is for all space actors, state, and non-state alike, to observe norms and tenets of responsible behavior in space.[65] These tenets include transparency of intent and clear communication, avoiding debris generation and harmful interference, and maintaining predictable and safe orbital trajectories.[66] In April 2020, the United States declared a moratorium on direct-ascent, debris-producing

[64] Paul Sonne et al., "Battle for Kyiv: Ukrainian Valor, Russian Blunders Combined to Save the Capital," *Washington Post* (website), August 24, 2022, https://www.washingtonpost.com/national-security/interactive/2022/kyiv-battle-ukraine-survival/.

[65] Lloyd J. Austin III, secretary of defense, to Secretaries of the Military Departments, Chairman of the Joint Chiefs of Staff, Under Secretaries of Defense, Chiefs of the Military Services, Commanders of the Combatant Commands, General Counsel of the Department of Defense, and Directors of Defense Agencies, "Tenets of Responsible Behavior in Space," July 7, 2021, https://media.defense.gov/2021/Jul/23/2002809598/-1/-1/0/TENETS-OF-RESPONSIBLE-BEHAVIOR-IN-SPACE.PDF.

[66] Austin, "Tenets of Responsible Behavior in Space."

kinetic ASAT testing.[67] NATO should encourage its members to observe the tenets of responsible behavior in space while reaffirming the mutual defense provisions of Article 5 for the protection of Allied space systems.

Incorporate Space Capabilities and Considerations into All Aspects of NATO Operational Planning

NATO can no longer assume that space is a benign environment and must consider that future competition and conflict will extend to the space domain. NATO's access to space capabilities is not guaranteed. Planners must anticipate threats and challenges and plan for space operations to mitigate those risks while preserving the key space roles required for NATO operations. Additionally, every NATO exercise should incorporate space elements and planning considerations that include as many Alliance members as possible

Maintain and Expand Partnerships with Commercial Operators

Commercializing certain aspects of NATO space systems (such as deploying passive NATO payloads on commercial satellites) can potentially reduce uncertainty about the purpose of military satellites and reduce risks associated with a security dilemma in the space domain.[68] Coupled with growing international consensus about the need for norms to govern behavior in space, contracting certain space capabilities to commercial operators can signal that NATO does not intend to dominate other space actors.[69] Additionally, increasing the capacity of certain space systems through partnerships with commercial operators can increase the resilience and redundancy of vital space functions, including SATCOM and certain ISR.

Promote Space Capability Development across the Alliance

Only about half of NATO members operate some aspects of NATO's space infrastructure. Under a memorandum of agreement signed in 2020 through the NCI, NATO relies on four member states for SATCOM capabilities. However, cooperative space programs and commercial partnerships can expand space capabilities across Alliance members to improve overall space competencies while increasing the deterrent effect of diffuse and redundant

[67] Kamala Harris, "Briefing Room: Remarks by Vice President Harris on the Ongoing Work to Establish Norms in Space," White House (website), April 19, 2022), https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/04/18/remarks-by-vice-president-harris-on-the-ongoing-work-to-establish-norms-in-space/.

[68] Brad Townsend, *Security and Stability in the New Space Age: The Orbital Security Dilemma* (New York: Routledge, 2020), 205.

[69] Townsend, *Security and Stability*, 205.

space capabilities.[70] NATO should also encourage members to increase space-specific budgets to expand the overall capabilities and capacity available to the Alliance.

Increase Resilience of Link and User Segment and Prepare to Conduct Operations in a Space-degraded Environment

NATO cannot assume it will continue enjoying unmolested access to essential space functions such as PNT and ISR. Allied forces across the land, maritime, and air domains must anticipate and train for operations in a degraded space environment where adversaries jam or spoof PNT signals to mislead NATO forces. The organization should be wary of commercially available jammers and consider stronger global regulation to control their sale.

Harden Ground Segment against Physical and Cyberattacks

Force protection and physical security remain important measures to mitigate direct attacks and terrorism risks. Although many ground-segment facilities are located on secure military installations, others (such as ESOC) are situated in dense urban areas. NATO members should consider increasing force protection measures at key ground segment facilities and strengthen cybersecurity protocols to defeat any attempts to penetrate networks. Adversaries can access satellites via SATCOM terminals using remote access tools from broader network activities such as file transfer protocols (FTP) and secure copy protocols (SCP).[71] The NATO satellite operators and users should monitor equipment at SATCOM access points and other receiver equipment in the user segment. In terms of physical security, NATO's recently upgraded satellite ground stations in Belgium, Italy, Greece, and Türkiye should be secured from potential eavesdropping, jamming, and physical attacks.

Consider Implementing a Space Personnel Reliability Program

NATO members should consider implementing a space personnel reliability program to ensure the trustworthiness of space professionals across all segments of NATO space systems. Nuclear-armed members of NATO use similar programs for personnel assigned to nuclear-related duties. Personnel reliability programs support the national security of states with sensitive weapons programs by ensuring only those with a demonstrated degree of allegiance, personal responsibility, trustworthiness, and conduct

[70] Gregory L. Schulte, "Protecting NATO's Advantage in Space" *Transatlantic Current* 5 (May 2012): 4.

[71] Ruben Santamarta, *SATCOM Terminals: Hacking by Air, Sea, Land*, Technical White Paper (Seattle: IOActive, 2014), https://www.blackhat.com/docs/us-14/materials/us-14-Santamarta-SATCOM-Terminals-Hacking-By-Air-Sea-And-Land-WP.pdf.

are allowed to perform duties associated with a particular program.[72] A space personnel reliability program could reduce the risks of espionage and other insider threats. NATO should adopt standardized screening and qualification procedures to ensure a trusted space workforce, military and civilian, across the Alliance.

Improve Supply Chain Resilience by Investing in NATO Defense Technical Industrial Base (DTIB)

Space systems require domestic supply chains and a stable aerospace industry to preserve NATO's leading edge in the development of space capability. NATO member defense budgets must ensure that space-related DTIB is sufficiently funded to preserve human capital and expertise and reduce the risk of corporate insolvency during periods of decreased demand.[73] Additionally, NATO members should consider partnering with commercial space operators and startups to foster space technology innovation, research, and development.

Conclusion

NATO depends on critical space systems to fulfill its core missions of defense and deterrence, including early warning, positioning, navigation and timing, communications, and imagery, among others. Space systems comprise national and Alliance critical infrastructure. However, the space systems that enable NATO operations are increasingly vulnerable to state and non-state threats, including terrorist actors. Russia's invasion of Ukraine in February 2022 suggests state actors continue to pose the greatest threat to Alliance security and interests, including in space. Thus, NATO members should focus on increasing segment resilience through redundant capabilities, cybersecurity measures, and physical security while incorporating space threat assessments in all planning, training, and exercises. Additionally, NATO should promote sustainable space capability development across the Alliance while expanding partnerships with institutions and commercial operators to promote norms, safe practices, and standards of orbital behavior.

[72] Department of Defense (DoD), *Nuclear Weapons Personnel Reliability Program*, DoD Manual 5210.42, change 4 (Washington, DC: DoD, January 13, 2015), 9, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/521042m.pdf?ver=2018-11-19-100837-003.

[73] Daniel Fiott, *Defence Industrial Cooperation in the European Union: The State, the Firm and Europe* (New York: Routledge, 2020), 137.

The growing number of low-cost commercial space service providers is an opportunity for NATO to expand access to members and partners. For example, commercial satellite imagery has been useful for identifying Russian positions to support Ukraine's defenses and providing evidence of war crimes perpetrated against innocent Ukrainians.[74] States can obtain access to routine space services more cheaply and easily than ever before, and NATO should strengthen its relationship with commercial providers to expand access and increase the redundancy of its systems for routine operations.

Despite the return of war in Europe, war has not extended into orbit. NATO continues to enjoy access to vital space services, but that access is no longer assured. Space systems remain vulnerable to kinetic and non-kinetic attacks. Although individual launching states bear operational responsibility for the objects they place in orbit, NATO lacks the ability to synchronize space operations among Alliance members. NATO must embrace an operational framework that builds on Article 5 commitments to include the ability to protect and defend Alliance space critical infrastructure. NATO's ability to accomplish its missions and ensure the territorial sovereignty of its members in a future conflict is at stake.

[74] Malachy Browne, David Botti, and Haley Willis, "Satellite Images Show Bodies Lay in Bucha for Weeks, Despite Russian Claims," *New York Times* (website), April 4, 2022, https://www.nytimes.com/2022/04/04/world/europe/bucha-ukraine-bodies.html.

Select Bibliography

Department of Defense (DoD). *Nuclear Weapons Personnel Reliability Program*. DoD Manual 5210.42, change 4. Washington, DC: DoD, January 13, 2015. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/521042m.pdf?ver=2018-11-19-100837-003.

Fiott, Daniel. *Defence Industrial Cooperation in the European Union: The State, the Firm and Europe*. New York, NY: Routledge, 2020.

Gallagher, Jill C., Alyssa K. King, and Clare Y. Cho. "Spectrum Interference Issues: Ligado, the L-Band, and GPS." Congressional Research Service (CRS) Report IF11558. Washington, DC: CRS, May 28, 2020. https://crsreports.congress.gov/product/pdf/IF/IF11558/2.

Johnson-Freese, Joan. *Space Warfare in the 21st Century: Arming the Heavens*. New York: Routledge, 2017.

Schulte, Gregory L. "Protecting NATO's Advantage in Space." *Transatlantic Current* 5 (May 2012).

Westbrook, Tegg. "The Global Positioning System and Military Jamming: Geographies of Electronic Warfare." *Journal of Strategic Security* 12, no. 2 (2019).

— 4 —

Terrorism, Disinformation, and Information Critical Infrastructure

Megan A. Ward

ABSTRACT: Using two distinct case studies of extremist disinformation content, this chapter addresses the intersection of terrorism and disinformation and contextualizes these case studies within the modern information landscape. Disinformation's pervasive reach, ability to incite violence, and potential to compromise critical human infrastructures makes it an effective and attractive weapon that is difficult to identify and combat. This chapter grounds these case studies of terrorist disinformation in contemporary disinformation and communication scholarship to provide flexible and tailorable recommendations for NATO countries and allies as they approach this phenomenon.

Keywords: disinformation, terrorism, "four layers of responsibility," extremist content, social media

Introduction

In the 2018 Brussels Summit Declaration, NATO highlighted the long-standing and developing threat posed by disinformation campaigns that target democratic elections, alliances, and public trust in institutional norms and processes.[1] As the disinformation threat has grown, there is evidence that terrorist groups and other threat actors have added disinformation campaigns to their arsenal. Terrorist groups and terrorist networks have targeted and corrupted information infrastructures with disinformation campaigns and

[1] "NATO's Approach to Countering Disinformation," NATO (website), July 17, 2020, http://www.nato.int/cps/en/natohq/177273.htm.

content. This false content aims to radicalize with divisive ideology, distract target countries with internal division and instability, compromise target countries' ability to combat external threats adequately, and spur domestic or "homegrown" terrorist activity. Those who track and study these violent movements have noted how these groups operate online to recruit members, drum up support, and organize. False information spread online plays a significant role in this process as inciting content attracts members to terrorist cells, creates support for their activities, and encourages individuals and groups to commit acts of public violence. For this reason, this chapter approaches online informational networks—particularly online social spaces—as a critical infrastructure.

The weaponization of disinformation by terrorist groups and networks is alarming. However, right-wing terrorist groups and hostile nation-states have targeted military personnel and veterans of NATO countries and allies, particularly with recruitment messaging and infiltration attempts. Right-wing groups that espouse the anti-immigration "great replacement" conspiracy theory and identify themselves as white nationalists or white identarian are an example of the racially or ethnically motivated violent extremist (REMVE) activity that has been on the rise for decades. These right-wing extremist groups have used coordinated disinformation campaigns to recruit and radicalize potential members and have extended their reach across various Europe and North American countries.[2] Scholars note that these right-wing groups, though active online and responsible for a growing number of terrorist attacks, have not been afforded the same attention as other terrorist groups.[3] Germany is facing an endemic rise of this right-wing, neo-Nazi violence, and scholars of extremism have

[2] Daniel Byman, *Spreading Hate: The Global Rise of White Supremacist Terrorism* (New York: Oxford University Press, 2022); Daniel Koehler, "Right-Wing Extremism and Terrorism in Europe Current Developments and Issues for the Future," *PRISM* 6 no. 2 (July 18, 2016), http://cco.ndu.edu/News/Article/839011/right-wing-extremism-and-terrorism-in-europe-current-developments-and-issues-fo/; Seth G. Jones, "The Rise of Far-Right Extremism in the United States," Center for Strategic and International Studies (CSIS) Briefs (website), November 7, 2018, https://www.csis.org/analysis/rise-far-right-extremism-united-states; and Yassin Musharbash, "The Globalization of Far-Right Extremism: An Investigative Report," *Combating Terrorism Center at West Point (CTC) Sentinel* 14, no. 6 (July/August 2021), https://ctc.westpoint.edu/wp-content/uploads/2021/07/CTC-SENTINEL-062021.pdf.

[3] Michael German, *Hidden in Plain Sight: Racism, White Supremacy, and Far-Right Militancy in Law Enforcement* (New York: New York University School of Law/Brennan Center for Justice, August 27, 2020), https://www.brennancenter.org/our-work/research-reports/hidden-plain-sight-racism-white-supremacy-and-far-right-militancy-law; Anna Meier, "Germany's White Supremacist Problem—and What It Means for the United States," *Lawfare* (blog), January 30, 2022, https://www.lawfareblog.com/germanys-white-supremacist-problem%E2%80%94and-what-it-means-united-states; and Janet Reitman, "U.S. Law Enforcement Failed to See the Threat of White Nationalism. Now They Don't Know How to Stop It," *New York Times*, November 3, 2018, https://www.nytimes.com/2018/11/03/magazine/FBI-charlottesville-white-nationalism-far-right.html.

highlighted how disinformation content is a crucial factor in its spread and the threat it poses to critical military infrastructures—though Germany is not the only country facing this challenge.[4] The US Commission on Security and Cooperation in Europe identified military personnel among the top three targets of Russian disinformation campaigns leveraged against OSCE countries, equal among political leaders and marginalized society members.[5]

Likewise, threat actors have used the COVID-19 pandemic to sow domestic instability and weaken target countries, allowing terrorist groups to extend their influence. Experts warned at the beginning of the pandemic that disinformation would represent a significant threat to effective public health messaging and the already strained public health infrastructure capacity.[6] These warnings proved accurate as the pandemic continued, and disinformation campaigns directly impacted vaccination efforts, adherence to lockdown measures, and incited domestic strife. Terrorist-led disinformation campaigns compromised public health measures to combat the spread of COVID-19 with distrust and anger toward the government and health-care systems.[7] These campaigns were doubly effective in regions that already reported high levels of institutional distrust, illustrating what

[4] Peter Kuras, "Germany Has a Neo-Nazi Terrorism Epidemic," *Foreign Policy* (website), July 2, 2019, https://foreignpolicy.com/2019/07/02/germany-has-a-neo-nazi-terror-epidemic/.

[5] *The Scourge of Russian Disinformation: Hearing before the Commission on Security and Cooperation in Europe*, 115th Cong. (2017), https://www.csce.gov/international-impact/events/scourge-russian-disinformation.

[6] Christina Pazzanese, "Social Media Used to Spread, Create COVID-19 Falsehoods," *Harvard Gazette* (blog), May 8, 2020, https://news.harvard.edu/gazette/story/2020/05/social-media-used-to-spread-create-covid-19-falsehoods/; Samikshya Siwakoti et al., "Localized Misinformation in a Global Pandemic: Report on COVID-19 Narratives around the World," Empirical Studies of Conflict (website), March 25, 2021, https://esoc.princeton.edu/publications/localized-misinformation-global-pandemic-report-covid-19-narratives-around-world; and Taylor Nelson et al., "The Danger of Misinformation in the COVID-19 Crisis," *Missouri Medicine* 117, no. 6 (2020): 510–12.

[7] Kate Cox et al., *COVID-19, Disinformation and Hateful Extremism: Literature Review Report* (London: Commission for Countering Terrorism, July 14, 2021), https://www.rand.org/pubs/external_publications/EP68674.html; Teun van Dongen, "Assessing the Threat of Covid 19-related Extremism in the West," International Centre for Counter-Terrorism (website), August 5, 2021, https://icct.nl/publication/assessing-the-threat-of-covid-19-related-extremism-in-the-west-2/; Michael King and Sam Mullins, "COVID-19 and Terrorism in the West: Has Radicalization Really Gone Viral?," *Just Security* (blog), March 4, 2021, https://www.justsecurity.org/75064/covid-19-and-terrorism-in-the-west-has-radicalization-really-gone-viral/; and Anne Craanen and Charley Gleeson, "The Overlap between Terrorist Content Online, Disinformation, and the Tech Sector Response," *VOX-Pol Network of Excellence* (blog), March 30, 2022, https://www.voxpol.eu/the-overlap-between-terrorist-content-online-disinformation-and-the-tech-sector-response/.

disinformation scholars have long observed about disinformation's ability to weaponize already present instability.[8]

This chapter proposes that the online information landscape is a site where various critical infrastructures are vulnerable to attack, particularly by threat actors who weaponize disinformation. It also provides beginning recommendations for preventing and mitigating the dissemination and effects of disinformation material through situational awareness, transparency, resiliency measures, and coordination and regulation of private-sector technology firms. Although all terrorist groups use disinformation content in some capacity to achieve their goals, this chapter provides two case studies where terrorist networks targeted NATO countries and allies using disinformation campaigns and material to sow instability, recruit, radicalize, and incite violence. Case study selection was based on strategic importance, the prevalence of disinformation that targets military groups and members, and the research available to researchers. Using Janis Sarts' "four layers of responsibility" in combating disinformation, this chapter addresses how national governments can mitigate disinformation threats to their military personnel and increase national and international security.[9]

Definitions

This chapter's definitions become important because the terms *misinformation*, *disinformation*, and *propaganda* overlap and are sometimes used interchangeably or differently within various fields. Similarly, distinctions between terrorist, militia, and vigilante violence associated with disinformation are often blurred in public and academic discourse. Likewise, terms used to categorize those who espouse and act on racially or ethnically motivated violent extremist (REMVE) ideology are common but sometimes misleading. The groups and networks discussed in the first case study self-identify as "white nationalist" or "identarian." They are characterized by their belief that there is a "white race," and it is a distinct and superior racial group. This chapter refers to these groups under their categorical distinction

[8] Rachel Kuo and Alice Marwick, "Critical Disinformation Studies: History, Power, and Politics," *Harvard Kennedy School Misinformation Review* 2, no. 4 (2021): 1–11; and Kate Starbird, "Disinformation Campaigns Are Murky Blends of Truth, Lies and Sincere Beliefs – Lessons from the Pandemic," *Conversation* (blog), July 23, 2020, http://theconversation.com/disinformation-campaigns-are-murky-blends-of-truth-lies-and-sincere-beliefs-lessons-from-the-pandemic-140677.

[9] Janis Sarts, "Disinformation as a Threat to National Security," in *Disinformation and Fake News*, ed. Shashi Jayakumar, Benjamin Ang, and Nur Diyanah Anwar (Singapore: Springer, 2021), 23–33, https://doi.org/10.1007/978-981-15-5876-4_2.

as REMVE groups or networks. The events and entities discussed range from online disinformation campaigns designed to garner support for violent groups and ideology to militia training camps to overt terrorist violence—all activities and events instigated by types and levels of right-wing dissidents or threat actors that use REMVE ideological content to further their aims.

NATO has released various documents defining disinformation "as the deliberate creation and dissemination of false and/or manipulated information with the intent to deceive and/or mislead." NATO stated that "Disinformation seeks to deepen divisions within and between Allied nations, and to undermine people's confidence in elected governments."[10] This chapter understands misinformation as "constituting a claim that contradicts or distorts common understandings of verifiable facts" that is spread purposefully or otherwise.[11] Disinformation is a subset of misinformation that constitutes information known to be false by the disseminator and spread with the intent to influence, deceive, or incite. Propaganda, however, should be understood as true or false information that can be used to "disparage opposing viewpoints," though in some cases, it may fall categorically under disinformation.[12] Scholars and experts have noted that these three categories often overlap even with the same piece of content, and any given content's label depends on the intentions through which it was spread.

As we approach case studies of disinformation and terrorist activity, we acknowledge that any given piece of disinformation content may be spread as propaganda or disinformation first and then spread further as misinformation. This spread does not lessen the threat of this type of false information or its potential to mislead and radicalize its audience. It does explains why this type of threat is particularly difficult to trace and attribute. It is often difficult, if not impossible, to attribute disinformation to a particular source or user and then respond with punitive action.

[10] "NATO's Approach to Countering Disinformation."

[11] Andrew M. Guess and Benjamin A. Lyons, "Misinformation, Disinformation, and Online Propaganda," in *Social Media and Democracy: The State of the Field and Prospects for Reform*, Social Science Research Council Anxieties of Democracy Series, ed. Nathaniel Persily and Joshua A. Tucker (Cambridge, UK: Cambridge University Press, 2020), 10–33, https://www.cambridge.org/core/books/social-media-and-democracy/misinformation-disinformation-and-online-propaganda/D14406A631AA181839ED896916598500.

[12] Joshua A. Tucker et al., *Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature* (Rochester, NY: Social Science Research Network, March 19, 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3144139.

Case Studies

The two cases in this section detail very different instances of terrorist disinformation content, the impact and purpose of the content, and how different actors sought to address and mitigate the effects of the weaponized disinformation. The first case study examines right-wing REMVE Terrorist Networks and loose but effective attempts to infiltrate military and law enforcement sectors by radicalizing members. The second case study addresses the terrorist organization al-Shabaab's COVID-19–related disinformation campaigns in Somalia and Kenya and the current local mobilization that has played a role combating this false content and its effects.

Right-Wing REMVE Terrorist Networks and Germany

Germany has been a frequent target of foreign influence information operations. The German government has been a core target of Russian disinformation due to the country's involvement in Ukraine, former Chancellor Angela Merkel's position on sanctions against Russia, and the country's key position in Europe. Germany's Parliamentary Oversight Panel (PKGr) has stated that individuals with an "extreme far-right and violence-oriented mindset" can be found throughout their federal and state police and intelligence agencies—presenting a considerable threat that has been under-investigated.[13] The extent of the threat is also highlighted by REMVE groups that publicly set strategic sights on Germany, such as Stanislav Anatolyevich Vorobyev, the founder of the Russian Imperial Movement (RIM), who stated that the future of his organization's operations and recruitment will be focused in Germany.

These operations are not limited to online spaces, and the presence and use of online content by REMVE networks cannot be understated. These networks include white power movements, neo-Nazi groups, and various active militia or anti-government movements that uphold white supremacy and work toward REMVE aims.[14] Terms like alt-right, White nationalist, White wellness, White identarian, pro-White, and White rights advocate are outdated or laundered terms for White supremacy and are often used by REMVE groups in disinformating content to disguise the inherent violence of their ideology.

[13] Florian Flade, "The Insider Threat: Far-Right Extremism in the German Military and Police," *CTC Sentinel* 14, no. 5 (May 20, 2021), https://ctc.usma.edu/wp-content/uploads/2021/05/CTC-SENTINEL-052021.pdf.

[14] Kathleen Belew and Ramón A. Gutiérrez, eds., *A Field Guide to White Supremacy* (Oakland: University of California Press, 2021).

In a study of far-right extremism across European Internet communities, the researchers highlighted the role of German far-right actors. They focused on general Twitter usage and the content produced by three active far-right and reactionary groups with varying levels of political credibility: the *Autonome Nationalisten* (Autonomous Nationalists – AN), the *Identitäre Bewegung Deutschland* (Identarian Movement Germany – IBD), and the *Alternative für Deutschland* (Alternative for Germany –AfD).[15]

This study was designed to determine whether key far right parties in Germany have radicalized into extremist ideology, armed violence, or definable terrorism via a general sampling of European Twitter activity and a complementary focused study of the Twitter activity of the groups above, but their focus on Germany provides data on how widespread REMVEs have mainstreamed conspiracy theories. Of the hashtags found in their data set of tweets, #whitegenocide was the most frequently used.[16] This hashtag refers to a false but core REMVE belief that White people are dying out globally due to forced assimilation and immigration and that a Jewish group of elites are orchestrating this plot.[17] The tweets in this sample often paired REMVE conspiracy and disinformation references with more mainstream political hashtags such as #merkel, #afd, #ukip, #brexit, and even #maga—the latter of which displays the lack of borders on REMVE disinformating content.[18]

The tweets regularly outlinked to known disinformating sites like Breitbart, Russia Today (RT), and Sputnik News to prove REMVE claims about immigrants and refugees. The researchers noted the rate at which these users were suspended for hate speech or disinformation violations. They also found English-language suspensions were more common—indicating far more content moderation focused on English-language content that any other language content.[19]

In a 2021 report, the Combating Terrorism Center at West Point compiled incidents of violent threats made by an entity calling themselves NSU 2.0, a reference to the neo-Nazi terrorist group *Nationalsozialistischer Untergrund* (NSU). These threats were levied against leftist politicians,

[15] Reem Ahmed and Daniela Pisoiu, "How Extreme Is the European Far-Right: A Twitter Analysis" *VOX-Pol* (blog), May 20, 2020, https://www.voxpol.eu/how-extreme-is-the-european-far-right-the-quantitative-analysis/.

[16] Ahmed and Pisoiu, "How Extreme Is European Far-Right."

[17] "Glossary Term: White Genocide," Anti-Defamation League (website), May 4, 2017, https://www.adl.org/resources/glossary-terms/white-genocide.

[18] Ahmed and Pisoiu, "How Extreme Is European Far-Right."

[19] Ahmed and Pisoiu, "How Extreme Is European Far-Right."

activists, comedians, and journalists, the majority of whom were female and of minority heritage. These threats were unique because they contained personally identifiable information only available in restricted databases. When investigated, many of the threats were traced back to the various police stations where they had been made and then to online networks and chat groups on Telegram and WhatsApp networks where law enforcement shared anti-Semitic and racist memes and disinformation regarding refugees and migrants.[20] Many of the investigations into the threats and perpetrators are still pending as of 2021.

In 2015, a *Kommando Spezialkräfte* (Special Forces Command, KSK) German soldier named André Schmitt set up a Telegram channel for German military and law enforcement members to socialize and share information—and eventually to plan violent action against pro-refugee politicians and prep for a civil war or collapse scenario called "Day X." Schmitt admits to posting false or inflated information about refugees and immigration's threat to Germany to "motivate" the chat's members.[21] This network also organized paramilitary training events and sold merchandise under a larger prepper and doomsday organization registered under the name "Uniter."[22] Another group would form out of this chat network and the disinformation it spread, *Nordkreuz* or Northern Cross. Marco Gross, a police sniper and former parachutist, acted as an unofficial leader of the spin-off group that included ex and current law enforcement and military members.[23] Using police records, this group compiled a list of pro-refugee politicians, stole and stockpiled police ammunition, and ordered body bags and quicklime to dispose of the anticipated bodies.[24]

These visible instances are small compared to the amount of REMVE content and organization that exists in online spaces across military, defense, and law enforcement message boards, social media groups, and online chat platforms. The extent of this threat has been underexamined in recent history. Many scholars have critiqued Germany's unwillingness to respond

[20] Flade, "Insider Threat."

[21] Katrin Bennhold, "As Neo-Nazis Seed Military Ranks, Germany Confronts 'an Enemy Within,'" *New York Times*, July 3, 2020 (late edition), https://www.proquest.com/docview/2419759243?parentSessionId=7QPUW0ouuHH9Ez8wjOAMcpq2nfhaYKdjkhEng6uNkwA%3D&pq-origsite=primo&accountid=14784.

[22] Flade, "Insider Threat."

[23] Katrin Bennhold, "Body Bags and Enemy Lists: How Far-Right Police Officers and Ex-Soldiers Planned for 'Day X,'" *New York Times* (website), August 1, 2020, https://www.nytimes.com/2020/08/01/world/europe/germany-nazi-infiltration.html.

[24] Philip Oltermann, "German Far-Right Group 'Used Police Data to Compile Death List,'" *Guardian* (website), June 28, 2019, https://www.theguardian.com/world/2019/jun/28/german-far-right-group-used-police-data-to-compile-death-list.

to or acknowledge the growth of REMVE terror in the country for what it is—and part of that critique comes from the lack of monitoring of the online spaces where disinformation spreads and radicalizes state agents into REMVE ideology.[25] REMVE networks steeped in disinformating content developed, organized, and evolved online for many years despite Germany having some of the most stringent anti-disinformation laws in Europe.[26]

Germany's *Netzwerkdurchsetzungsgesetz*, often called the NetzDG law or the Internet transparency law, is a case study of a policy solution to disinformation. This law requires social media companies to remove posts that incite violence or contain hate-speech content within 24 hours—and has levied fines as high as $2.3 million US dollars to the US-based company Facebook for violating the law.[27] Originally proposed in 2017 to reduce hate speech and associated crimes online, the law has been leveraged against disinformation—though not without criticism from international bodies like the United Nations and human rights advocacy groups for its potential to curb free speech and weaponization against peaceful government dissidents.[28]

There is also evidence that far-right and neo-Nazi groups have avoided suspension and social media bans by refraining from overt keywords or recognition by the algorithm—but still operating in encrypted chats and online merchandise stores.[29] Germany has also successfully coordinated preemptive responses to potential disinformation attacks and influence operations. In the lead up to the 2017 German election, the domestic intelligence agency *Bundesamt für Verfassungsschutz* (BfV) shared information with German political parties regarding likely threats. Measures were also

[25] Byman, *Spreading Hate*, 174; Daniel Byman, "Counterterrorism and Modern White Supremacy," *Studies in Conflict & Terrorism* (July 27, 2021): 1–28, https://doi.org/10.1080/1057610X.2021.1956100; Melissa Eddy, "Far-Right Terrorism Is No. 1 Threat, Germany Is Told after Attack," *New York Times* (website), February 21, 2020, https://www.nytimes.com/2020/02/21/world/europe/germany-shooting-terrorism.html; and Laura Tharsen, "Ethnic Nationalism in Germany," *Philosophia Africana* 8, no. 2 (2005): 117–42.

[26] Kate Connolly, "Hundreds of Rightwing Extremist Incidents by German Security Services Revealed," *Guardian* (website), October 6, 2020, https://www.theguardian.com/world/2020/oct/06/report-reveals-hundreds-of-rightwing-extremist-incidents-by-german-security-services.

[27] Raphael S. Cohen et al., *Combating Foreign Disinformation on Social Media: Study Overview and Conclusions* (Santa Monica, CA: RAND Corporation, July 19, 2021), https://www.rand.org/pubs/research_reports/RR4373z1.html, 68.

[28] Erik Brattberg and Tim Maurer, "Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks," Carnegie Endowment for International Peace (website), May 23, 2018, https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435.

[29] Erika Kinetz, "Neo-Nazis Are Still on Facebook. And They're Making Money," *ABC News* (website), September 25, 2021, https://abcnews.go.com/Politics/wireStory/neo-nazis-facebook-theyre-making-money-80225218.

taken to ensure Russia knew any attempts to sway results or incite distrust of election results would have far-reaching diplomatic repercussions. Analysts suggest these preparatory measures successfully deterred interference.[30] The latter case study concerns elections, which are set and scheduled events that can be planned in advance. Disinformating content designed to radicalize individuals and incite violence presents a more nebulous challenge. Nonetheless, the German case study showcases the potential of resilience and deterrence measures against threat actors who use disinformation campaigns.

These localized upswings in REMVE and right-wing domestic terrorism in Germany are part of a larger transnational trend that poses significant risks to NATO countries, their security infrastructure, and their citizenry. Moreover, a failure in many cases to recognize the coordinated campaigns and organized movements as such, in favor of falsely labeling them "lone wolf" attacks, has resulted in these networks' largely unmonitored and unchecked growth and expansion into various countries.[31] Loose networks of REMVEs have coordinated with larger threat actors to conduct influence operations and compromise military members and veterans in many countries.[32] Understanding these networks, their use of disinformation and similar radicalizing content, and the impact of their radicalization efforts is a vital step in mitigating the adverse effects of disinformation and preventing the spread of dangerous ideologies through critical military infrastructures.

REMVE extremists have found external allies in Russia. The mutually beneficial relationship between these entities has allowed both to leverage disinformation and conspiracy content to affect, radicalize, and impact military

[30] Brattberg and Maurer, "Russian Election Interference."

[31] Belew and Gutiérrez, *White Supremacy*.

[32] Tim Lister, "The Nexus between Far-Right Extremists in the United States and Ukraine," CTC (website), April 28, 2020), https://ctc.westpoint.edu/the-nexus-between-far-right-extremists-in-the-united-states-and-ukraine/; "Canadian Report Warns of Extremist Infiltration in Military," *ABC News* (website), accessed May 12, 2022, https://abcnews.go.com/International/wireStory/canadian-report-warns-extremist-infiltration-military-84301400; Elizabeth Grimm Arsenault and Joseph Stabile, "Confronting Russia's Role in Transnational White Supremacist Extremism," Just Security (website), February 6, 2020, https://www.justsecurity.org/68420/confronting-russias-role-in-transnational-white-supremacist-extremism/; and Simon Purdue, "The Other Epidemic: White Supremacists in Law Enforcement," Open Democracy (website), August 6, 2020, https://www.opendemocracy.net/en/countering-radical-right/other-epidemic-white-supremacists-law-enforcement/.

forces in various NATO and NATO-aligned countries.[33] The exact relationship between these groups and national threat actors like Russia is still debated, but they have deliberately borrowed Russian active-measure tactics for their aims. REMVE disinformation, like other types of disinformation, flourishes when trust in traditional institutions is low, when there is an "overload" of information from the many sources available to users, and when the target audience is primed to accept disinformation as truth because of their cultural, social, and political beliefs.[34]

COVID-19 Disinformation and al-Shabaab

In 2020, al-Shabaab, the Somalia-based al-Qaeda affiliate, warned Muslims in East Africa about the infectious COVID-19 virus, stating it has been spread "by the crusader forces who have invaded the country and the disbelieving countries that support them."[35] After a gathering of approximately 100 elders and tribal leaders that discussed the state of terror activities in East Africa, al-Shabaab issued a communique that blamed COVID-19 on Western powers' past and present military interventions. From the beginning of the pandemic, the group targeted Muslims in Somalia and Kenya with disinformation that questioned the government's capacity to keep the public safe and blamed diseases like HIV and the novel coronavirus on Western militaries.[36] Unlike other powerful extremist groups in Africa

[33] Hijacking Our Heroes: *Exploiting Veterans through Disinformation on Social Media: Hearings before the House Committee on Veterans' Affairs*, 116th Cong. (2019) (statement of Vladimir Barash, science director, Graphika), https://veterans.house.gov/events/hearings/full-committee-hearing-hijacking-our-heroes-exploiting-veterans-through-disinformation-on-social-media; and John D. Gallacher et al., "Data Memo No. 2017.9: Junk News on Military Affairs and National Security: Social Media Disinformation Campaigns against US Military Personnel and Veterans," Programme on Democracy & Technology (website), October 9, 2017, https://demtech.oii.ox.ac.uk/research/posts/junk-news-on-military-affairs-and-national-security/.

[34] Alice Marwick and Rebecca Lewis, *Media Manipulation and Disinformation Online* (New York: Data & Society Research Institute, May 15, 2017), https://datasociety.net/wp-content/uploads/2017/05/DataAndSociety_MediaManipulationAndDisinformationOnline-1.pdf; Whitney Phillips and Ryan M. Milner, *You Are Here: A Field Guide for Navigating Polarized Speech, Conspiracy Theories, and Our Polluted Media Landscape* (Cambridge: Massachusetts Institute of Technology Press, 2021); Edson C. Tandoc Jr., *Tools of Disinformation: How Fake News Gets to Deceive* (Singapore: Springer, 2020), 35–46, https://doi.org/10.1007/978-981-15-5876-4_3; Shuo Tang, Lars Willnat, and Hongzhong Zhang, "Fake News, Information Overload, and the Third-Person Effect in China," *Global Media and China* 6, no. 4 (December 1, 2021): 492–507, https://doi.org/10.1177/20594364211047369; and Alena Bermes, "Information Overload and Fake News Sharing: A Transactional Stress Perspective Exploring the Mitigating Role of Consumers' Resilience during COVID-19," *Journal of Retailing and Consumer Services* 61 (July 1, 2021): 102555, https://doi.org/10.1016/j.jretconser.2021.102555.

[35] "Coronavirus: Fighting al-Shabab Propaganda in Somalia," *BBC News*, April 1, 2020, https://www.bbc.com/news/world-africa-52103799.

[36] "Snapshot: How Extremist Groups Are Responding to Covid-19," Tony Blair Institute for Global Change (website), April 9, 2020, https://institute.global/policy/snapshot-how-extremist-groups-are-responding-covid-19-9-april-2020.

(for example, Boko Haram), al-Shabaab acknowledged the severity and threat COVID-19 posed to public health instead of claiming the pandemic was a hoax or the adherence to their extreme version of religion would keep its practitioners safe from the virus.[37] However, al-Shabaab, like other extremist religious organizations, did actively manipulate public discontent over the closure of religious congregations to incite anger against the government and lockdown efforts to curb the spread of COVID-19.[38]

To complicate these matters, mid-pandemic, the group opened public health facilities in competition with government-run sites.[39] They publicized the creation and operation of these sites to prove they were a viable alternative to government services and highlight the weaknesses of official international and domestic COVID-19 responses.[40] Scholars observe that when extremist organizations set up and provide alternative or stopgap social services in competition with government services, the results are often mixed and lack the stability needed to ensure persistent and accessible support—and rarely, if ever, supersede the violent activities of the group.[41] The extent to which al-Shabaab's medical centers were effective responses to the COVID-19 pandemic is debatable. It is clear, however, that they leveraged their coverage of this action as a form of propaganda for their group and as a form of disinformation to decrease institutional trust in government measures.[42]

[37] Yusuf Anka, "Abubakar Shekau Mocks World Leaders And Derides Social Distancing in New Audio Message," HumAngle Media (website), April 15, 2020, https://humanglemedia.com/abubakar-shekau-mocks-world-leaders-and-derides-social-distancing-in-new-audio-message/.

[38] Abdullahi Abdille Shahow, "Al-Shabab's Territory in Somalia Is a COVID-19 Powder Keg," World Politics Review (website), May 1, 2020, https://www.worldpoliticsreview.com/articles/28726/in-al-shabab-s-territory-in-east-africa-pandemic-could-spread-like-wildfire; and "Coronavirus: Fighting al-Shabab."

[39] Abdi Sheikh, "Somalia's Islamist Group al Shabaab Says Sets up COVID-19 Treatment Centre," Reuters (website), June 12, 2020, https://www.reuters.com/article/us-health-coronavirus-somalia-idUSKBN23J32C.

[40] Christopher Hockey and Michael Jones, "The Limits of 'Shabaab-CARE': Militant Governance amid COVID-19," *CTC Sentinel* 13, no. 6 (June 29, 2020), https://ctc.westpoint.edu/the-limits-of-shabaab-care-militant-governance-amid-covid-19/.

[41] Pierre-Emmanuel Ly, "The Charitable Activities of Terrorist Organizations," *Public Choice* 131, no. 1/2 (2007): 177–95; and Emilia Columbo and Marielle Harris, "Commentary: Extremist Groups Stepping Up Operations during the Covid-19 Outbreak in Sub-Saharan Africa," CSIS (website), May 1, 2020), https://www.csis.org/analysis/extremist-groups-stepping-operations-during-covid-19-outbreak-sub-saharan-africa.

[42] Hockey and Jones, "Limits of 'Shabaab-CARE.'"

At the same time, al-Shabaab used the instability of the pandemic to increase violent attacks and operational activity.[43]

As with most disinformating material, al-Shabaab's campaigns leveraged already present vulnerabilities in the target—in this case, a lack of adequate health-care resources, discontent over Western involvement in the region, and diaspora isolation and frustration—with false material that inflamed already present sentiment regarding real concerns and issues.[44] As the pandemic advanced, the group continued to use disinformation campaigns to mock the weaknesses of the region's health-care infrastructure and inflame the public's fear of the virus.[45] When vaccines became available, al-Shabaab took steps to compromise faith in the official measures and vaccination campaigns, spreading rumors that the vaccine was a conspiracy to decrease fertility. Social media posts spread by al-Shabaab via YouTube, chatrooms, and Twitter claimed the vaccine contained pig products, would kill Muslim children, decrease women's fertility, and was designed by Western countries to decrease the Somalian population.[46] This instance is not the first where vaccine and public-health measures have been targeted by al-Shabaab; the group spread similar rumors about the polio vaccine in 2014.[47]

[43] Stephanie Carver and Samantha Kruber, "To Act, or Not? Al-Shabaab's Response to a Covid-19 Crisis in Somalia," Interpreter (website), May 15, 2020, https://www.lowyinstitute.org/the-interpreter/act-or-not-al-shabaab-s-response-covid-19-crisis-somalia; and Eren Ersozoglu, "Al-Shabaab in the Age of COVID-19," Grey Dynamics (website), April 15, 2021, https://www.greydynamics.com/al-shabaab-in-the-age-of-covid-19/.

[44] Anne Speckhard, Othman Mahamud, and Molly Ellenberg, "When Religion and Culture Kill: COVID-19 in the Somali Diaspora Communities in Sweden," Homeland Security Today (website)," April 4, 2020, https://www.hstoday.us/subject-matter-areas/counterterrorism/when-religion-and-culture-kill-covid-19-in-the-somali-diaspora-communities-in-sweden/; and Timothy A. Sikorski, *Airwaves and Microblogs: A Statistical Analysis of Al-Shabaab's Propaganda Effectiveness* (master's thesis, Naval Postgraduate School, 2014).

[45] Abdullahi Abdille Shahow, "Al-Shabab's Territory in Somalia Is a COVID-19 Powder Keg," World Politics Review (website), May 1, 2020, https://www.worldpoliticsreview.com/articles/28726/in-al-shabab-s-territory-in-east-africa-pandemic-could-spread-like-wildfire; "Snapshot: How Extremist GroupsAre Responding"; and Columbo and Harris, "Extremist Groups Stepping up Operations."

[46] Abjata Khalif, "Kenya: The Women Resisting Al-Shabaab's War on Covid-19 Vaccines," Nation (website), July 6, 2021, https://allafrica.com/stories/202107060099.html; Emma Ogao, "Use Honey Instead of COVID Vaccines, Al-Qaeda Backed Militants Say," Vice (website), April 8, 2021, https://www.vice.com/en/article/5dbmpq/al-shabaab-somalia-covid-vaccine-anti-vax; Abjata Khalif, "The Kenyan Women Resisting Al-Shabaab's War on Vaccines," *Evening Standard* (website), July 26, 2021, https://www.standard.co.uk/optimist/vaccine-world/kenyan-women-al-shabaab-war-on-covid19-vaccines-b942939.html; and Ken Menkhaus, "Al-Shabaab and Social Media: A Double-Edged Sword," *Brown Journal of World Affairs, Technology and Terrorism* 20, no. 2 (July 26, 2018), http://bjwa.brown.edu/20-2/al-shabaab-and-social-media-a-double-edged-sword/.

[47] Abdi Guled, "In Somalia, Polio Vaccines Rejected over Rumours Spread by Islamic Extremists," *CTV News* (website), June 1, 2013, https://www.ctvnews.ca/health/health-headlines/in-somalia-polio-vaccines-rejected-over-rumours-spread-by-islamic-extremists-1.1306774.

Al-Shabaab has an established history of using social media and disinformation to reach and target enemy soldiers and international audiences successfully. Beginning on Internet forums, the group moved to Twitter and YouTube to recruit and spread videos of violence as propaganda (such as their high-profile attack on the Westgate shopping mall in Nairobi, Kenya, in 2013). Since the group's rise to prominence in 2007—partly due to the growth of online life and technologies at the time—al-Shabaab has used the Internet effectively to fundraise, recruit, and incite violence.[48] This success means they have decades of experience leveraging social media and online networks to influence operations. These activities have targeted their base in Somalia and Kenya and diaspora populations across other countries.[49]

Responses to al-Shabaab's disinformation have ranged from large social media bans and content moderation to localized efforts to engage community partners. After live-tweeting and taking responsibility on Twitter for an attack and siege on Nairobi's Westgate mall, Twitter banned all al-Shabaab accounts and content. Analysts report these bans to have limited impact as banned users can quickly make new accounts. Content moderation in languages other than English also remains limited.[50] These limitations are not unique to the al-Shabaab case. They are compounded by the low institutional trust and low literacy levels found in the regions al-Shabaab influences and controls.[51]

A potentially more effective means of combating al-Shabaab's disinformation came from localized efforts in rural areas to engage elders and other sources of regional authority. Early in the pandemic,

[48] Menkhaus, "Al-Shabaab and Social Media."

[49] Dominic Pkalya, "Kenyan Stakeholders Call for Implementation of Local Action Plans to Stem Youth Radicalisation and Extremism," *Strong Cities Network* (blog), January 15, 2021, https://strongcitiesnetwork.org/en/kenyan-stakeholders-call-for-implementation-of-local-action-plans-to-stem-youth-radicalisation-and-extremism/.

[50] Mathew Ingram, "The Media Today: The Challenges of Global Content Moderation," *Columbia Journalism Review* (website), June 10, 2021, https://www.cjr.org/the_media_today/the-challenges-of-global-content-moderation.php; Delia Marinescu, "Facebook's Content Moderation Language Barrier," New America (website), September 8, 2021, http://newamerica.org/the-thread/facebooks-content-moderation-language-barrier/; Sara Correia, "Regulating Terrorist Content on Social Media: Automation and the Rule of Law," *International Journal of Law in Context* 15, no. 2 (2019): 183; "Moderating Extremism: The State of Online Terrorist Content Removal Policy in the United States," Homeland Security Today (website), December 20, 2021, https://www.hstoday.us/subject-matter-areas/counterterrorism/moderating-extremism-the-state-of-online-terrorist-content-removal-policy-in-the-united-states/; and Neal Ungerleider, "Despite Ban, YouTube Is Still a Hotbed of Terrorist Group Video Propaganda," Fast Company (website), November 12, 2010, https://www.fastcompany.com/1701383/despite-ban-youtube-still-hotbed-terrorist-group-video-propaganda.

[51] "Women on the Frontline: Delivering COVID-19 Vaccines on the Kenya-Somalia Border," Gavi (website), April 16, 2021, https://www.gavi.org/vaccineswork/women-frontline-delivering-covid-19-vaccines-kenya-somalia-border.

analysts suggested a widespread alliance between public-health workers and Muslim religious leaders to help combat disinformation and resistance to lockdown, social distancing, and other public-health measures.[52] To a certain extent, the alliance was attempted. However, the most salient examples of success in the face of terrorist disinformation have come from localized efforts to engage traditional sources of local authority and social capital.

When hospitals and dispensaries on the Kenyan-Somalia border closed, local women mobilized to deliver medical care and provide updated health information and vaccines to their communities and others through local and personal contacts. Women and their local networks throughout Somalia and Kenya have been at the forefront of combating terrorist disinformation through house-to-house information campaigns, radio interview broadcasts, village visits, and public forums like markets and village events.[53] By speaking to key traditional leaders like elders and religious authorities and building rapport through everyday interactions across communities, these women have successfully countered terrorist narratives by working within the networks where disinformation is likely to spread. These successes are limited by the resources these women can access and the danger and retaliation they face working against al-Shabaab's narratives. They continue to request security protection and now solar-power systems and coolers crucial for storing and transporting the vaccine."[54]

Analysis

Stopping disinformation is a difficult, if not impossible, task. The nature of modern information systems ensures there will always be false information circulating online. Disinformation has proven to be an efficient weapon against individuals, nations, and democratic processes, and it is unlikely that threat actors will abandon the tactic. This is not to say that countries, social media platforms, and international bodies should not cease efforts to deplatform disinformation creators, create policies and requirements for content hosts and platforms, or moderate harmful online posts, but that these efforts are ultimately reactive. These solutions also require substantial coordination with and regulation of private social media platforms, which brings in issues

[52] "Coronavirus: Fighting al-Shabab Propaganda."

[53] Abjata Khalif, "The Kenyan Women Resisting Al-Shabaab's War on Vaccines," *Evening Standard* (website), July 26, 2021, https://www.standard.co.uk/optimist/vaccine-world/kenyan-women-al-shabaab-war-on-covid19-vaccines-b942939.html.

[54] Khalif, "Kenyan Women."

of government overreach, free speech, and the extensive manpower commitment that comprehensive content moderation requires.

Currently, the international community and the countries discussed above cannot address the disinformation threat as it exists with merely reactive means. Solutions like social media content bans, fact-checking, and taking down platforms have been implemented in a patchwork manner and require continuous investment in resources to determine what is and is not false information. Moderators scramble to keep up with the flexible and changing nature of the online information ecosystem, and automated content moderation notoriously has difficulty protecting freedom of expression and vulnerable users.[55] Multiple studies have indicated that content moderation is limited by its focus on English language posts—leaving large amounts of content unmonitored—and that moderation standards are applied unevenly across different terrorist groups.[56]

Disinformating actors are adept at avoiding bans with "dog whistles," which is speech that seems innocuous and forgettable to the general public but simultaneously communicates "hidden meaning to fellow far-right sympathizers." Take, for example, the creative presentation of banned words, such as representing the word "Vaccine" with "V—cc—n3" to avoid automatic

[55] Heidi Tworek, "History Explains Why Global Content Moderation Cannot Work," Brookings Tech Stream (website), December 10, 2021, https://www.brookings.edu/techstream/history-explains-why-global-content-moderation-cannot-work/; Jillian C. York and Corynne McSherry, "Content Moderation Is Broken. Let Us Count the Ways," Electronic Frontier Foundation (website), April 29, 2019, https://www.eff.org/deeplinks/2019/04/content-moderation-broken-let-us-count-ways; Thiago Dias Oliva, Dennys Marcelo Antonialli, and Alessandra Gomes, "Fighting Hate Speech, Silencing Drag Queens? Artificial Intelligence in Content Moderation and Risks to LGBTQ Voices Online," *Sexuality & Culture* 25, no. 2 (April 1, 2021): 700–732, https://doi.org/10.1007/s12119-020-09790-w; Robert Gorwa, Reuben Binns, and Christian Katzenbach, "Algorithmic Content Moderation: Technical and Political Challenges in the Automation of Platform Governance," *Big Data & Society* 7, no. 1 (January 1, 2020): 2053951719897945, https://doi.org/10.1177/2053951719897945; Elizabeth Stewart, "Detecting Fake News: Two Problems for Content Moderation," *Philosophy & Technology* 34, no. 4 (December 1, 2021): 923–40, https://doi.org/10.1007/s13347-021-00442-x; and Emma J. Llansó, "No Amount of 'AI' in Content Moderation Will Solve Filtering's Prior-Restraint Problem," *Big Data & Society* 7, no. 1 (January 1, 2020): 2053951720920686, https://doi.org/10.1177/2053951720920686.

[56] Ángel Díaz and Laura Hecht-Felella, "Research & Reports: Double Standards in Social Media Content Moderation," Brennan Center for Justice (website), August 4, 2021), https://www.brennancenter.org/our-work/research-reports/double-standards-social-media-content-moderation.

flagging and numerous backup accounts.[57] In addition, researchers of online extremism have noted the phenomenon that occurs as everyday users are deplatformed for nonviolent content. They often travel to more "fringe" sites where they are exposed progressively to more extreme content.[58] The current state of anti-disinformation measures has failed to curb the spread or effects of disinformation with any consistency.

Reactive measures may also potentially threat users' freedom of expression and the ability to engage with political discourse. Governments and political leaders have claimed "fake news" when faced with criticism from journalists or citizens. State-sponsored disinformation is turned against citizens as it is weaponized against other countries.[59] Governments have used reactive measures like deplatforming, bans, and criminalization against political opponents as a way to keep them from organizing or voicing dissent.[60] Since 2018, journalists and human-rights scholars have noted the trend wherein various governments

[57] Prashanth Bhat and Ofra Klein, "Covert Hate Speech: White Nationalists and Dog Whistle Communication on Twitter," in *Twitter, the Public Sphere, and the Chaos of Online Deliberation*, ed. Gwen Bouvier and Judith E. Rosenbaum (Cham, CH: Springer International Publishing, 2020), 151–72, https://doi.org/10.1007/978-3-030-41421-4_7; Sarah Myers West, "Censored, Suspended, Shadowbanned: User Interpretations of Content Moderation on Social Media Platforms," *New Media & Society* 20, no. 11 (November 1, 2018): 4366–83, https://doi.org/10.1177/1461444818773059; Mathilda Åkerlund, "Dog Whistling Far-Right Code Words: The Case of 'Culture Enricher' on the Swedish Web," *Information, Communication & Society* 25, no. 12 (February 23, 2021): 1808–25, https://www.tandfonline.com/doi/pdf/10.1080/1369118X.2021.1889639; and Ysabel Gerrard, "Beyond the Hashtag: Circumventing Content Moderation on Social Media," *New Media & Society* 20, no. 12 (December 1, 2018): 4492–4511, https://doi.org/10.1177/1461444818776611.

[58] Ryan Greer, "Insights: Weighing the Value and Risks of Deplatforming," Global Network on Extremisn & Technology (website), May 11, 2020, https://gnet-research.org/2020/05/11/weighing-the-value-and-risks-of-deplatforming/; and Network Contagion Research Institute and Anti-Defamation League's Center on Extremism, "When Twitter Bans Extremists, GAB Puts Out the Welcome Mat," *ADL Blog Online: Hate & Harassment* (website), March 11, 2019, https://www.adl.org/blog/when-twitter-bans-extremists-gab-puts-out-the-welcome-mat.

[59] David M. Beskow and Kathleen M. Carley, "Characterization and Comparison of Russian and Chinese Disinformation Campaigns," in *Disinformation, Misinformation, and Fake News in Social Media: Emerging Research Challenges and Opportunities,* Lecture Notes in Social Networks Series, ed. Kai Shu et al. (Cham, CH: Springer, 2020), 63–81; Savvas Zannettou et al., "Disinformation Warfare: Understanding State-Sponsored Trolls on Twitter and Their Influence on the Web," in *Companion Proceedings of the 2019 World Wide Web Conference* (San Francisco: Association for Computing Machinery, May 2019), 218–26, https://dl.acm.org/doi/10.1145/3308560.3316495; and Samantha Bradshaw and Philip N. Howard, "The Global Organization of Social Media Disinformation Campaigns," *Journal of International Affairs* 71, no. 1.5 (2018): 23–32.

[60] Chengli Wang and Haifeng Huang, "When 'Fake News' Becomes Real: The Consequences of False Government Denials in an Authoritarian Country," *Comparative Political Studies* 54, no. 5 (April 1, 2021): 753–78, https://doi.org/10.1177/0010414020957672; and Jacob Mchangama, "Censorious Governments Are Abusing 'Fake News' Laws: The Pandemic Is Giving Them an Excuse to Gag Reporters," *Economist* (website), February 13, 2021, https://www.economist.com/international/2021/02/11/censorious-governments-are-abusing-fake-news-laws.

have rushed "fake news" laws and subsequently used them to imprison and silence critique, political expression, and reporting.[61]

Therefore, the following analysis and recommendations focus on proactive measures that may better address the threat of disinformation. It analyzes the threat posed by content created and spread by terrorist networks. Reactive measures should not be discarded entirely, and the below recommendations reflect reactive measures to be used in tandem with proactive approaches. As we acknowledge disinformation's inescapable presence in the current information ecosystem, the focus should instead turn to addressing and mitigating disinformation's ability to be weaponized strategically. If disinformation is here to stay, how might it be defanged?

Before addressing how disinformation may be rendered less effective, it is necessary to understand why disinformation is effective. It is here that the featured case studies become illustrative. Disinformation plays into the audience's preexisting desires, anxieties, and values in order to seem credible where it would otherwise not be.[62] Disinformation is most effective when it says something people feel is true—it leverages confirmation bias, that is, their tendency to interpret new data as confirmation of already existing beliefs.[63] The methods through which this is spread also play a role and are one of the reasons why threat actors target online communities and spaces of online engagement. Credibility is determined not by any given source for the information but by the virality of the content—meaning the likes, reposts, and shares any given piece of content has collected.[64] Disinformation also becomes potent on social media, where users are exposed to false content by people they trust and know personally.

This method of disinformation is one of the reasons REMVE ideologies are such a threat to military, security, and law enforcement communities. In the Germany case study, the security communities have historically been, and often still are, dominated by white men. The military and law enforcement professions are commonly perceived to be important and crucial to society. REMVE disinformation and conspiracy content warns of the

[61] Mchangama, "Censorious Governments"; and Caroline Lees, "Fake News: The Global Silencer: The Term Has Become a Useful Weapon in the Dictator's Toolkit against the Media. Just Look at the Philippines," *Index on Censorship* 47, no. 1 (April 1, 2018): 88–91, https://doi.org/10.1177/0306422018769578.

[62] Tom Buchanan, "Why Do People Spread False Information Online? The Effects of Message and Viewer Characteristics on Self-Reported Likelihood of Sharing Social Media Disinformation," *PLOS ONE* 15, no. 10 (October 7, 2020): e0239666, https://doi.org/10.1371/journal.pone.0239666.

[63] Tandoc, *Tools of Disinformation*, 35–46.

[64] Tandoc, *Tools of Disinformation*, 35–46.

end of this dominance and the subsequent weakening of a community's strength through "feminization" or the loss of homogeneity.[65] This content leverages an audience's existing anxieties about shifts in gender roles and racial demographics and distorts these normal changing conditions into existential threats. This distortion is where terms like "white genocide" may be explicit or couched within dog whistles about "declining birth rates among white women."

Similarly, memes present images of "feminized" men to be laughed at and compared with historically, and white, soldiers from past wars who supposedly exemplified traditional masculine traits and were emblematic of those successful conflicts.[66] Because REMVE disinformation extols examples of traditional masculinity and physical prowess—while positioning immigration and increasing civil rights for women, LGBTQIA members, and racial minorities as threats to those examples—disinformation coming from these spaces may find fertile ground in fields that have historically been dominated by white men and given high status within society.

Likewise, COVID-19 disinformation in the al-Shabaab case study was specifically designed to resonate with the preexisting resentment against Western military interventions, low trust in the Somalian government and its health-care system, and the isolation and instability experienced by the Somalian diaspora. Disinformating content that argued the government would do little to help their population survive the pandemic and that people should look to al-Shabaab instead, and then content that claimed international vaccination efforts were designed to depopulate Somalia and destroy Muslims, was directed at an already primed audience. Unique to the al-Shabaab case is how informal public-health advocates could reach this already primed audience and mitigate disinformation's effect on the ground. The women in Somalia and Kenya who mobilized to offset the reach of al-Shabaab's disinformation campaigns are a model for other countries and a potential ally for stakeholders interested in the East African case.

The following recommendations are formed from these observations and take the task of preventative measures against weaponized disinformation seriously. Because the online information landscape can impact and affect how various critical infrastructures operate, weaponized disinformation that compromises this information landscape is a significant threat. Moreover,

[65] Jessica Johnson, "The Self-radicalization of White Men: 'Fake News' and the Affective Networking of Paranoia," *Communication Culture & Critique* 11, no. 1 (2018): 100–15.

[66] Nellie Bowles, "'Replacement Theory,' A Racist, Sexist Doctrine, Spreads in Far-Right Circles," *New York Times* (website), https://www.nytimes.com/2019/03/18/technology/replacement-theory.html.

the networked and nebulous nature of this information landscape makes it difficult to isolate with confidence the source of disinformation and its harmful effects on any given infrastructure. For this reason, this chapter structures recommendations on Janis Sarts' four layers of responsibility that prioritizes preemptive and flexible measures that can help curb terrorist-sponsored disinformation's ability to deceive and incite violence.

Four Layers of Responsibility

Sarts reiterates the above by explaining that the "contemporary information environment has created a favorable space for the spread of hostile disinformation campaigns."[67] Their four layers of responsibility are prescriptive steps for creating a space where disinformation campaigns are not as effective. Sarts' prescriptive layers are not entirely self-contained, and investment in one will aid the development of others. This method allows countries to invest as they are capable and develop these layers, building on one another.

The first layer is "awareness," which includes governments and national bodies maintaining a clear and accurate picture of the information space their citizens and state agents exist and engage with—and this can be done without surveillance overreach by consistent coordination and investment in academic scholarship and nonprofit research. States should always stay abreast of the echo chambers existing across information ecosystems, what actors are participating in and for what purpose, and what organic and nonorganic influences are at play in any given online social space. This surveillance also includes monitoring what organized troll networks exist in a country's information space. This awareness may seem obvious, but REMVE networks in the above case study have expanded online unmonitored in the last two decades, increasing their capacity and resources to do harm because governments ignored warnings.[68]

Governing bodies should examine their cultural positionality to ensure key threats are not underestimated and resource allocation is based on realistic risk metrics. By developing accurate awareness of a country's information space, these decisions can be made with confidence. States and international agencies should invest in effective awareness tools and partnerships with researchers that allow them to understand how national and

[67] Sarts, "Disinformation as a Threat to National Security."

[68] Phillips and Milner, *You Are Here*; Daniel Byman, *Spreading Hate*; Meier, "Germany's White Supremacist Problem; Reitman, "U.S. Law Enforcement Failed"; and German, *Hidden in Plain Sight*.

international extremist groups are networked and operate to radicalize new online spaces. Tools should include consistent training and education for members of security communities and other critical infrastructures who are likely to be targeted. This curriculum should cover the threat emerging terrorist groups pose, and how these networks use false content to leverage common biases and grievances found in those spaces.

The second layer, labeled "government coordination and capability development" by Sart, is designed to set protocols and reactive measures preemptively to combat hostile and damaging disinformation campaigns when detected and target critical infrastructures. These protocols can ensure that when disinformation is detected, there is a standard process to address its effects instead of patchwork or inconsistent responses that may only confuse the information space.[69] In 2018, Sweden reported the success of their "psychological defense" authority that would focus on election-related disinformation, amplify independently verified information, and confront influence operations "as a form of consumer protection."[70] Their focus on coordination between various levels of government, civil society institutions, and independent expert communities was released to the public and allowed consistent messaging while mitigating the potential for any government monopoly on political narratives. As disinformation leverages chaos, fear, and confusion, effective protocols will include clear messaging and transparency.

Moreover, the second aspect of this layer speaks to the potential for governments to expand their ability to reach those directly affected by disinformation on the ground, as seen in the second case study. The Somalia case study provides an excellent example of the potential for expanded coordination and capability. The Somalian women running local efforts to combat terrorist-sponsored disinformation have openly communicated the support and protection they require to continue their anti-disinformation measures and public-health work—support that could come in the form of international military support and resources

[69] Cohen et al., *Combating Foreign Disinformation*; and Shuo Tang, Lars Willnat, and Hongzhong Zhang, "Fake News, Information Overload, and the Third-Person Effect in China," *Global Media and China* 6, no. 4 (2021): 492–507.

[70] Adela Suliman, "Sweden Sets Up Psychological Defense Agency to Fight Fake News, Foreign Interference," *Washington Post* (website), January 6, 2022, https://www.washingtonpost.com/world/2022/01/06/sweden-fake-news-psychological-defence-agency/; and Jean-Baptiste Jeangène Vilmer, *Effective State Practices against Disinformation: Four Country Case Studies*, Hybrid CoE Research Report 2 (Helsinki: European Centre of Excellence for Countering Hybrid Threats, July 2021), https://www.hybridcoe.fi/wp-content/uploads/2021/07/20210709_Hybrid_CoE_Research_Report_2_Effective_state_practices_against_disinformation_WEB.pdf.

for infrastructure development of their efforts.[71] By coordinating with and learning from those who have successfully combated terrorist disinformation on the ground, international military and governing agencies can protect vital infrastructures without alienating the population.[72] Personnel tackling disinformation should look at regional solutions that support those already doing the work.

The third layer, "society and resilience," focuses on efforts to inoculate a population against disinformation effects. Due to disinformation's penchant for leveraging individuals' confirmation bias, this layer can be considered one of the most important. However, creating resilience against false content is difficult, and there is no scholarly consensus on this inoculation process. Many research institutions have posited that media literacy campaigns, training, and schooling are the solution—and this curriculum works to encourage critical thinking regarding personal and media bias, identification of credible sources, and personal accountability in online interactions and behavior. These relatively new media literacy efforts have yet to yield observable returns as these efforts have not been implemented widely. Early results indicate that media literacy and critical thinking alone cannot combat disinformation. In one study of disinformation-spreading behavior, individuals with low and high media literacy were just as likely to spread disinformation.[73] Nevertheless, other studies produced more encouraging conclusions documenting that media literacy education, when tailored to be culturally sensitive and appropriate, has some effect reducing disinformation's credibility.[74]

[71] "Fostering Misinformation Literacy: Runtu Waa Nabad in Somalia," *Sentinel Project* (blog), April 16, 2021, https://thesentinelproject.org/2021/04/16/fostering-misinformation-literacy-runtu-waa-nabad-in-somalia/; and Khalif, "Kenyan Women."

[72] Bharat Mehra, "Information ACTism in 'Trumping' the Contemporary Fake News Phenomenon in Rural Libraries," *Open Information Science* 3, no. 1 (January 1, 2019): 181–96, https://doi.org/10.1515/opis-2019-0013; and Aaron Bailey-Athias and Abbie Richards, "How to Tackle Mis/Disinformation with a Human Centred Approach," ODI (website), 2021, https://odi.org/en/insights/how-to-tackle-misdisinformation-with-a-human-centred-approach/.

[73] Buchanan, "Why Do People Spread False Information Online?"

[74] Andrew M. Guess et al., "A Digital Media Literacy Intervention Increases Discernment between Mainstream and False News in the United States and India," *Proceedings of the National Academy of Sciences* 117, no. 27 (July 7, 2020): 15536–45, https://doi.org/10.1073/pnas.1920498117; Michael Hameleers, "Separating Truth from Lies: Comparing the Effects of News Media Literacy Interventions and Fact-Checkers in Response to Political Misinformation in the US and Netherlands," *Information, Communication & Society* 25, no. 1 (January 2, 2022): 110–26, https://doi.org/10.1080/1369118X.2020.1764603; Melissa Tully, Emily K. Vraga, and Leticia Bode, "Designing and Testing News Literacy Messages for Social Media," *Mass Communication and Society* 23, no. 1 (January 2, 2020): 22–46, https://doi.org/10.1080/15205436.2019.1604970; and Yoori Hwang, Ji Youn Ryu, and Se-Hoon Jeong, "Effects of Disinformation Using Deepfake: The Protective Effect of Media Literacy Education," *Cyberpsychology, Behavior, and Social Networking* 24, no. 3 (March 1, 2021): 188–93, https://doi.org/10.1089/cyber.2020.0174.

Anyone combating terrorist-sponsored disinformation should consider multipronged approaches that increase media literacy and trust in government and nongovernment institutions. As discussed previously, disinformation is adept at leveraging a population's fear, isolation, distrust, and grievance into acts of violence against individuals, groups, and both government and nongovernment institutions. In a European Centre of Excellence for Countering Hybrid Threats comparison of successful information-resilience measures, countries with the highest index ratings for institutional trust and accessible civil life were the least affected by coordinated disinformation campaigns.[75] Studies suggest that providing transparency into government operation, protecting and supporting a free press, and facilitating accessible civic participation will have a curative effect on one of the main drivers of disinformation's success—the lack of institutional trust.[76] Finally, governments should look to areas with alternative forms of authority (such as regional, cultural, or religious institutions) and seek partnerships with those who work daily with the populations they wish to address.

The fourth layer, the development of regulatory frameworks with tech platforms, stabilizes the information landscape and creates agreed-upon norms for online socialization and content moderation. Large social media companies like Facebook, Twitter, and TikTok have explicit bans on terrorist content on their platforms. However, the extent to which this content still circulates speaks to the limits of social media bans and content moderation. It also presents an accountability problem, as these corporations have little fiscal incentive to moderate often-profitable disinformation, and efforts to fine these companies for violating national content-hosting laws pale in comparison to profit potential of disinformating material.[77] As disinformation is hosted and spread through these companies' platforms, coordination is required in some facet. These partnerships should be designed with regulatory oversight and shared responsibility to protect users' rights to safety and privacy.

[75] Vilmer, *Effective State Practices against Disinformation*.

[76] Tarun Khanna, *Trust: Creating the Foundation for Entrepreneurship in Developing Countries* (Oakland, CA: Berrett-Koehler Publishers, 2018); and William D. Eggers et al., "Rebuilding Trust in Government: Four Signals That Can Help Improve Citizen Trust and Engagement," Deloitte (website), March 9, 2021, https://www2.deloitte.com/us/en/insights/industry/public-sector/building-trust-in-government.html.

[77] Denise Clifton, "Here's Why Facebook and Twitter Aren't Stopping the Flood of False and Toxic Content: Tech Insiders and Expert Expose the Dark Side of the Wildly Lucrative Social Media Business," *Mother Jones* (blog), December 4, 2018, https://www.motherjones.com/media/2018/12/facebook-twitter-fake-news-toxic-content-social-media-companies/.

Recommendations

The recommendations below are distilled from the above. Intergovernmental alliances (such as NATO and other organizations) can encourage their members to adopt the following recommendations under the premise that an effective response might involve:

- Investment in intelligence and accurate mapping of the online information ecosystem that actively monitors known and emerging threat actors
- Awareness about disinformation threats on various levels, not just nationally, but also provincially, regionally, and locally
- State readiness and messaging protocols if disinformation targets key critical infrastructures
- Engagement with civil society organizations and experts from industry, civil society, and academia when creating and implementing legal, educational, regulatory, or structural solutions to disinformation
- Consistent coordination with trusted forms of authority on the ground (such as religious and cultural leaders) to better understand the regional impact of disinformation and how it might be addressed
- Efforts to increase resilience against disinformation through critical-thinking education like media literacy and digital education curriculum at all ages.
- Support for accessible and quality independent journalism in terms of funding, transparency protocols, and open flow of information
- Interorganization codes of conduct that pose consequences for those that knowingly create or spread disinformation
- Cooperative and regulatory relationships with social media companies to address how false content will be handled while ensuring the protection of users' safety and rights to privacy

Conclusion

Disinformation will likely continue to be a part of the modern information ecosystem for as long as people interact online, and it will also likely be weaponized by threat actors to compromise the military response capability and incite instability. Intergovernmental organizations, like NATO, can provide guidance and resources to countries seeking to secure their online information infrastructure. The layers of responsibility outlined in this chapter provide a general approach that an individual country can tailor to its needs when approaching weaponized disinformation.

Select Bibliography

Beskow, David M., and Kathleen M. Carley. "Characterization and Comparison of Russian and Chinese Disinformation Campaigns." In *Disinformation, Misinformation, and Fake News in Social Media*. ed. Kai Shu et al. Cham: CH: Springer, 2020.

Bradshaw, Samantha, and Philip N. Howard. "The Global Organization of Social Media Disinformation Campaigns." *Journal of International Affairs* 71, no. 1.5 (2018).

Hwang, Yoori, Ji Youn Ryu, and Se-Hoon Jeong. "Effects of Disinformation Using Deepfake: The Protective Effect of Media Literacy Education." *Cyberpsychology, Behavior, and Social Networking* 24, no. 3 (March 1, 2021). https://doi.org/10.1089/cyber.2020.0174.

Kuo, Rachel, and Alice Marwick. "Critical Disinformation Studies: History, Power, and Politics." *Harvard Kennedy School Misinformation Review* 2, no. 4 (2021).

Nelson, Taylor et al. "The Danger of Misinformation in the COVID-19 Crisis." *Missouri Medicine* 117, no. 6 (2020).

Sarts, Janis. "Disinformation as a Threat to National Security." In *Disinformation and Fake News*. ed. Shashi Jayakumar, Benjamin Ang, and Nur Diyanah Anwar. Singapore: Springer, 2021. https://doi.org/10.1007/978-981-15-5876-4_2.

Stewart, Elizabeth. "Detecting Fake News: Two Problems for Content Moderation." *Philosophy & Technology* 34, no. 4 (December 1, 2021). https://doi.org/10.1007/s13347-021-00442-x.

Tucker, Joshua A. et al. *Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature*. Rochester, NY: Social Science Research Network, March 19, 2018. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3144139.

— 5 —

Critical Election Infrastructure: Backbone of Democracy with Relevance for NATO?

Denise Feldner

ABSTRACT: Democratic resilience and election integrity are foundational to NATO's future success as a military alliance. The Alliance underlined in the 2022 Strategic Concept an intent to reinforce political unity and deepen consultations to address all matters that affect security—including democratic resilience. With election infrastructures being the backbone of liberal democracies, they are NATO mission critical infrastructures—with all due respect to national sovereignty. They stand at the epicenter of NATO adversaries' activities against the Alliance's stability. One weak democracy in NATO can harm the Alliance. NATO's active role as a political alliance in creating defense and democratic resilience against disruptions to critical societal functions (such as elections and cohesion) is therefore central to a prosperous future of liberal democracies and the unity of member states.

Keywords: election security, critical election infrastructures, societal and democratic resilience

Introduction and Definition

In the last seven years, much strategic discussion has focused on election integrity in the United States, Europe, and the United Kingdom.[1] It was mainly a reaction to Russian election interference in the United States,

[1] "Die Wahlinfrastruktur aller EU-Mitgliedstaaten muss als kritische Infrastruktur erheblich besser geschützt werden [The Electoral Infrastructure of All EU Member States as Critical Infrastructure Must Be Significantly Better Protected]," FDP (German Liberal Party) Election Programme 2021, Summer 2021, FDP_Programm_Bundestagswahl2021_1.pdf, 52.

starting in 2014. It was also a response to other civil adversaries' hackings and election manipulations (such as the Cambridge Analytica Scandal and activities conducted by political movements that pay little heed to democratic values or the rule of law in many member countries of the Alliance). Discussions centered around the following topics: competition among states of "great power" as a reason for election interferences, election integrity and critical election infrastructures being weaponized to fight liberal democracies, and specific and new types of adversaries: politically motivated terrorism.

Competition of Political Philosophies

The international competition among states has been increasingly focused on the long-term success of different political systems and political philosophies (such as China and Russia) but also on newly invented types of governance in democracies and in NATO member states. In this political ecosystem, election infrastructures have been leveraged and weaponized as a strategic instrument of hybrid warfare against other states, against democracies but also within democracies. This is true for weaker states like Ukraine and Northern Macedonia but also for superpowers like the United States.[2]

Democracy Depends on Trust of the People in Election Infrastructures

The discussion on election integrity, especially in the United States, has mostly centered around the idea of a democracy depending on the stability of the will of most of the people. They trust in their votes to be counted correctly and not manipulated. This is seen as a critical pillar of democratic stability. When a breach of trust occurs in the complex physical and societal election system, a critical disruption might follow that affects defense capabilities. In fact, democracies are not governed by one party or person. They depend on the functionality of a myriad of institutions. The will of millions of people and the stability of critical infrastructures are key to their unity. The trust of their constituencies in election infrastructures, whether critical infrastructures, administrative processes, or political organizations, is important to the core stability of a Western democracy.

Russian interferences in the 2016 US election caused operational measures to secure democratic values and infrastructures in the United States.

[2] "Ukrainian Election Task Force, Foreign Interference in Ukrainian Democracy," Atlantic Council (website), May 2019, https://www.atlanticcouncil.org/wp-content/uploads/2019/05/Foreign_Interference_in_Ukraines_Election.pdf; and Carol V. Evans, "Future Warfare: Weaponizing Critical Infrastructure," *Parameters* 50, no. 2 (Spring 2020), https://press.armywarcollege.edu/parameters/vol50/iss2/6/.

The possible involvements of Donald Trump in the US Capitol riot on January 6, 2021, have led to legal investigations against the 45th president of the United States. Both events have created distrust among US citizens about the elections, although the US Elections Infrastructure Government Coordination Council (GCC) announced there was no evidence of any impact on and interference with the election infrastructure in the 2020 elections.[3]

An official reaction to the 2016 events conducted by the authorities was the classification of election infrastructure, voting systems, the associated infrastructure, and storage for ballots and equipment as critical infrastructure in the government facilities sector by the US Department of Homeland Security (DHS) in 2017.

Then DHS Secretary Jeh Johnson observed: "Given the vital role elections play in this country, it is clear that certain systems and assets of election infrastructure meet the definition of critical infrastructure, in fact and in law."[4] Further, he stated:

> election infrastructure should be designated as a subsector of the existing Government Facilities critical infrastructure sector. As such, election infrastructure belongs now to the group of critical national infrastructure in the definition catalogue of NATO. . . . . Particularly in these times, this designation is simply the right and obvious thing to do.[5]

Johnson's decision put election equipment in a highly protected strategic category alongside the other 16 critical and vital infrastructures in the country's basic operations like power grids and the financial sector.[6] Election infrastructures now have higher awareness and support and better financing sources available.

This decision to classify election infrastructure came the same day three of the top intelligence agencies in the United States released unclassified reports concluding Russian President Vladimir Putin ordered a hacking

[3] US Government Coordination Council, "Joint Statement from Elections Infrastructure Government Coordinating Council and the Election Infrastructure Sector Coordinating Executive Committees," CISA, November 12, 2020.

[4] US Department of Homeland Security (DHS), "News Archive: Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector," DHS (website), January 6, 2017, https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.

[5] DHS, "Statement by Secretary Jeh Johnson."

[6] "Critical Infrastructure Sectors," CISA (website), n.d., https://www.cisa.gov/critical-infrastructure-sectors.

campaign against Democratic organizations and officials that eventually aimed to help elect Donald Trump, who then was considered by Russian officials as a friend of Russia.[7]

Following the Department of Homeland Security classified election infrastructure, the US GCC defined critical election infrastructure (CEI) as follows:

> Critical Election Infrastructures includes voter registration databases and associated IT-systems as well as IT-infrastructure and systems used to manage elections (such as the counting, auditing, and displaying of election results, and post-election reporting to certify and validate results), voting systems and associated infrastructure, additionally storage facilities for election and voting system infrastructure as well as polling places and early voting locations.

The definition explicitly does not include political action committees, campaigns, or any other non-state or local government election related group.[8]

Behind the classification and specific definition of CEI and the DHS decision in 2017 stood discoveries from the investigations on the broad and Russian-backed election campaign interference, starting well before (2014) and lasting after the 2016 US presidential election.[9] The interference in the 2016 US general election was said to have been unprecedented. Widespread foreign interference and meddling were reported. Specifically in 2019, the US Senate Intelligence Committee confirmed all 50 states were subject to some form of attack on their elections process in 2016.[10] Such activity inherently brought increased focus to the 2020 general election, especially given that Special Counsel Robert Mueller III testified to Congress (also in 2019) that interference was ongoing and continuing.

[7] Yara Bayoumy and Warren Strobel, "U.S. Intel Report: Putin Directed Cyber Campaign to Help Trump," Reuters (website), January 6, 2017, https://www.reuters.com/article/us-usa-russia-cyber-idUSKBN14Q1T8.

[8] "Election Security," DHS (website), n.d., https://www.dhs.gov/topics/election-security.

[9] US Congress, *Report of the Select Committee on Intelligence, United States Senate, on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 1: Russian Efforts against Election Infrastructure with Additional Views*, 116th Cong. (2020), https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf, 3.

[10] David E. Sanger and Catie Edmonson, "Russia Targeted Election Systems in All 50 States, Report Finds," *New York Times* (website), July 25, 2019, https://www.nytimes.com/2019/07/25/us/politics/russian-hacking-elections.html.

Broader Activities against Democratic Elections Ongoing

In 2020, another election year, the NATO Parliamentary Assembly (PA) in Brussels—the NATO-independent discussion forum for parliaments of NATO members and consulting forum for NATO—adopted a resolution on what they called "the Russian Challenge" and turned their eyes on other countries and NATO allies rather than only the United States. The resolution focused on the broader Russian activities and how NATO could deal with additional aggression conducted by Russia, its affiliates, and proxies in other regions of NATO and within the territories of NATO allies. In No. 13 of the resolution, the signatories condemn illegal organization and holding by Russia of the elections to the State Duma in the annexed Crimea as well as compelling Ukrainian citizens with illegally issued Russian passports to take part in elections in the occupied territories in Donetsk and Luhansk regions.[11] The resolution says Russia has also sought to undermine necessary reforms and interfered in elections in the Republic of North Macedonia and Montenegro.[12] It is therefore recognized the problem of election integrity does not exist in one state only, but in many states.

Manifold Types of Adversaries on the Rise

At the same time, recognized types of adversaries and terrorist attacks against democratic structures and processes have become more diverse than they were when NATO adopted its 2010 Strategic Concept in an "age of relative stability."[13]

In that past order, eastern Europe (and potentially Russia) could find a place while the United States remained as an affirmative European power. NATO's 2022 Strategic Concept reads differently.

[11] Political Committee, *Maintaining NATO'S Focus on the Russian Challenge: Resolution 470* (Brussels: NATO Parliamentary Assembly, 2021), https://www.nato-pa.int/download-file?filename=/sites/default/files/2021-10/2021%20-%20NATO%20PA%20Resolution%20470%20-%20Russia.pdf.

[12] Gerald E. Connolly, "2019 – NATO@70: Why the Alliance Remains Indispensable," NATO Parliamentary Assembly (website), October 12, 2019, https://www.nato-pa.int/document/2019-nato70-why-alliance-remains-indispensable-146-pctr-19-e-rev1-fin.

[13] Daniel S. Hamilton, "One Plus Four: What NATO's New Strategic Concept Should Say, and How to Achieve It," Real Instituto Elcano (website), December 17, 2021, https://www.realinstitutoelcano.org/en/analyses/one-plus-four-what-natos-new-strategic-concept-should-say-and-how-to-achieve-it/.

Current Situation in NATO

NATO's Resilience Challenge

The military Alliance needs to anticipate, identify, mitigate, and recover from attacks with minimum disruptive impacts on the Alliance's social, political, and military cohesion. As the current geopolitical competition for political leadership goes beyond the traditional power play and the use of hard power, the last 10 years have been primarily about new forms of governance and livelihoods. Despite this, political systems and the violation of borders and national territories re-emerged in Europe in 2014 with the invasion of Ukraine and after the Yugoslav wars in the 1990s. This continuing problem became evident within NATO member states and placed the challenge of strengthening democratic and social resilience at the center of the new international system and competition after an era of stability that began in 1989 with the fall of the Berlin Wall.

This age of stability is a paradigm lost. In Europe and elsewhere, lower trust in institutions, increasing political apathy, and political polarization and fragmentation takes place. Different kinds of manipulation and disinformation, especially during electoral campaigns, are on the rise, and highly polarized societies are the most vulnerable to this. The key challenge for NATO democracies in the twenty-first century is to find the right means to protect the democratic freedoms that come with more access to information and infrastructures while limiting the risks that go along with them. To adapt to the new situation and the ongoing change in the international order, the alliance must reaffirm shared values and principles—the glue binding NATO together and the raison d'être for NATO.[14]

Democratic Resilience: Foundation of the Cohesion of the Alliance

Within the broad field of democratic resilience, the specific field of election integrity/election infrastructures is the strategic backbone that needs to be secured first. In some countries, this area is mostly unguarded compared to emerging threats. A breach on the other side could cause a massive disruption. A portion of Germany's election infrastructures is exempt because it is not fully digitized and as vulnerable as other systems have been (for example, in the United States and Estonia, which

[14] NATO Parliamentary Assembly, *The NATO Parliamentary Assembly's Contribution to the NATO 2022 Strategic Concept* (Brussels: NATO, February 22, 2022), https://www.nato-pa.int/download-file?filename=/sites/default/files/2022-03/NATO%20PA%20contribution%20to%20the%202022%20Strategic%20Concept.pdf.

have a blockchain-based i-Voting system, and in Northern Europe, where digitalization has made progress).

At first glance, the diversity of election systems in countries and their vulnerabilities forms a second-tier resilience challenge as it falls under the scope of national sovereign decisions and responsibilities. NATO is foremost a military alliance, focusing on the three core tasks of deterrence and defense, crisis prevention and management, and cooperative security, even after the announcement of the renewed NATO 2022 Strategic Concept at the NATO Summit 2022 in Madrid.[15]

Nonetheless, with the Preamble of the North Atlantic Treaty, NATO members committed themselves to "safeguard the freedom, common heritage and civilization of their peoples, founded on the principles of democracy, individual liberty and the rule of law."[16] By doing so, they accepted and bound themselves to shared values, including the Western way of living, rights for the people, and the rule of law as common denominator among Allied partners. This also makes NATO a political alliance.

Yet, is there a broader and growing need to implement operationally a comprehensive concept of resilience to secure those shared values among NATO members? Does NATO need to strengthen the Alliance's ability to anticipate, prevent, and, if necessary, protect against and bounce forward from disruptions to critical functions of member societies? Does that mean election security became one of NATO's core tasks and is essential to the other three core tasks of NATO as Daniel S. Hamilton and Gerald E. Connolly of the United States, the president of the NATO Parliamentary Assembly, have been promoting since the NATO Parliamentary Assembly's 2019 report on the 70th anniversary of the founding of NATO?[17]

Such an additional task has not been integrated into allied planning or operational activities. Comprehensive concepts of resilience haven't been implemented beyond country-by-country baseline requirements at the 2022 NATO Summit in Madrid.[18] However, the 2022 Strategic Concept

[15] Parliamentary Assembly, *NATO 2022 Strategic Concept*.

[16] "North Atlantic Treaty, Released to the Press, March 18, 1949," *International Organization* 3, no. 2, (1949): 393–96.

[17] NATO Parliamentary Assembly, *Working Group on a NATO Democratic Resilience Centre* (Brussels: NATO, October 2021), https://www.nato-pa.int/download-file?filename=/sites/default/files/2021-11/NATO%20PA%20WORKING%20GROUP%20ON%20A%20NATO%20DEMOCRATIC%20RESILIENCE%20CENTRE_5.pdf.

[18] Hamilton, "One Plus Four," 5.

refers to the will of the Allies to continue to stand together to defend security, values, and the democratic way of life to ensure the Alliance's continued success only.

The idea for establishing a NATO Democratic Resilience Centre within NATO Headquarters was promoted by the president of the NATO Parliamentary Assembly. It should provide support to individual Allies, upon their request, for strengthening societal resilience to resist interference from hostile actors in the functioning of their democratic institutions and processes. The idea was not made concrete by the decisions at the Madrid summit, though 29 out of 30 members of the Parliamentary Assembly and its resolution No. 466 backed the proposal. The countries who wished to deter and defend more effectively below the threshold of Article 5 of the treaty did not have their vote reflected in a decision.

Does this demonstrated interest of member states, based on a recognized growing threat and need, lead to a duty of care on the part of NATO, but at a much lower level than that of the usual NATO missions?

Why NATO Should Care for Critical Election Infrastructure

Enabling Effective Fulfillment of NATO's Three Core Tasks

The strongest line of defense against threats are resilient democratic institutions with robust and transparent accountability mechanisms that enable NATO's three core missions to be fulfilled effectively. Therefore, the heads of state and government of the North Atlantic Alliance affirmed in Madrid that national and collective resilience are an essential basis for credible deterrence and defense, the effective fulfillment of the Alliance's three core tasks and vital in efforts to safeguard societies, populations, and shared values. These democratic values and institutions upon which the NATO alliance was founded are under pressure and permanently being investigated from external and internal adversaries.

While NATO members are under permanent surveillance and attacks conducted by adversaries, they have seen fundamental technological changes and changes of control in their infrastructures. Most member states are now owned by private parties and some by adversary state-owned or related companies (such as the Chinese telecom giant Huawei). The Alliance and its members and partners face interdependency and large-scale challenges in all critical infrastructure sectors and the public sector—depending on their specific circumstances. Together, they rely much more on cooperation and coordination between different sectors of society, industry, and technology than ever before to fulfill NATO's three core tasks. Allies and partner countries with weak protection are vulnerable and threaten the strength of the Alliance.

Broader and Coordinated Approaches to Resilience as a National Duty

NATO 2030 Agenda

In another reaction to that ever-growing complex threat landscape, the NATO 2030 agenda set up an ambitious plan to make sure NATO remains ready, strong, and united for a new era of increased global competition. It includes an improved and coordinated resilience approach and the goal to uphold the rule-based international order. Member states agreed to develop resilience objectives to guide tailored-by-nation resilience goals and implementation plans based on more measurable Alliance-wide resilience objectives. The Allies agreed to strengthen NATO's relationship with like-minded partners such as the European Union.

NATO Brussels Summit Communiqué

In the NATO Brussels Summit Communiqué of June 14, 2021, the heads of participating state and governments agreed on securing the Alliance and its members from threat actor's interferences. Russia was identified as an actor using hybrid actions against NATO, including through proxies. The attacks identified and included in the NATO document cover attempted interference in Allied elections and democratic processes, political and economic pressure and intimidation, widespread disinformation campaigns, malicious cyber activities, and those of cybercriminals operating from member states' territories, including those who target and disrupt critical infrastructure in NATO countries.[19]

While the Alliance is already active in the field of election security and has accepted this emerging threat to NATO stability, specific action is now necessary and has been agreed to with the broader view of democratic resilience. Critical infrastructure security remains a matter of national

[19] "Brussels Summit Communiqué: Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Brussels, 14 June 2021," NATO (website), last updated on July 1, 2022, https://www.nato.int/cps/en/natohq/news_185000.htm?selectedLocale=en.

security.[20] NATO has expressed in communiques and frameworks that it is concerned about the broader effects of resilience caused by attacks on elections, election integrity, and infrastructures in member states and partner countries. It would be possible for NATO member states to classify their election infrastructure as critical infrastructure, as has been done in the United States. They could also build on political wishes of European ruling parties (such as Germany's Free Democratic Party) that focus on securing election infrastructures across Europe as critical infrastructures. The next section discusses whether NATO can take the helm and initiate concrete measures and if so, what these measures could be.

Measures NATO Can Apply to Election Security

NATO could indirectly support democratic resilience in member states with a few measures. It was also stated in the 2022 Strategic Concept that consultations shall be deepened to address all matters affecting security. Additional measures include creating a new framework based on the 2014 Wales Summit Framework Nation Concept, establishing a Democratic Resilience Centre within NATO, and developing resilience objectives to guide nationally tailored goals and implementation plans as stated in the NATO 2030 agenda, but with a specific view to critical election infrastructure.

A New Framework Concept

Based on the Framework Nations Concept (FNC) of the 2014 Wales Summit, NATO could establish new frameworks.[21] In 2013, the idea behind the new concept was to enhance collective defense through multinational cooperation. The concept proved to be successful in all three types of FNCs that have been established since 2014 (UK-led FNC, German-led FNC, Italian-led FNC).[22] The basic principle of treaty planning is that each nation should undertake the task, or tasks, for which

[20] "Building Transatlantic Resilience: Why Critical Infrastructure Is a Matter of National Security," NATO (website), December 10, 2020, https://www.nato.int/cps/en/natohq/opinions_180067.htm; and "Strengthened Resilience Commitment," NATO (website), June 14, 2021, https://www.nato.int/cps/en/natohq/official_texts_185340.htm.

[21] "Wales Summit Declaration Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Wales," no. 67, NATO (website), September 5, 2014, https://www.nato.int/cps/en/natohq/official_texts_112964.htm?mode=pressrelease.

[22] Sean Monaghan and Ed Arnold, "Indispensable, NATO's Framework Nations Concept beyond Madrid," CSIS (website), June 27, 2022, https://www.csis.org/analysis/indispensable-natos-framework-nations-concept-beyond-madrid.

it is best suited. Certain nations because of their geographic location or capabilities will conduct appropriate specific missions.[23]

The FNC-concept of 2014 encouraged nations within NATO to work "multinationally for the joint development of forces and capabilities required by the Alliance, facilitated by a framework nation."[24] The concept includes regional FNCs intricately linked to thematic specializations. While not a new concept, it has proven to be a complex challenge due to different views and the tendency of states not to give up on their sovereignty. The concept of an FNC, however, could offer a more flexible approach to solve critical problems among member states.

FNCs could also be built on existing NATO Centres of Excellence.[25] In the case of election security, these centres could be the Tallinn-based NATO Cooperative Cyber Defense Centre of Excellence, the Ankara-based NATO COE DAT, and the Riga-based NATO Strategic Communications Centre of Excellence. These centres could tackle the challenges relating to election integrity and the safeguarding of critical election infrastructures—cyber security and elections as a social process with a specific view to strategic communications.[26] New work could build on the work already done by the US GCC that outlined further actions to strengthen the security of elections and election infrastructures.[27]

A thematic FNC could develop best practices and share information and knowledge. It would offer additional working space and operational and deployable capability to complement existing COE activities. It could also work on assessments and shared definitions, checklists, and key performance indicators to be achieved by member states, safeguarding their critical election infrastructure from emerging threats. The United States could be viewed as a key opinion leader (KOL) for inventing the definition of CEI. The United States could be joined by Germany, where some politicians

[23] C. H. Donnelly, *Note by the Secretary of the North Atlantic Defense Committee on the Strategic Concept for the Defence of the North Atlantic Area* (Brussels: NATO, 1949), https://www.nato.int/docu/stratdoc/eng/a491201a.pdf.

[24] "Wales Summit Declaration: Issued by the Heads of State and Government participating in the Meeting of the North Atlantic Council in Wales," NATO (website), September 5, 2014, https://www.nato.int/cps/en/natohq/official_texts_112964.htm.

[25] Monaghan and Arnold, "Indispensable."

[26] Sebastian Bay and Guna Šnore, Protecting Elections: A Strategic Communications Approach (Riga, LV: NATO Strategic Communications Centre of Excellence, 2019), https://stratcomcoe.org/cuploads/pfiles/nato_report_-_protecting_elections_1.pdf.

[27] "Election Infrastructure Subsector: Government Coordinating Council Charter," February 2021, https://www.cisa.gov/sites/default/files/publications/gov-facilities-EIS-gcc-charter-2021-508.pdf.

advocate for a shared CEI-model on a European level. The framework would include partners from two continents, which could help overcome differences and individual political views, especially since the United States and Germany represent two continents' views on national security based on shared values.

Centre for Democratic Resilience within NATO

In 2019, the NATO Parliamentary Assembly president proposed the creation of a centre within NATO to coordinate Allied efforts to strengthen democratic resilience. The recommendation was endorsed by the full Assembly in resolution 457. The president has placed safeguarding the Alliance's shared democratic values at the heart of his presidency. The establishment of the NATO Democratic Resilience Centre is a key priority. The proposal is a response to the growing threat to democracies from within and without. As stated in its founding treaty, NATO is an alliance of democracies, committed to safeguarding "the freedom, common heritage and civilization of their peoples, founded on the principles of democracy, individual liberty and the rule of law."[28] Yet, no structure fully dedicated to democratic resilience exists within NATO.

The centre's activities would be centered around two broad lines of effort safeguarding critical election infrastructures. First, it would monitor and identify challenges to democracy, human rights, and the rule of law among member states. Second, it would facilitate democracy and governance assistance to member states on a voluntary basis. The centre could assist member-state governments to improve election integrity and other governance challenges undermining democracy and making member states vulnerable to external malign influence.[29] This centre could be the place to exchange information on a trusted basis and help member states better understand the vulnerabilities of critical election infrastructures.

Future Definition of Critical Election Infrastructure

The first job of the centre would be creating a NATO-wide definition of critical election infrastructure. The US definition of CEI is currently based on lessons learned and results from investigations in 2017. The public knows the Russian campaign included the following tools, events, and actions from the 2016 presidential election. Theses actions included hacking state voter databases

[28] "North Atlantic Treaty," 1949, https://www.nato.int/cps/en/natolive/official_texts_17120.htm.

[29] "Working Group on NATO Democratic Resilience Centre, Origins and Purpose."

for insecurities and hacking e-mails of the Hillary Clinton campaign, the Democratic Congressional Campaign Committee, and the Democratic National Committee.[30] It also included hacking attempts on e-mails from Senator Marco Rubio's campaign and the Republican National Committee, releasing politically damaging information about certain candidates on the Internet and spreading propaganda on Twitter, Facebook, YouTube, and Instagram. The interference also included using fake social media profiles to invite people to events and stage rallies in Florida and Pennsylvania, set up meetings with members of the Trump campaign and associates, and float business propositions for a skyscraper in Moscow dedicated to the Trump Organization.[31]

The Senate Select Committee on Intelligence (SSCI) oversaw analyzing evidence gathered by Special Counsel Robert S. Mueller III, who discovered Russian actors scanned databases for vulnerabilities, attempted intrusions, and, in a small number of cases, successfully penetrated voter registration databases. The SSCI also discovered the final goal of the interference—to damage the Clinton campaign, boost Trump's chances, and sow distrust in American democracy overall. These actions reflect Russia's clear intent to affect votes, destabilize American society, and threaten societal resilience in the United States.[32]

Internet of Behaviors as a Driver for a Changing Security Threat Landscape

Especially with a view to the power of social media platforms, be they classified critical infrastructures or not, the business and technological development of such platforms is relevant for NATO. Facebook changed its strategy and renamed the company "Meta." With that step, a new technological era of the metaverse has risen in the lives of many people. The metaverse is the digital reality that combines aspects of social media, online gaming, augmented reality (AR), virtual reality (VR), and cryptocurrencies to allow users to interact virtually. This new world and its business models are built on the behavior of its users, the people.

[30] Abigail Abrams, "Here's What We Know So Far about Russia's 2016 Meddling," TIME (website), April 18, 2019, https://time.com/5565991/russia-influence-2016-election/.

[31] Special Counsel Robert S. Mueller III, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, vol. 1 of 2 (Washington, DC: Department of Justice, March 2019), https://www.justice.gov/archives/sco/file/1373816/download.

[32] US Congress, *Report of the Seelct Committee on Intelligence, United States Senate on Russian Active Measures Campaign and Interference in the 2016 U.S. Election: Volume 1: Russian Efforts against Election Infrastructure with Additional Views*, 116th Cong. (2020), 116–290, https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf.

Gartner, a US tech research analytics firm, has announced the rise of the new "Internet of Behaviors" (IoB). The term is explained in Gartner's 2021 *Top Strategic Technology Trends-Report*.[33] It is defined as the use of IoT's data to influence behavior, which will, potentially create a new group of threat actors at a place where influencing people's behavior stands at the center of the platform's purpose.[34] In a world where everything happens in cyberspace—shopping, socializing, working, forming wills, voting in elections, advertising, and marketing—the Metaverse should be considered part of a future critical electoral infrastructure.

Threat Actors

A second program line should focus on types of threat actors. Shared assessment and shared information could help the Alliance strengthen resilience and fight interferences when they arise.

Internal Threat Actors

Although Russia has caused most of the reactions from NATO member states with its interferences and activities, the country is not alone in the group of adversaries weaponizing election infrastructures. In democracies, once elected, populist politicians with authoritarian leanings can work to paralyze the executive branch of government. For example, politicians started using "dark posts" and propaganda to target voters and undermine the electorate's faith long before Brexit in 2016 and the US elections in 2016 and 2020.[35] There are forces at work that intend to eat away at liberalism from within democracies.

In 2021, retired US Marine Corps General James Mattis said the West, to him, seems to be in a strategy-free mode where democratic values are doubted.[36] In Germany, Querdenker spread bizarre conspiracy theories, and it was revealed in December 2022 that the anti-constitutional group

[33] Kasey Panetta, "Garnter Top Strategic Technology Trends for 2021," Gartner (website), October 19, 2020, https://www.gartner.com/smarterwithgartner/gartner-top-strategic-technology-trends-for-2021.

[34] Panetta, "Top Strategic Technology."

[35] "Virtual Propaganda – Reporter Peter Kreysler in Conversation," ARD Audiothek (website), September 1, 2021, https://www.ardaudiothek.de/episode/das-ard-radiofeature/virtuelle-propaganda-reporter-peter-kreysler-im-gespraech/ard-de/92319872.

[36] James N. Mattis, "Allies, Allies, Allies" (speech, 2021 Atlantik-Brücke Young Leaders Conference, Brandenburg, 2021), https://www.atlantik-bruecke.org/en/allies-allies-allies-general-james-mattis-at-the-young-leaders-conference/?pk_campaign=RECAP+13%2F2021&pk_kwd=https%3A%2F%2Fwww.atlantik-bruecke.org%2Fen%2Fallies-allies-allies-general-james-mattis-at-the-young-leaders-conference%2F.

"Reichsbuerger" planned to storm the Reichstag in Berlin, knock out electricity, and take over the government.[37] In the US, armed militias and extremists stormed the US Capitol on January 6, 2021, spreading their views on the election results, claiming the election was stolen from Donald Trump. In Western societies, politically motivated activists, be they left-wing or right-wing or politically motivated, are classified as adversaries against the core values of democracy.[38]

External Threat Actors

At the same time, NATO as a military alliance faces stronger headwinds from outside adversaries weaponizing critical infrastructure inside NATO. The enormous increase in the number of non-state actors relates to the end of the Cold War, globalization, and processes of democratization since the 1990s. With the liberalization of the flows of goods and financial services and the lifting of stringent barriers to the movement of persons, companies, media, and nongovernmental organizations, all types of actors can move easily across the world and have quicker and easier access to capital and labor. Cheap information technology means even the smallest organizations and movements can portray themselves as actors not bound by national sovereignty.

The combination of a high diversity of actors and the ongoing technological developments makes it difficult to determine where threats originate. Dual-use technologies that can make life more pleasant can also fall into the hands of ill-intentioned non-state actors. Increasingly, these terrorist groups and adversaries organize themselves individually as loose illegal networks that are difficult to track. The groups make smart use of global communications chains and secret communication channels (such as dark net, crypto mobile phones, and chat programs). These terrorist groups seek to undermine weak state institutions and the precarious security situation of citizens in fragile states. Like nation-states, those groups use "hard" military means and "softer" instruments (such as media, social media,

[37] Svenja Moller, "Bundesweite Razzia: Gruppe soll Staatsstreich geplant haben," Augsburger Allgemeine (website), December 7, 2022, https://www.augsburger-allgemeine.de/panorama/bundesweite-razzia-in-reichsbuergerszene-25-festnahmen-id64800536.html; and see Michael Nienaber, "Germany Conducts Nationwide Raid to Thwart Right-Wing Extremists Planning Coup," Bloomberg (website), December 7, 2022, https://www.bloomberg.com/news/articles/2022-12-07/germany-detains-25-suspects-in-nationwide-domestic-terror-raids?leadSource=uverify%20wall.

[38] *Verfassungsschutzbericht 2021* (Berlin: Bundesministerium des Innern und für Heimat, 2022), https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/verfassungsschutzberichte/2022-06-07-verfassungsschutzbericht-2021-startseitenmodul.pdf?__blob=publicationFile&v=2, 26.

and the Internet) to bolster their legitimacy and win the hearts and minds of potential supporters.

Specific actors with known interest in interfering with the will of the people are China and affiliated groups, Russia and affiliated groups, and other authoritarian states (Iran and North Korea), and terrorist groups (al-Qaeda, Boko Haram and Da'esh, and the Taliban).[39]

The Influence Industry: A New Type of Adversary

In an assessment of interferences in election processes in 2018, the UK House of Commons Digital, Culture, Media and Sport Committee in London published the "Disinformation and Fake News: Interim Report."[40] In the report, the committee focused on distinct types of threat actors. It included data analytics firms and strategic communications companies as adversaries. The committee members picked the company Strategic Communications Laboratories (SCL) Elections and related companies as examples and stated the companies worked on campaigns that were not financed in a transparent way, overstepping legal and ethical boundaries.[41] The companies were said to run campaigns globally. Representatives of the companies were cited with talking about using misinformation, dirty tricks, and social media manipulation to influence elections around the world and boasted of using bribery, honey traps, and sex workers to discredit politicians and influence the political outcome of elections in several countries.[42]

Information was provided to the committee about the manipulation of social media companies, in order to play on and distort people's negative views of themselves and others.[43] Election campaigns and referenda manipulated by SCL are said to have taken place in the Kenya Kenyatta campaign 2013, the Kenya Kenyatta campaign 2017, Ghana 2013, Mexico, Brazil, Australia, Thailand, Malaysia, Indonesia, India, Nigeria, Pakistan, Philippines, Germany, England, Guyana, Czech Republic, Kosovo; and the Caribbean, St. Kitts and Nevis,

[39] "Exploiting Disorder: al-Qaeda and the Islamic State," Crisis Groups (website), March 14, 2016, https://www.crisisgroup.org/global/exploiting-disorder-al-qaeda-and-islamic-state.

[40] Digital Culture, Media, and Sport Committee, *Disinformation and "Fake News": Final Report*, HC 1791 (London: House of Commons, February 18, 2019), https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf.

[41] Digital Culture, Media, and Sport Committee, *Disinformation and "Fake News."*

[42] Digital Culture, Media, and Sport Committee, *Disinformation and "Fake News,"* 53.

[43] Digital Culture, Media, and Sport Committee, *Disinformation and "Fake News."*

and Dominica.[44] Part of that work was also a referendum in St. Vincent and the Grenadines. The report says Henley and Partners organized funding for the campaigns in exchange for citizenship-by-investment (CBI) programs.[45] The companies' representatives admitted they worked for the British government, the US government, and other Allied governments.[46]

The report concludes with a statement from the committee: "We . . . urge the Government to ensure that the National Crime Agency thoroughly investigates these allegations."[47] The report also urged the government to audit the public relations and strategic communications industries, warning in its final report how "easy it is for discredited companies to reinvent themselves and potentially use the same data and the same tactics to undermine governments, including in the UK."[48] It was said those companies need to be monitored and regulated as they operate in a constant conflict of interest situation.

Emma Briant, a researcher who consulted with UK authorities, supported stricter regulation of strategic communications companies—as she sees them as adversaries of democratic societies, with the establishment of professional licensing that can be revoked if necessary. Such licensing "would commercially protect the industry itself, creating a resulting "soft power" economic benefit for industry and Western governments."[49]

She gave two examples of Cambridge Analytica's perceived conflicts of interest: (1) Cambridge Analytica pitched an offer to Lukoil, a Russian oil company with ubiquitous political connections, while at the same time, the SCL Group delivered counter-Russian propaganda training for Western states, and (2) "around the same time, Alexander Nix from Cambridge Analytica contacted Julian Assange at Wikileaks amplifying the release of damaging e-mails; Russia has been accused of the hacking of these, which it denies."[50]

[44] Digital Culture, Media, and Sport Committee, *Disinformation and "Fake News,"* 54.

[45] Digital Culture, Media, and Sport Committee, *Disinformation and "Fake News,"* 58.

[46] Digital Culture, Media, and Sport Committee, *Disinformation and "Fake News,"* 58.

[47] Digital Culture, Media, and Sport Committee, *Disinformation and "Fake News,"* 50, 59, 72.

[48] Jesse Witt and Alex Pasternack, "The Strange Afterlife of Cambridge Analytica and the Mysterious Fate of Its Data," Fast Company (website), July 26, 2019, https://www.fastcompany.com/90381366/the-mysterious-afterlife-of-cambridge-analytica-and-its-trove-of-data.

[49] Emma Briant, "Written Evidence: Dr. Emma Briant, Senior Lecturer at University of Essex" (London: House of Commons, Committee on Culture, Media, and Sport), https://committees.parliament.uk/writtenevidence/39329/pdf/.

[50] Briant, "Written Evidence."

Briant suggested US and UK inquiries examining the intelligence and oversight mechanisms in information operations contracting strengthen these systems.[51] Further, the countries should ensure defense-derived expertise and techniques are not used in electoral campaigns or pitched to organizations with risk factors for national security. She proposed additional solutions like the monitoring and restriction of technologies and methods developed by contractors with defense collaboration and funding being used in elections or pitched for any work abroad. A need for greater transparency in government contracting, reporting mechanisms, and substantial penalties for defense contractors found to be obscuring overlaps and company relationships from government was included in her report.

Threat Responses

Another program line for the work on securing critical election infrastructure could be the broader sector of responses to threats against CEI. It should begin with a dynamic and holistic view of the complex and evolving security landscape in which NATO and NATO members operate.

Holistic Monitoring Approach to Threat Responses

Election infrastructure security is a complex problem covering several layers of infrastructures and types of organizations and groups of people, responses, and recommendations. For this reason, the Riga-based NATO Strategic Communications Centre divides elections into three types: the administrative process, the will and ability of voters to participate in elections, and the election as a political process.

NATO could eventually come from different angles to analyze the problem and find appropriate answers. Starting at the infrastructural angle might not be sufficient. With the intensifying digital penetration of everything in the world that transforms into the Internet of Behaviors, blurring lines between the individual human's behavior, online life and traditional organizations should be considered, and with them, all layers of the system.

[51] Briant, "Written Evidence."

Those layers are the:

- Organizational layer
- Individual layer
- Time layer
- Impact layer
- Layer and scope of uncertainty

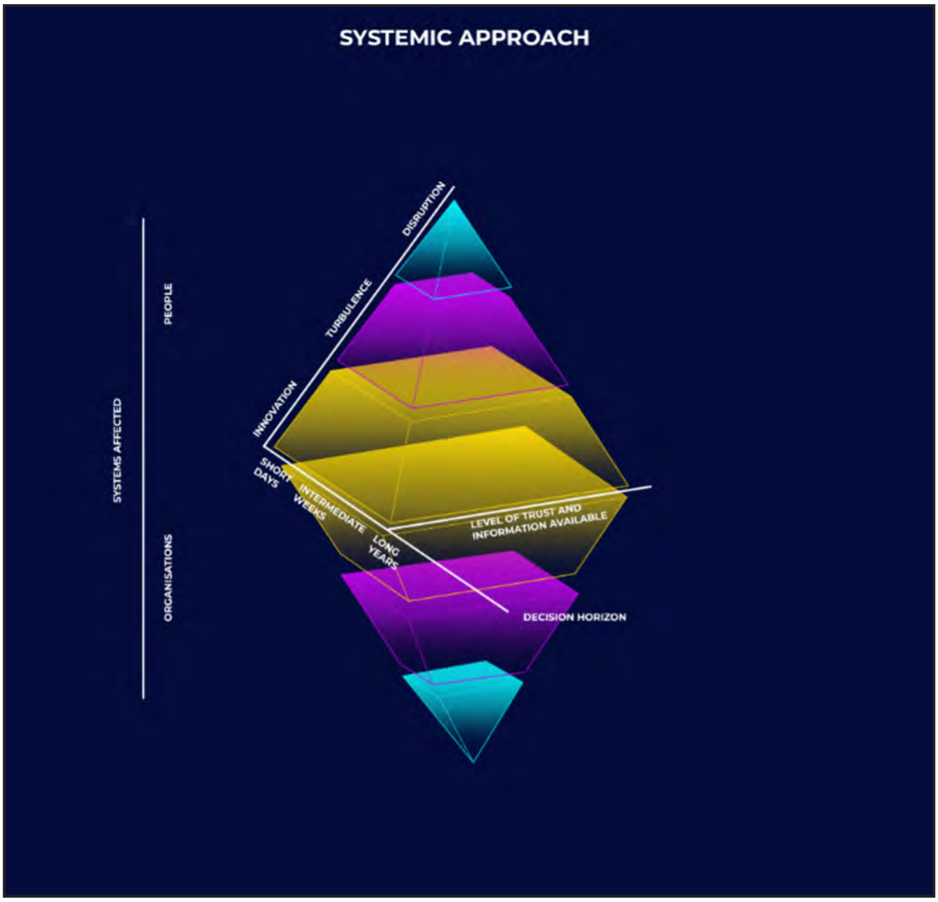


Figure 5-1. Layers of systems affected by the Internet of Behaviors
(Original by author)

This holistic view, which considers that different layers influence each other at the same time but can have different effects because there are so many interdependencies, could be of significant use in the current rapidly evolving and changing security landscape. To tackle the challenge of the multilayer matrix, the GCC thinks of the people involved in election processes. These people and decisionmakers need additional human support to navigate the cyber sphere. All people involved in election processes need better training. In addition, a management and staffing plan needs to be implemented to support the efforts.

The GCC also aims to secure voting equipment and voter data, update all operating systems and software, establish incident tracking systems and software, and deploy multifactor authentication products and new password management software. The GCC recommended auditing the entire election process; patching management systems, network architecture, and cybersecurity assessment; and enabling network segmentation and air-gapping.[52]

A Strategic Communications Approach 2019

The NATO Strategic Communications Centre of Excellence in Riga, Latvia, addressed the social part of election processes and published a study in 2019 on how to respond to election threats from a strategic communication perspective.[53] The study outlines three types of threats to elections, types of interferences, and common stratagems having relations to CEI.[54]

- Threats against the election as an administrative process
- Threats against the will and ability of voters to participate in elections
- Threats against the election as a political process

The centre suggests a mapping of the strategic communications dimensions.

[52] Election Infrastructure Subsector Government Coordinating Council, *Election Infrastructure Security Funding Considerations* (Washington, DC: DHS/CISA, March 12, 2020), https://www.cisa.gov/sites/default/files/publications/20_0311_cisa_eis-gcc-funding-considerations.pdf.

[53] Sebastian Bay and Guna Šnore, *Protecting Elections: A Strategic Communications Approach*, (Riga, LV: NATO Strategic Communications Centre of Excellence, 2019), https://stratcomcoe.org/cuploads/pfiles/nato_report_-_protecting_elections_1.pdf.

[54] Bay and Šnore, *Protecting Elections*, 10–11.

Information Landscape

What is the situation NATO and NATO members are in, and what are they protecting? It suggests mapping the core elements of the information environment and the election process, identifying elements affecting the decision making of voters in a country, and identifying and prioritizing the most important things to protect.

Threat Assessment

What is the threat? What does the current threat assessment look like, and what are the publicly recognized security risks? What does the threat consist of? How could activities aimed at influencing information materialize? What are the likelihood and consequences of influence activities? Which risks do we accept?

Risk and Capability Assessment

How do countries handle the identified risks? How can they reduce the probability of election interference? How can they reduce the consequences of election interference? What is the monitoring capability (such as scope, stakeholders, mandates, and tasks)? What are the deterrence mechanisms at the members' disposal? What are the mechanisms through which the countries will coordinate responses?[55]

In the analysis, the team found that individual methods and techniques for election interference are rarely used in isolation. Rather, influence operations and campaigns most often combine a multitude of methods and techniques into a complex chain of events or stratagems. While such combinations are theoretically infinite, some stratagems are frequently encountered in contemporary influence operations.[56]

These different findings and their broad scope, interdependencies, and diverse playing fields support the idea of starting with a holistic view to election integrity and safeguarding CEI in NATO in a new cooperation structure within the Alliance.

[55] Bay and Šnore, *Protecting Elections*, 8.

[56] Bay and Šnore, *Protecting Elections*, 12.

Recommendations and Conclusion: Protection of Election Infrastructure against Terrorism Threat

Democratic resilience and election integrity are foundational to NATO's future successes as a military alliance. This fact was also underlined in the 2022 Strategic Concept where member states reflected an intent to reinforce political unity and deepen consultations to address all matters affecting security—including democratic resilience.

The safeguarding of Western democracies' elections and election infrastructures stand at the epicenter of NATO's assessments and secures the Alliance's core stability. One weak democracy in NATO can weaken the Alliance. NATO's role as a political alliance in creating defense and democratic resilience against disruptions to critical societal functions and cohesion is central to a prosperous future for the Western way of life and the unity of member states.

Putting Election Security High on the Agenda

To protect election infrastructure in the future and safeguard the basic framework of democracy, NATO member states must put election integrity high on the agenda and support shared knowledge from all NATO members. New platforms for discussion, research, or exchange of information can be created to gather and share current developments.

Act on Fast-moving Technological Developments

The rapid development of technologies, including digital technologies and artificial intelligence, should be closely monitored and acted upon as they can fundamentally change the basic characteristics of current electoral infrastructures and the industries behind them.

Concrete Actions Regarding Adversaries

The group of politically motivated terrorists focusing on elections and election infrastructures as key targets need to be monitored, and responses to these growing challenges within and outside democratic societies need to be developed. Monitoring and preventive activities resulting from observation and information sharing must be followed by the development of concrete actions to contain growing threats. These activities require a joint effort by NATO members, as weak members can damage the strength of the community.

Set Up a Dedicated Structure

NATO should implement the 2022 Strategic Concept and the NATO 2030 agenda and set up a dedicated structure to assess election-critical infrastructure in member states. In addition, resilience objectives are needed to guide nationally tailored resilience goals—with a specific focus on critical election infrastructures and election security. Implementation plans on measurable Alliance-wide objectives help member states and allies respond quickly to the ever-changing security landscape.

Select Bibliography

Bay, Sebastian, and Guna Šnore. *Protecting Elections: A Strategic Communications Approach*. NATO Strategic Communications Centre of Excellence. 2019.

Connolly, Gerald E. NATO "2019 – @70: Why the Alliance Remains Indispensable." NATO Parliamentary Assembly (website). October 12, 2019. https://www.nato-pa.int/document/2019-nato70-why-alliance-remains-indispensable-146-pctr-19-e-rev1-fin.

Digital Culture, Media, and Sport Committee. *Disinformation and "Fake News": Final Report*, HC 1791. London: House of Commons, February 18, 2019. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf.

"Election Infrastructure Subsector: Government Coordinating Council Charter." February 2021. https://www.cisa.gov/sites/default/files/publications/gov-facilities-EIS-gcc-charter-2021-508.pdf.

Evans, Carol V. "Future Warfare: Weaponizing Critical Infrastructure." *Parameters* 50, no. 2 (Spring 2020). https://press.armywarcollege.edu/parameters/vol50/iss2/6/.

Verfassungsschutzbericht 2021. Berlin: Bundesministerium des Innern und für Heimat, 2022. https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/verfassungsschutzberichte/2022-06-07-verfassungsschutzbericht-2021-startseitenmodul.pdf?__blob=publicationFile&v=2.

"Wales Summit Declaration Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Wales." no. 67. NATO (website). September 5, 2014. https://www.nato.int/cps/en/natohq/official_texts_112964.htm?mode=pressrelease.

US Congress. *Report of the Select Committee on Intelligence, United States Senate on Russian Active Measures Campaign and Interference in the 2016 U.S. Election: Volume 1: Russian Efforts against Election Infrastructure with Additional Views*. 116th Cong. 2020. https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf.

— Section 2 —

Countering the Terrorist Threat to Medical Resilience

— 6 —

Medical Resilience and Pandemics

Wuraola Oyewusi

ABSTRACT: Medical resilience is a key critical infrastructure in a nation's preparedness against vulnerabilities. Pandemics such as COVID-19 are one of the potent disruptors of this infrastructure. Health systems that are considered low resourced have adapted and deployed seemingly simple but effective methods to survive such disruptions.

Keywords: medical resilience, pandemics, COVID-19, low-resourced health systems

Introduction

In this chapter, medical resilience will be explored as a component of critical infrastructure, and pandemics will be assessed as a disruption using a low-resourced health system to build resilience. Medical resilience is one of the components of critical infrastructure, security, and resilience of any nation. It is aligned with the ability to deal with mass casualties, one of the NATO's seven baseline requirements of resilience for member states. While there are several definitions of resilience across fields, a common feature is the capacity of a system, (such as health care or public health) to identify small or large disruptions and invoke mechanisms to bounce back or establish a new normal situation. There are different scales of disruptions. They could be positive when innovative solutions are deployed or negative, as in a pandemic.

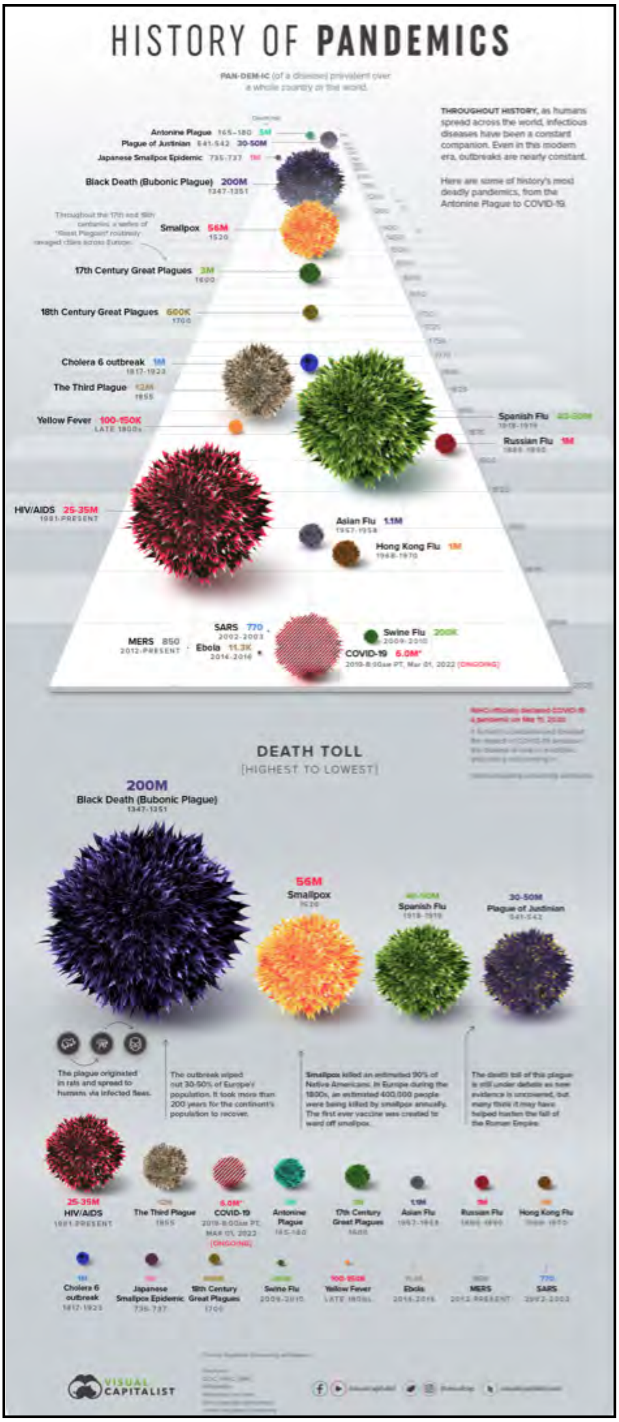
Pandemics are large-scale outbreaks of infectious diseases that can greatly increase morbidity and mortality over a wide geographic area and cause significant economic, social, and political disruption. These pandemic-induced disruptions are often linked to terrorism and armed conflict as terrorists use the power vacuum left by the outbreaks to incite violence and further their causes. A pandemic is different from an epidemic, which is the occurrence of an illness in a community or region beyond normal expectancy. Pandemics are global and defined by geographical scale rather than the severity of illness. Throughout history, there have been several pandemics—the plague in the fourteenth century, smallpox in the mid-eighteenth century, and the Spanish flu in 1918. See figure 6-1. More recent events include tuberculosis, HIV/AIDS, or most currently SARS-CoV-2.

This chapter will discuss COVID-19 in relation to health system capacity and insecurity, leveraging low technology, experience from previous outbreaks, and other lessons from Nigeria that may be useful in other health systems (such as NATO countries). It will also use Boko Haram as a case study in the linkage of terrorism to pandemics and propose recommendations for how such conflicts can be addressed.

COVID-19 Pandemic and Nigeria

COVID-19 is an illness caused by a novel coronavirus called severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2; formerly called 2019-nCoV). Coronaviruses comprise a vast family of viruses. While they typically infect animals, seven of the known types cause disease in humans. Severe acute respiratory syndrome coronavirus 2 likely belongs to one of these. The disease was officially named by the World Health Organization (WHO) on February 11, 2020, and declared a global pandemic on March 11, 2020.[1]

[1] David J. Cennimo and Michael Stuart Bronze, "Coronavirus Disease 2019 (COVID 19)," Medscape (website), https://emedicine.medscape.com/article/2500114-overview?; and Domenico Cucinotta and Maurizio Vanelli, "WHO Declares COVID-19 a Pandemic," *Acta Biomedica* 91, no. 1 (2020): 157, https://www.mattioli1885journals.com/index.php/actabiomedica/article/view/9397.



PAN-DEM-IC (of a disease) prevalent over a whole country or the world.

THROUGHOUT HISTORY, as humans spread across the world, infectious diseases have been a constant companion. Even in this modern era, outbreaks are nearly constant.

Here are some of history's most deadly pandemics, from the Antonine Plague to COVID-19.

Throughout the 17th and 18th centuries, a series of "Great Plagues" routinely ravaged cities across Europe.

WHO officially declared COVID-19 a pandemic on Mar 11, 2020

The plague originated in rats and spread to humans via infected fleas.

The outbreak wiped out 30-50% of Europe's population. It took more than 200 years for the continent's population to recover.

Smallpox killed an estimated 90% of Native Americans. In Europe during the 1800s, an estimated 400,000 people were being killed by smallpox annually. The first ever vaccine was created to ward off smallpox.

The death toll of this plague is still under debate as new evidence is uncovered, but many think it may have helped hasten the fall of the Roman Empire.

Figure 6-1. Infographic showing the history of pandemics
(Image by Visual Capitalist)

Although there is speculation of earlier presence, the first official reported case in humans was recorded in Wuhan, Hubei Province, China, in December 2019. It began as a pneumonic case.[2] The common symptoms are cough, shortness of breath, and loss of smell, and complications could lead to pneumonia, viral sepsis, acute respiratory distress syndrome, kidney failure, or worse, depending on the health status of the individual.[3] People with comorbidities (such as diabetes, respiratory tract infections, or immune suppression) experience worse symptoms.

The principal mode of transmission of the COVID-19 virus is through exposure to respiratory droplets carrying infectious viruses within a space of up to six feet or 1.82 meters. Other methods are contact transmission (such as shaking hands) and airborne transmission of droplets that linger in the air over long distances (greater than six feet). Viruses released in respiratory secretions (such as during coughing, sneezing, or talking) can infect other individuals via contact with mucous membranes.[4] Two months after the first known case of COVID-19 was diagnosed in China, the first confirmed Nigerian case was a passenger who flew into the country from Italy on February 24 and presented with symptoms at a small clinic in Ogun state. The clinician on duty suspected it could be COVID-19. This suspicion was confirmed at the Infectious Disease Centre, Yaba, Lagos State, Nigeria on February 27, 2020.[5]

Health Capacity, COVID-19, and Insecurity in Nigeria

In response to the COVID-19 pandemic, access to critical care was one of the global indicators of readiness. Nigeria's epidemic response is carried out in the context of a fragile and under-resourced existing health delivery system and is complicated by economic, political, social, and security issues throughout the country.[6] To give a context to the capacity, Nigeria has an equivalent of 0.07 intensive care unit (ICU) beds per 100,000 population compared to countries like Germany, the United States, and Türkiye

[2] Nita Madhav et al., "Pandemics: Risks, Impacts, and Mitigation" in *Disease Control Priorities: Improving Health and Reducing Poverty*, 3rd ed. (Washington, DC: International Bank for Reconstruction and Development/World Bank, 2017), https://pubmed.ncbi.nlm.nih.gov/30212163/.

[3] Oluwaseun Oyeranti and Babajide Sokeye, "The Evolution and Spread of COVID-19 in Nigeria," Centre for Petroleum, Energy Economics and Law (website), 2020, 1–18, https://cpeel.ui.edu.ng/publication/evolution-and-spread-covid-19-nigeria.

[4] Madhav et al., "Pandemics."

[5] Chioma Dan-Nwafor et al., "Nigeria's Public Health Response to the COVID-19 Pandemic: January to May 2020," *Journal of Global Health* 10, no. 2 (December 2020), https://jogh.org/documents/issue202002/jogh-10-020399.pdf.

[6] Dan-Nwafor et al., "Nigeria's Public Health Response."

with 29.2, 34.7, and 46 ICU beds per 100,000 respectively.[7] Attacks on critical infrastructure, including health care were not unusual before the COVID-19 pandemic, but the COVID-19 pandemic enabled the proliferation of insecurity via different mechanisms (such as increased armed group activities that can be linked to economic hardship due to lockdown, movement restriction, and gaps in security provisions).

Figure 6-2 shows a detailed framework and the degree of connectedness of three key pathways of the COVID-19 pandemic and conflict in Nigeria—increasing armed group activities, intensifying youth grievances, and shifting pattern of social cohesion. While none of them were solely created by the COVID-19 pandemic, specific elements of the pandemic aggravated and reinforced patterns of behavior by the government, armed groups and community.[8]

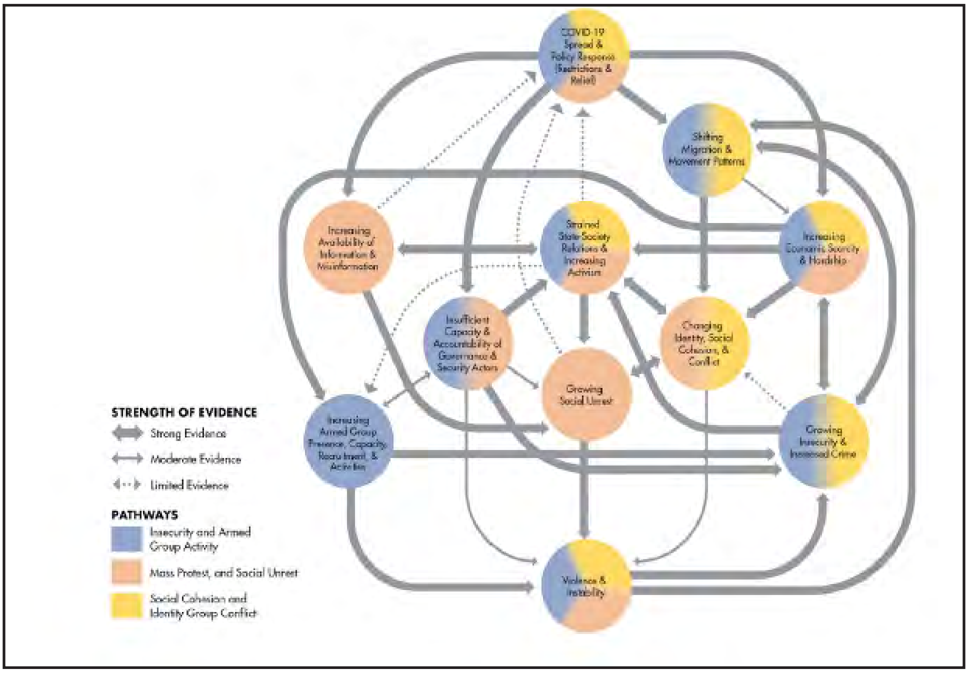

COVID-19 Spread & Policy Response (Restrictions & Relief)
Shifting Migration & Movement Patterns
Increasing Availability of Information & Misinformation
Strained State-Society Relations & Increasing Activism
Increasing Economic Scarcity & Hardship
Insufficient Capacity & Accountability of Governance & Security Actors
Changing Identity, Social Cohesion, & Conflict
Growing Social Unrest
Increasing Armed Group Presence, Capacity, Recruitment, & Activities
Growing Insecurity & Increased Crime
Violence & Instability
STRENGTH OF EVIDENCE
Strong Evidence
Moderate Evidence
Limited Evidence
PATHWAYS
Insecurity and Armed Group Activity
Mass Protest, and Social Unrest
Social Cohesion and Identity Group Conflict

Figure 6-2. Summary of connections between COVID-19 and conflict in Nigeria
(Image by MERCY CORPS)
Source: Mercy Corps, *Living with Two Worrisome Pandemics*

[7] Adeteju Ogunbameru et al., "Estimating Healthcare Resource Needs for COVID-19 Patients in Nigeria," *Pan African Medical Journal* 37, no. 293 (December 2, 2020), https://www.panafrican-med-journal.com/content/article/37/293/full/; and Kamlesh Khunti et al., "Is Ethnicity Linked to Incidence or Outcomes of COVID-19?," BMJ (website), April 20, 2020, https://www.bmj.com/content/369/bmj.m1548.

[8] Mercy Corps, *Living with Two Worrisome Pandemics: How the COVID-10 Pandemic Is Shaping Nigeria* (Portland, OR: Mercy Corps, June 28, 2021), https://www.mercycorps.org/sites/default/files/2021-06/Clash-of-Contagions-Nigeria-Case-June-2021.pdf.

Boko Haram, a prominent terror group, leveraged the COVID-19 pandemic to promote the disruption of health systems and cross border activities and used the lockdown to expand territories and propagate misinformation in a way that undermines public health.[9] The Borno state in Nigeria, considered the epicenter of Boko Haram activities, was one of the worst hit. During the COVID-19 pandemic, the group continued their attack on the region. In February 2020, the group attacked and set ablaze about 18 vehicles carrying passengers in Auno town, Maiduguri, Borno State, and killed three military men in Damboa town, Borno State. In March, the Nigerian military responded with counterinsurgency operations, and about 100 insurgents were reportedly killed near Gorgi village in Borno State.[10]

A faction of Boko Haram, Jama'atu Ahlis Sunna Lidda'awati wal-Jihad, (People Committed to the Propagation of the Prophet's Teachings and Jihad, abbreviated as JAS) led by Abubakar Shekau, released its position in an audio message. Shekau asserted the virus is a divine punishment for world sins and was being used by hypocrites to stop believers from practicing their faith. He urged the continuation of congregational prayers, which was against the public health recommendation.[11] He also claimed his group members were immune from the virus, debunked the claim of his willingness to surrender, and attempted to lure new recruits by the promise of safety and a better life in the Sambisa Forest, where he operates.[12]

Rural banditry due to multifaceted and complex factors characterized by armed robbery, kidnapping, cattle rustling, and raids using both local and sophisticated arms, had escalated. The emergence of the COVID-19 pandemic escalated it—especially in the Northwestern states of Kaduna, Katsina, Sokoto, and Zamfara of Nigeria.[13] Rural banditry—characterized by large-scale killings, abductions, raids on vulnerable communities, and violence against women—started as localized disputes in the agro-pastoral sector of the country but continued and worsened during the COVID-19 pandemic. The intensity and pervasiveness of banditry was also enabled

[9] Audu Bulama Bukarti, "How Is Boko Haram Responding to COVID-19?," Tony Blair Institute for Global Change (website), May 20, 2020, https://institute.global/policy/how-boko-Haram-responding-COVID-19.

[10] Philip Olayoku, "Boko Haram and the COVID-19 Propaganda Dynamics," Spoor Africa (website), September 15, 2020, https://medium.com/spoor-africa/boko-haram-and-the-covid-19-propaganda-dynamics-philip-olayoku-4c9e076b80cb.

[11] Bukarti, "Boko Haram Responding."

[12] Olayoku, "Boko Haram and COVID-19."

[13] Noah Echa Attah et al., "COVID 19 and Increased Security Challenges in Northern Nigeria: Interrogating Armed Banditry in Northwestern Nigeria," *SIASAT* 6, no. 1 (January 31, 2021): 33–44, https://siasatjournal.com/index.php/siasat/article/view/87.

by porous borders and reduced efficiency of law and order due to the overstretch of security agencies.[14] During the lockdown and interstate travel ban, there was free movement of armed bandits and increased attacks. For example, in April 2020, several villages were attacked in Katsina state, and about 50 people were killed. Bandits also demanded villagers surrender COVID-19 palliatives donated as food items.[15] The elements of instability, such as banditry and terrorism, created an atmosphere where people were more concerned about protecting their lives and belongings than adhering to precautionary health measures.[16]

Key Lessons on Managing Pandemics from Nigeria

Leveraging Previous Experience in Outbreaks

One of the defining factors of controlling the COVID-19 pandemic in Nigeria was the experience of managing previous public health crises. For context, the Ebola Virus Disease (EVD) of 2014 came out of the affected countries of Guinea, Nigeria, Liberia, and Sierra Leone. Nigeria should have been the perfect medium for transmission due to its high population of freely mobile people, who are well connected to the rest of the world. However, the swift prevention of community transmission and management by the Nigerian Center for Disease Control (NCDC) nullified the various disease spread mathematical models.[17]

There were several factors in Nigeria, not present in the other countries, that enabled quick action, including the availability of trained health workers with hands-on experience in field epidemiology managing diseases like Lassa fever and cholera. They were educated through the Nigeria Field Epidemiology and Laboratory Training Program (NFELT), established in Nigeria in 2008 by the US Centers for Disease Control and Prevention (CDC) and the Federal Ministry of Health to train field

[14] Angela Ajodo-Adebanjoko, “Rural Banditry in Northwest Nigeria amidst a Global Pandemic: A Gender Perspective,” *Political Crossroads* 24, no. 1 (September 1, 2020): 59–78, https://www.ingentaconnect.com/content/jnp/pc/2020/00000024/00000001/art00005.

[15] Attah et al., “COVID 19 and Increased Security Challenges.”

[16] Yusuff Adebayo Adebisi, “Political Instability in the Context of Health Security amid COVID-19 Pandemic,” *Epidemiology International Journal* 5, no. 4 (December 2021), https://medwinpublishers.com/EIJ/political-instability-in-the-context-of-health-security-amid-covid-19-pandemic.pdf.

[17] Obinna Ositadimma Oleribe, Mary Margaret Elizabeth Crossey, and Simon David Taylor-Robinson, “Nigerian Response to the 2014 Ebola Viral Disease Outbreak: Lessons and Cautions,” *Pan African Medical Journal* 22, no. S1 (October 2015), https://www.panafrican-med-journal.com/content/series/22/1/13/full/.

epidemiologists and functional state epidemiology units in interdisciplinary collaboration and setting up temporary and permanent infectious disease centers and emergency operation centers.[18] This expertise sensitized the health system to the impact of highly infectious diseases, and allowed for the fast reactivation of proactive frameworks used in the management of COVID-19. This lesson makes a case for leveraging existing management frameworks in a pandemic and not reinventing the wheel.

Surveillance, Data Analysis, and Public Data Sharing

During the COVID-19 pandemic, the surveillance and epidemiology team at the Nigerian Centre for Disease Control (NCDC) deployed Surveillance, Outbreak Response Management, and Analysis System (SORMAS), an open and free software for tracking information about confirmed or suspected cases. Its availability aided real-time data analysis, data-based trend analysis, prediction of patterns, rumor management, and interoperability with other systems like the Distinct Health Information System (DHIS), an open-source software platform used in up to 60 countries for reporting, analysis, and dissemination of data for all health programs. A central database like SORMAS is important because there is currently no centralized database for general electronic health records.[19]

The Surveillance, Outbreak Response Management, and Analysis System, an initiative of the Helmholtz Centre for Infection Research (HZI), Germany, was first deployed in Nigeria and Ghana during the Ebola outbreak. SORMAS has been implemented in Nepal and the Ivory Coast, and these partnerships are depicted in figure 6-4. Before COVID-19, its use was expanded for other diseases like Mpox and Lassa fever. The modular design, ease of use, joint ownership, and cross-platform availability of SORMAS enabled it to scale and be updated easily as shown in figure 6-3.[20]

[18] Oleribe, Crossey, and Taylor-Robinson "Nigerian Response."

[19] "Tracking Coronavirus in West Africa and Beyond," European Commission (website), April 23, 2021, https://wayback.archive-it.org/12090/20210423131754/https://ec.europa.eu/info/strategy/recovery-plan-europe/recovery-coronavirus-success-stories/global-response/tracking-coronavirus-west-africa-and-beyond; and "SORMAS in Nigeria: Adapting a Fully Integrated Surveillance System to Track COVID-19," Exemplars in Global Health (website), n.d., https://www.exemplars.health/emerging-topics/epidemic-preparedness-and-response/digital-health-tools/sormas-nigeria.

[20] "SORMAS in Nigeria."

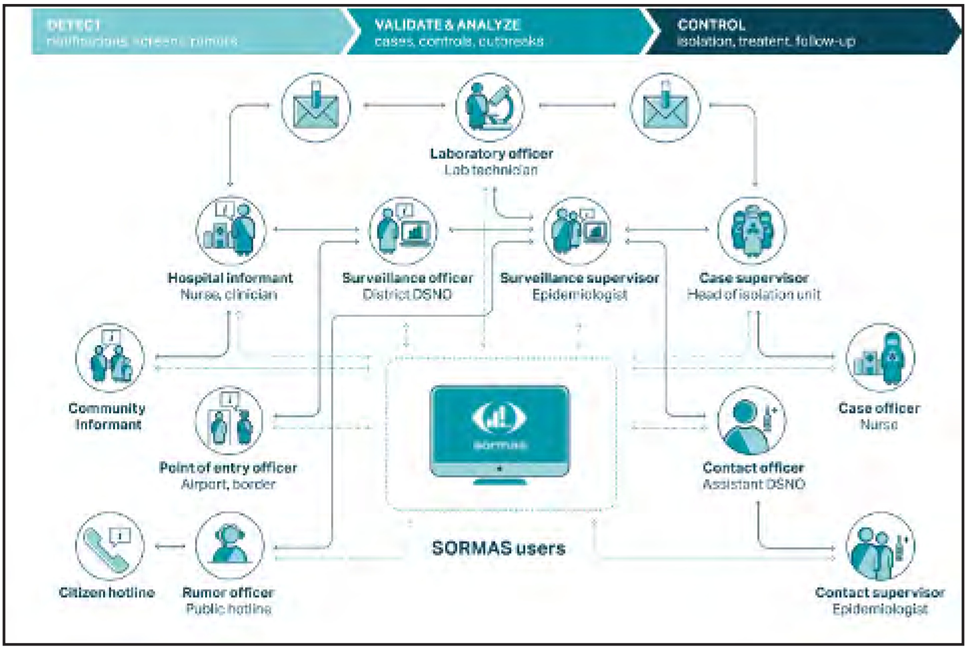


Figure 6-3. How SORMAS works

(Image by Exemplars)

Source: "SORMAS in Nigeria"

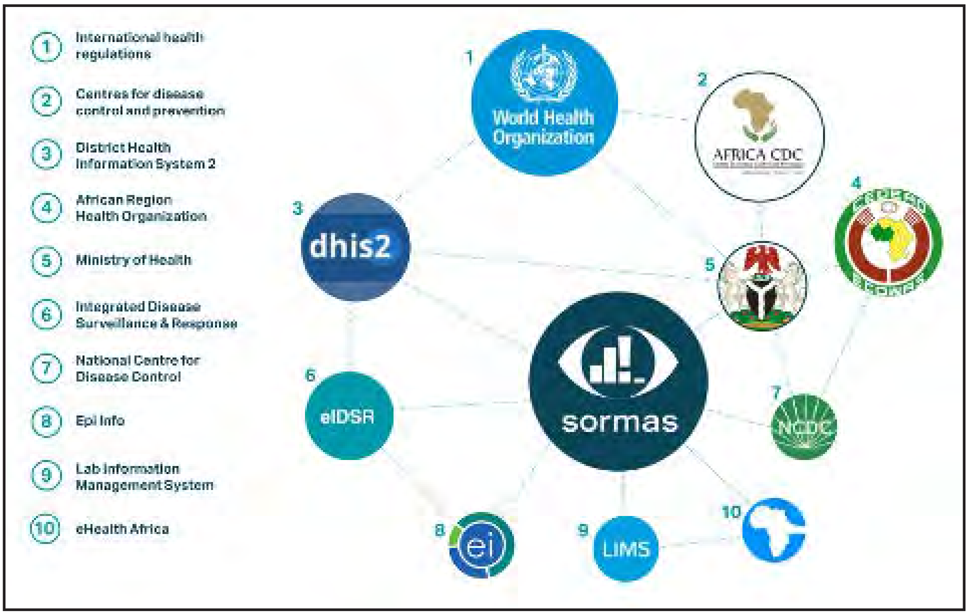

1 International health regulations
2 Centres for disease control and prevention
3 District Health Information System 2
4 African Region Health Organization
5 Ministry of Health
6 Integrated Disease Surveillance & Response
7 National Centre for Disease Control
8 Epi Info
9 Lab Information Management System
10 eHealth Africa
1
World Health Organization
2
AFRICA CDC
3
dhis2
4
ECOWAS
5
6
eIDSR
sormas
7
NCDC
8
ei
9
LIMS
10

Figure 6-4. Technical and organizational interoperability of SORMAS

(Image by Exemplars)

Source: "SORMAS in Nigeria"

The NCDC also provided daily easy-to-understand infographics on social media platforms (like Facebook and Twitter) showing the total number of cases confirmed, detected, and discharged as well as deaths.

Non-pharmacological Intervention (NPI)

Low-resourced health systems have perfected the leveraging of non-pharmacological interventions (NPI). Nigeria leveraged several NPIs such as handwashing, face-mask wearing, lockdowns, travel restrictions, restricted public gatherings, and school closures. Enforcement of these interventions required intense, effective, and socioculturally relevant communications.[21] Public education materials were prepared in different languages and disseminated via several channels (such as print, radio, social media, and television). The reference to languages is important. While English is the official language of Nigeria, there are at least 500 other languages spoken there, creating opportunities for regional influence in how the government, nonprofits, organized religion, and volunteers disseminate information.[22]

"Learn at Home," an educational intervention by the Mastercard Foundation, shows how influential information dissemination through the radio can be. This program delivered offline remote learning to one million children via radio and low-end mobile devices using unstructured supplementary service data (USSD) and short messaging service (SMS) through Data Science Nigeria.[23] Its goal was to ensure universal learning was compatible with the national education curriculum to mitigate the effects of being out of school and improve access to quality learning content for children who did not have access before the pandemic.

The culture of hand hygiene was also implemented. Most public places mandated handwashing, hand sanitization, face-mask wearing, and temperature checking before entry. Figure 6-6 shows a sample of how handwashing is communicated and implemented in the described context.

[21] Olumuyiwa O. Odusanya et al., "COVID-19: A Review of the Effectiveness of Non-pharmacological Interventions," *Nigerian Postgraduate Medical Journal* 27, no. 3 (October–December, 2020): 261.

[22] "Language Data for Nigeria," Translators without Borders (website), n.d., https://translatorswithoutborders.org/language-data-nigeria.

[23] "About Us," Learn at Home (website), https://learnathome.com.ng/; and "1 Million Disadvantaged School Children to Benefit from 'Learn at Home' Project by Data Science Nigeria/Malezi in Partnership with the Mastercard Foundation," Mastercard Foundation (website), n.d., https://mastercardfdn.org/1-million-disadvantaged-school-children-to-benefit-from-learn-at-home-project-by-data-science-nigeria-malezi-in-partnership-with-the-mastercard-foundation/.

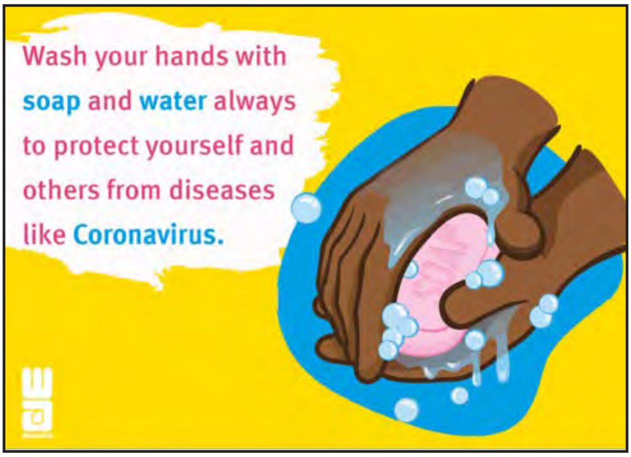


Figure 6-5. Poster by WaterAid encouraging handwashing
(Image by WaterAid)
Source: "Responding to Coronavirus," WaterAid, May 12, 2021, https://www.wateraid.org/us/wateraids-covid-19-response#Nigeria.

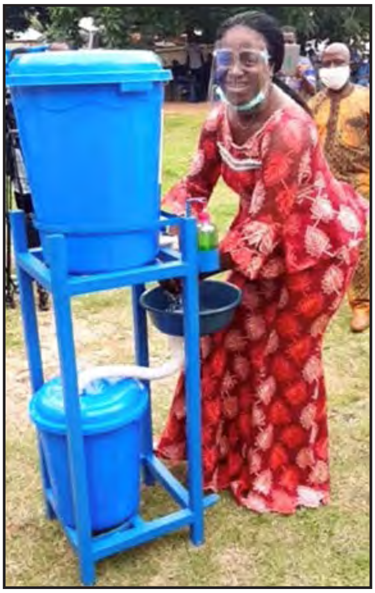


Figure 6-6. A makeshift handwashing station
Source: Peter Duru, "COVID-19: UNICEF Donates 5,000 WASH Kits, 100 Touchless Hand Washing Stations to Benue IDPs," Vanguard Media (website), https://www.vanguardngr.com/2020/07/COVID-19-unicef-donates-5000-wash-kits-100-touchless-hand-washing-stations-to-benue-idps/.

Conclusion

This chapter explored medical resilience, a core component of the NATO seven baseline resilience requirements for its member states. For the use case, the chapter explored pandemics as disruptors and what can be learned from their management in a low-resourced health system. The research showed how Nigeria effectively managed the COVID-19 pandemic despite the low-resourced health system and insecurity due to terrorism and banditry. To help readers understand the situation's complexity, COVID-19 and a conflict-connected framework, which defined three key pathways, were explored. The pathways include increasing armed group activities, intensifying youth grievances, and shifting patterns of social cohesion based on work by the Mercy Corps. Some of the key points of strength in how Nigeria managed the situation are leveraging experience and tools from previous outbreaks like Ebola (SORMAS) and the use of low-cost and non-pharmacological public health interventions (effective communications on precautions via radio and social media channels and multilingual printed materials).

When disruptions occur concurrently with insecurity, managing outcomes is complex, and the solutions are multidimensional. A key lesson for high-resourced systems within NATO is that much can be achieved even with resource constraints. If there is a call for support by these systems, it is also important to understand the local and historical context through collaboration with the resident military of the low-resourced system, as underscored in the case study on the fight against terrorism with groups like Boko Haram and bandits, where the home militaries had approaches that worked well and may only require reinforcement. NATO can also support local and national activities that strengthen trust in the government to keep citizens safe when disruptions (such as pandemics) occur concurrently with terrorist activities. These solutions include focusing on communications, logistics, and community health campaigns and providing contacts for local community questions. These whole-of-government approaches are building blocks to aiding medical resilience and strengthening the Alliance.

Select Bibliography

Adebisi, Yusuff Adebayo. "Political Instability in the Context of Health Security amid COVID-19 Pandemic." *Epidemiology International Journal* 5, no. 4 (December 2021). https://medwinpublishers.com/EIJ/political-instability-in-the-context-of-health-security-amid-covid-19-pandemic.pdf.

Attah, Noah Echa et al. "COVID 19 and Increased Security Challenges in Northern Nigeria: Interrogating Armed Banditry in Northwestern Nigeria." *SIASAT* 6, no. 1 (2021). https://www.siasatjournal.com/index.php/siasat/article/view/87.

Dan-Nwafor, Chioma et al. "Nigeria's Public Health Response to the COVID-19 Pandemic: January to May 2020." *Journal of Global Health* 10, no. 2 (2020). https://www.jogh.org/documents/issue202002/jogh-10-020399.pdf.

Madhav, Nita et al. "Pandemics: Risks, Impacts, and Mitigation." In *Disease Control Priorities: Improving Health and Reducing Poverty.* 3rd ed. Washington, DC: International Bank for Reconstruction and Development/World Bank, 2017. https://pubmed.ncbi.nlm.nih.gov/30212163/.

Ogunbameru, Adeteju et al. "Estimating Healthcare Resource Needs for COVID-19 Patients in Nigeria." *Pan African Medical Journal* 37, no. 293 (December 2, 2020). https://www.panafrican-med-journal.com/content/article/37/293/full/.

Oleribe, Obinna Ositadimma, Mary Margaret Elizabeth Crossey, and Simon David Taylor-Robinson. "Nigerian Response to the 2014 Ebola Viral Disease Outbreak: Lessons and Cautions." *Pan African Medical Journal* 22, no. S1 (October 2015). https://www.panafrican-med-journal.com/content/series/22/1/13/full/.

Oyeranti, Oluwaseun and Babajide Sokeye. "The Evolution and Spread of COVID-19 in Nigeria." Centre for Petroleum, Energy Economics and Law (website). 2020. https://cpeel.ui.edu.ng/publication/evolution-and-spread-covid-19-nigeria.

— 7 —

Military Health Surveillance Systems Supporting Resilience and Critical Infrastructure

Silke Ruhl and Máté Tóth

ABSTRACT: Military mission's health surveillance of soldiers is one key to enforce operational readiness. It can help provide the commander and medical personnel with adequate information about the epidemiological situation of the contingent and their options to intervene in a timely way in the case of an outbreak. Current surveillance systems are not providing the full range of needed tools to ensure this goal for the alliance, therefore additional near-real-time surveillance is needed. This chapter introduces case studies for surveillance systems, existing and in development, and provides an outlook into future surveillance abilities to support NATO and its partners, with an outline of the necessary developmental factors and requirements for a successful system.

Keywords: health surveillance systems, pandemics, EpiNATO2, Q fever, MILMED COE

Since 2019, the world has experienced the first real global pandemic of the century, disrupting nearly every aspect of life, including the world economy and overall military readiness. For military forces, health surveillance systems are an essential element in disease prevention and control as these forces are confronted with a continuum of operational scenarios, including war, peacekeeping, potential terrorist use of biological weapons, and natural disasters. Health surveillance, defined as the ongoing, systematic collection, analysis, interpretation, and dissemination of health events in the NATO Standardization Agreement (STANAG) 2535, delivers critical health status information about serving military personnel, which can assist in early the identification of new or emerging public health threats. The epidemiological data collected by surveillance systems are critically important for military leaders and planners to identify trends in the overall medical situation and treatment requirements, and they are an important facet to consider when planning for future operations. Altogether, the data and findings of such a system provide a basis for immediate action and can help NATO prepare appropriate response measures in the future.

The effect of transmissible diseases and possible biological attacks and the importance of preparing for them cannot be overstated as they can have a massive impact on mission readiness and the potential to weaken troop strength and pose a risk to the civilian population. This chapter provides a case study of how existing and newly developed health surveillance systems are critical in mitigating the effects of such emerging threats. It compares how a well-established medical system for civilian and military use can provide proactive solutions and be deployed in more austere conditions.

The Allied Joint Doctrine for Medical Support outlines the personnel and national security importance of such systems: "Deployment health surveillance aims to provide a key indication of the forces heath status and an estimate of its impact on manpower and working day losses. Surveillance and reporting may also identify chemical, biological, radiological, or nuclear (CBRN) weapons involvement. Deployment of health surveillance is intended to serve as a warning system to trigger further investigation and implement preventive countermeasures or other command actions needed to reduce the adverse impacts of health threats. A comprehensive disease and non-battle injury analysis can produce more effective preventive medicine measures, including recommended policy on immunization, prophylaxis, and personal health education. It can also be a driving factor in the size and capability of medical resources required in different scenarios."[1]

EpiNATO2:
NATO's Only Health Surveillance System

In 2002, one year after the September 11 attacks in the United States, North Atlantic Treaty Organization's (NATO's) heads of state and government endorsed five initiatives to enhance the capacity of the Alliance for deterrence and defense against nuclear, biological and chemical (NBC) weapons:

[1] NATO, *Allied Joint Doctrine for Medical Support*, Allied Joint Publication (AJP)-4.10, ed. C, ver. 1 (Brussels: NATO Standardization Office, September 2019), https://www.coemed.org/files/stanags/01_AJP/AJP-4.10_EDC_V1_E_2228.pdf.

"a Prototype Deployable NBC Analytical Laboratory; a Prototype NBC Event Response team; a virtual Centre of Excellence for NBC Weapons Defence; a NATO Biological and Chemical Defence Stockpile; and a Disease Surveillance system."[2]

Currently, deployed NATO forces use a NATO surveillance tool called EpiNATO2, where every NATO Medical Treatment Facility (MTF) reports cases of predefined events such as "gastro-intestinal illnesses" to the Force Health Protection Branch (FHPB) in Munich, Germany, on a weekly basis. EpiNATO2 is the current and only interoperable military health surveillance system defined in the NATO doctrine.[3] In 2013, it was first implemented in the Kosovo Force and European Union Training Mission Mali.

EpiNATO-2 is mandated for use during all NATO operations. Its coverage has increased over time and now includes all NATO Joint and Component Command Operations and several non-NATO operations.[4] The feedback provided by the FHPB for every mission is needed to enhance situational awareness about evolving trends in health issues across the deployed force in a multinational theater and is intended to provide information for action and medical decision making and force health protection assurance at the local and theater levels. Additionally, most nations use a national disease surveillance system working with ICD-10 codes from primary care once a week.

Case Study: Military Public Health Surveillance Systems Exemplified by a Q Fever Outbreak in Kosovo

During recent military interventions, 65 to 80 percent of hospitalizations of soldiers were due to infectious diseases.[5] Military forces are expected to maintain maximum operational readiness before, during, and after the mission. Therefore, a reliable health surveillance system is needed

[2] "Prague Summit Declaration Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Prague, Czech Republic," NATO (website), November 21,2002, https://www.nato.int/cps/en/natohq/official_texts_19552.htm.

[3] NATO, *Allied Joint Doctrine for Medical Support*.

[4] Jean L. Wilson, Maureen T. Carew, and Barbara A. Strauss, "Canadian Forces Evaluation of the EPINATO Health Surveillance System in Bosnia-Herzegovina," *Military Medicine* 171, no. 10 (2006): 955–61, https://academic.oup.com/milmed/article/171/10/955/4577942; and Hagen Frickmann et al., "Infectious Diseases during the European Union Training Mission Mali (EUTM MLI) – A Four-year Experience," *Military Medical Research* 5, no. 19 (2018), https://doi.org/10.1186/s40779-018-0166-5.

[5] Matthew Smallman-Raynor and Andrew Cliff, *War Epidemics: A Historical Geography of Infectious Diseases in Military Conflict and Civil Strife, 1850–2000* (New York: Oxford University Press, 2004).

to provide commanders and medical personnel with adequate information about the epidemiological situation of the contingent and options to intervene in a timely way in case of an outbreak.

In March 2016, a cluster of confirmed influenza A and B virus cases was diagnosed at the German KFOR-Field Hospital in Priene, Kosovo. In April, soldiers could still be seen with the same clinical signs without confirmation of influenza. Most of the cases expressed a radiologically confirmed atypical pneumonia. Because of the nature of the diseases and the known endemicity of its pathogen (*Coxiella burnetii*) in the Balkan region, the suspected diagnosis of Q fever was mentioned. On-site, no diagnostic test was available for the confirmation of this differential diagnosis. Therefore, to investigate the outbreak, a Rapidly Deployable Outbreak Investigation Team (RDOIT) was sent to the camp in the 15th calendar week.

Q fever is an important but underestimated public health problem in the Balkan region, due to inadequate surveillance. Outbreaks within KFOR have been described regularly since the beginning of the mission.[6] Due to the nature of the work of military personnel who must patrol farmland, train on grounds that are grazed upon by sheep, or breathe in air from such fields during helicopter loading and unloading, they are generally deemed to be at a high risk of contracting vector-borne and zoonotic infections.[7] This is exacerbated by a lack of expertise in the differential diagnosis of such zoonotic or tropical diseases, which leads to reduced sensitivity and specificity within the diagnostic process. Therefore, the latter should be supported by a robust and reliable health surveillance system. *Coxiella burnetti* infections often go undiagnosed because of their nonspecific symptoms or lack of adequate diagnostic capabilities.[8] Q fever can lead to severe chronic disease (such as endocarditis and fatigue syndrome) if not treated properly in the early stage of the infection, ending a military career and severely

[6] Alicia Anderson et al.,"Q Fever and the US Military," *Emerging Infectious Diseases* 11, no. 8 (August 2005), https://wwwnc.cdc.gov/eid/article/11/8/05-0314_article.

[7] Wiebke Hellenbran, Thomas Breuer, and Lyle Petersen, "Changing Epidemiology of Q Fever in Germany, 1947–1999," *Emerging Infectious Diseases* 7, no. 5 (October 2001): 789–96, https://wwwnc.cdc.gov/eid/article/7/5/01-0504_article; and Edmund N. C. Newman et al., "Seroconversion for Infectious Pathogens among UK Military Personnel Deployed to Afghanistan, 2008–2011," *Emerging Infectious Diseases* 20, no. 12 (December 2014), https://wwwnc.cdc.gov/eid/article/20/12/13-1830_article.

[8] R. Eibach et al., "Q Fever: Baseline Monitoring of a Sheep and a Goat Flock Associated with Human Infections," *Epidemiology & Infection* 140, no. 11 (January 5, 2012), https://www.cambridge.org/core/journals/epidemiology-and-infection/article/q-fever-baseline-monitoring-of-a-sheep-and a-goat-flock-associated-with-human-infections/4762E4A96F54D145AF45DD21C5375562; and Dennis Faix et al., "Outbreak of Q Fever among US Military in Western Iraq, June–July 2005," *Clinical Infectious Diseases* 47, no. 7 (April 1, 2008), https://academic.oup.com/cid/article/46/7/e65/293077.

impeding the quality of life of the patient.[9] A robust microbiological diagnostic capability and effective surveillance is needed to detect cases as fast as possible to protect an individual's health, maintain military readiness, and raise awareness for the presence of the disease.[10]

One of the main objectives of military health surveillance systems is the early detection of outbreaks to limit their impact on operational capacity through appropriate interventions. These systems can differ from civilian systems.[11] Military peculiarities like variable geographic location of missions, high mobility of forces, difficult working and living conditions in the field, multinational target populations, regular turnover of the population in short intervals, heightened levels of security, or lack of historical surveillance data for the target population must be integrated into the creation.

In this case study, the current surveillance systems, EpiNATO-2, and a national system were critically reviewed based on numbers and information collected during the Q fever outbreak in 2016 and improvement actions were defined.

Descriptive Analysis of the Q Fever Data

The two systems worked both technically as well as procedurally but showed misclassifications and could not detect the previously mentioned cases early in the outbreak. Even though the Q fever outbreak could be clearly detected in both systems with a high unique peak in addition to the typical temporal window for seasonal influenza or upper respiratory tract diseases (figure 7-1), there are differences. A likely reason for the almost double incidence in the national system compared to EpiNATO2 is the raised awareness among medical personnel and the presence of the RDOIT team.

[9] Florence Fenollar et al., "Risks Factors and Prevention of Q Fever Endocarditis," *Clinical Infectious Disease* 33, no. 3 (August 1, 2001), https://academic.oup.com/cid/article/33/3/312/277191.

[10] Shannon Ellis et al., "Outbreak of Sandfly Fever in Central Iraq, September 2007," *Military Medicine* 173, no. 10 (October 2008): 949–53, https://academic.oup.com/milmed/article/173/10/949/4283061.

[11] Jean-Baptiste Meynard et al., "Proposal of a Framework for Evaluating Military Surveillance Systems for Early Detection of Outbreaks on Duty Areas," *BMC Public Health* 8, no. 146 (2008), https://bmcpublichealth.biomedcentral.com/articles/10.1186/1471-2458-8-146.

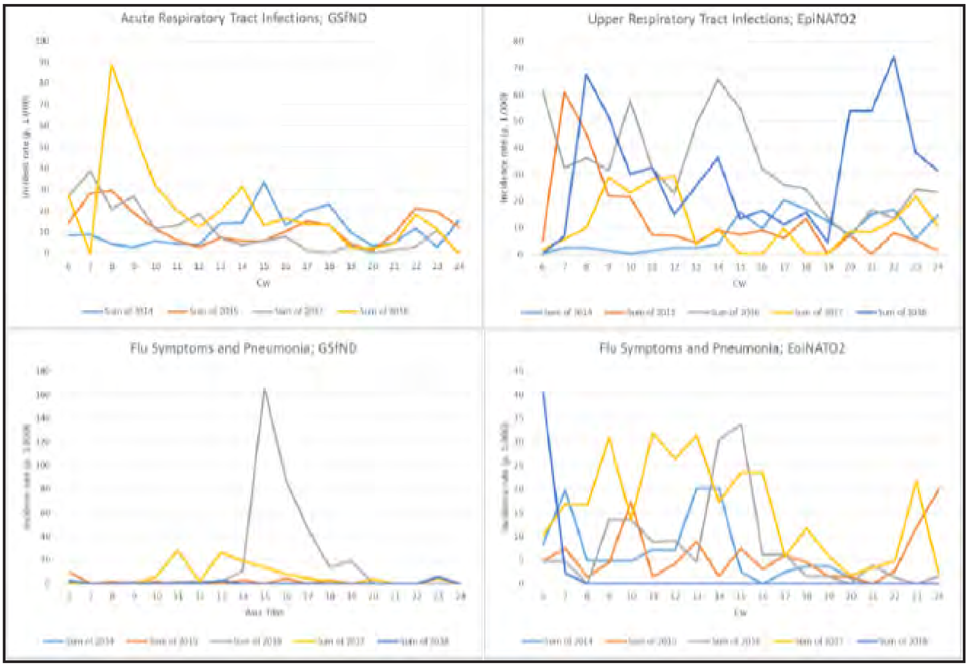


Figure 7-1. Notified respiratory tract infections due to ICD-10 code and EpiNATO-2

Source: NATO Standardization Office (NSO), "Deployment Health Surveillance," Edition A Version 2, January 2017, https://www.coemed.org/files/stanags/03_AMEDP/AMedP-4.1_EDA_V2_E_2535.pdf.

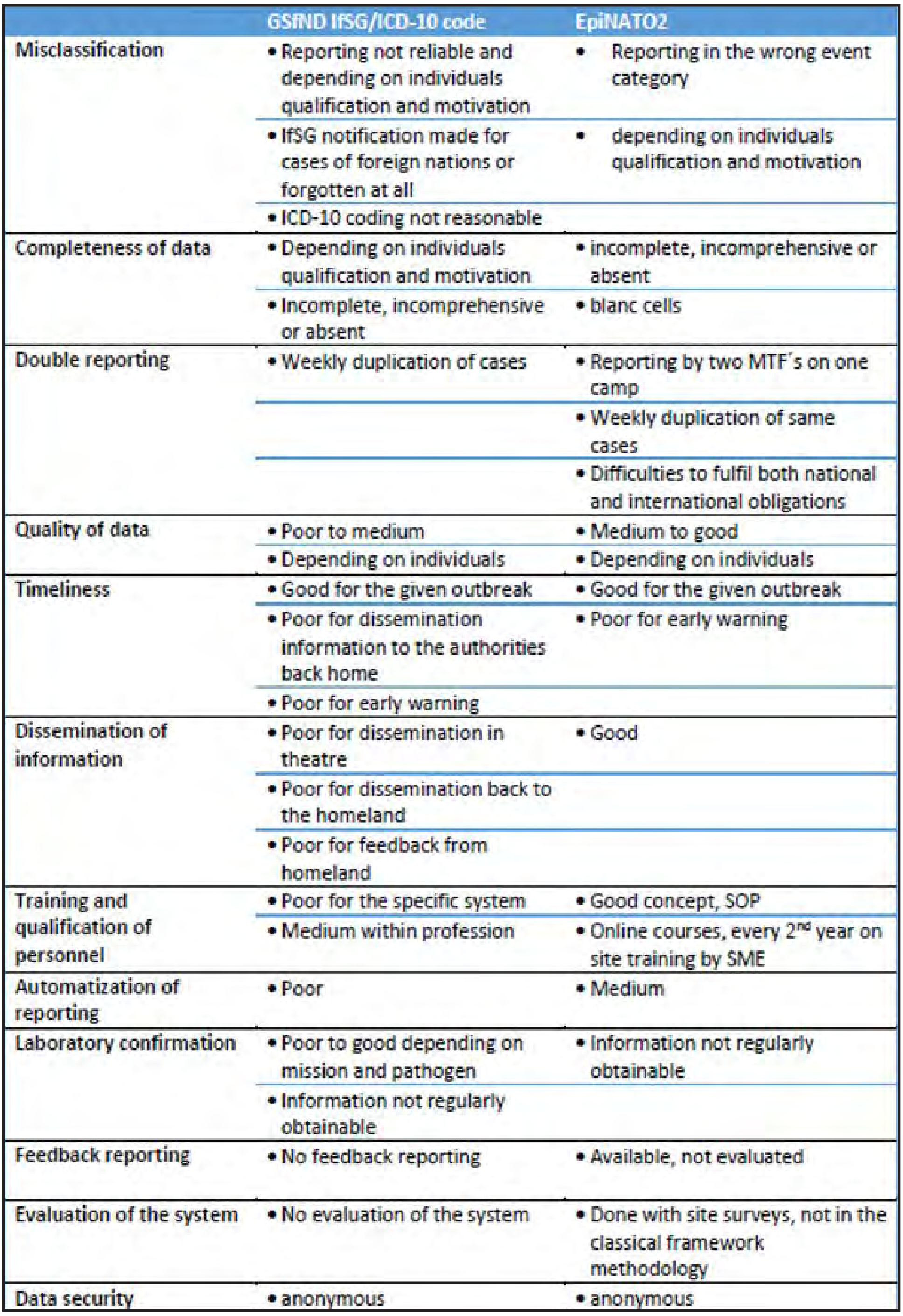
The partial overlap of influenza and Q fever cases in 2016 is likely responsible for the latter's initial misinterpretation as influenza cases (see table 7-1). Only the unusual decision for lung X-rays showing a high number of atypical pneumonia cases led to the potential differential diagnosis of Q fever, which was eventually confirmed through serum samples by the reach-back laboratory.

This confirmation resulted in a high-quality but delayed final diagnosis, which was not useful for early-warning purposes. Such a delay has the potential of missing an outbreak.[12] The differences between the national system and EpiNATO2 in picking up the first influenza peak in figures 7-1 and 7-2 suggest the EpiNATO2 could be more sensitive than the national system.

[12] Colleen Lau "Combating Infectious Diseases in the Pacific Islands: Sentinel Surveillance, Environmental Health, and Geospatial Tools," *Reviews on Environmental Health* 29, no. 1–2 (February 24, 2014), https://www.degruyter.com/document/doi/10.1515/reveh-2014-0028/html.

Table 7-1. Limitations of the current surveillance systems obtained from screening Q fever data

Source: "Deployment Health Surveillance."



	GSfND IfSG/ICD-10 code	EpiNATO2
Misclassification	• Reporting not reliable and depending on individuals qualification and motivation	• Reporting in the wrong event category
	• IfSG notification made for cases of foreign nations or forgotten at all	• depending on individuals qualification and motivation
	• ICD-10 coding not reasonable	
Completeness of data	• Depending on individuals qualification and motivation	• incomplete, incomprehensive or absent
	• Incomplete, incomprehensive or absent	• blanc cells
Double reporting	• Weekly duplication of cases	• Reporting by two MTF´s on one camp
		• Weekly duplication of same cases
		• Difficulties to fulfil both national and international obligations
Quality of data	• Poor to medium	• Medium to good
	• Depending on individuals	• Depending on individuals
Timeliness	• Good for the given outbreak	• Good for the given outbreak
	• Poor for dissemination information to the authorities back home	• Poor for early warning
	• Poor for early warning	
Dissemination of information	• Poor for dissemination in theatre	• Good
	• Poor for dissemination back to the homeland	
	• Poor for feedback from homeland	
Training and qualification of personnel	• Poor for the specific system	• Good concept, SOP
	• Medium within profession	• Online courses, every 2nd year on site training by SME
Automatization of reporting	• Poor	• Medium
Laboratory confirmation	• Poor to good depending on mission and pathogen	• Information not regularly obtainable
	• Information not regularly obtainable	
Feedback reporting	• No feedback reporting	• Available, not evaluated
Evaluation of the system	• No evaluation of the system	• Done with site surveys, not in the classical framework methodology
Data security	• anonymous	• anonymous

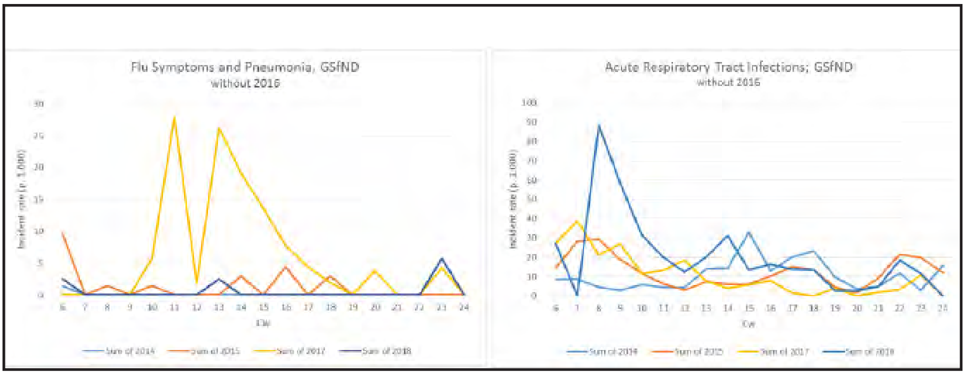


Figure 7-2. Notified respiratory tract infections due to the national system without 2016 data

Source: "Deployment Health Surveillance."

Qualitative Analysis of the Current Military Surveillance Systems – Lessons Identified

In both systems, misclassification due to lack of training or qualification and completeness of data were the main problem areas. Overall, the EpiNATO2 systems show fewer limitations than the national system. Most highlighted issues were difficulties in classification of patients' presentation, absence of a feedback report to motivate data-entering personnel, and the inadequate automation of the national system.

For the national system, one likely reason is the lack of analysis and feedback of the reported data at the evaluation unit in the homeland due to staffing shortages, leading to severe problems with data quality.[13] The major problems of all health surveillance systems are related to human factors, including lack of qualification, training, motivation, and supervision.[14] This problem was especially notable in the national system—data quality depends on the actions of the hygiene inspector in the mission and

[13] K. Wilkins et al., "The Data for Decision Making Project: Assessment of Surveillance Systems in Developing Countries to Improve Access to Public Health Information," *Public Health* 122, no. 9 (September 2008): 914–22, https://www.sciencedirect.com/science/article/abs/pii/S0033350607003563?via%3Dihub; and Weiyi Xiong, Jun Lv, and Liming Li, "A Survey of Core and Support Activities of Communicable Disease Surveillance Systems at Operating-level CDCs in China," *BMC Public Health* 10, no. 704 (November 17, 2010), https://bmcpublichealth.biomedcentral.com/articles/10.1186/1471-2458-10-704.

[14] Henry Jefferson et al., "Evaluation of a Syndromic Surveillance for the Early Detection of Outbreaks among Military Personnel in a Tropical Country," *Journal of Public Health* 30, no. 4 (December 2008): 375–83, https://academic.oup.com/jpubhealth/article/30/4/375/1508419.

his enthusiasm to go to visit the MTF physically and ask weekly for the necessary information.

Second, the same information must be sent to two different databases, using two different spreadsheets and dissemination routes for the national system and EpiNATO2, doubling the workload. Thus, personal motivation becomes crucial to the quality of the reported data. A possible solution is to use automated routine reporting and a single dissemination chain.[15]

Alternatively, both systems could be linked with primary-care patient documentation mandated by law. Both the national system (disease-specific) and EpiNATO2 (event-based surveillance) could generate data automatically from the entered data and distribute it to the different SMEs for analysis and feedback, benefiting the personnel workload and the data quality of the systems.[16] Both systems were designed to assess the public health burden of diseases and injuries but not for early detection of outbreaks as they use only weekly reporting and rely on the reporting of clinical diagnoses with the associated temporal lag. To close the capability gap to detect an outbreak in a timely manner, a syndromic surveillance should be designed that can also be fed from the same real-time (or at least daily) data source in primary care.

Another challenge for both systems is reliable coding. The observed misclassifications can limit the early detection of an outbreak, overlap the severity of a disease, and indirectly affect military operations. The most important way to reduce misclassification is the willingness and qualification of users to participate in the system. Lack thereof leads to poor data quality. Acceptance is also increased by feedback where the users see a result of their efforts.

Both systems work without laboratory confirmation. Laboratory results are needed to decrease the percentage of misdiagnosing and incorrect management.[17] Therefore, results should be automatically fed into the

[15] Badraih Alotaibi et al., "Strengthening Health Security at the Hajj Mass Gatherings: Characteristics of the Infectious Diseases Surveillance Systems Operational during the 2015 Hajj," *Journal of Travel Medicine* 24, no. 3 (May–June, 2017), https://academic.oup.com/jtm/article/24/3/taw087/305346; and James W. Buehler et al., "Framework for Evaluating Public Health Surveillance Systems for Early Detection of Outbreaks: Recommendations from the CDC Working Group," Morbidity and Mortality Weekly Report, Recommendations and Reports, May 7, 2004.

[16] Cédric Abat et al., "Traditional and Syndromic Surveillance of Infectious Diseases and Pathogens," *International Journal of Infectious Diseases* 48 (July 2016): 22–28, https://www.sciencedirect.com/science/article/pii/S1201971216310384?via%3Dihub.

[17] Lau, "Infectious Diseases in the Pacific Islands."

surveillance system to support the analysis.[18] Routine laboratory service has a temporal lag of one to two weeks—often due to the necessity of sending specimens to a reach-back laboratory, which is not useful for a timely response.[19] In the context of an outbreak, appropriate laboratory capabilities according to endemic agents on-site are necessary to provide timely laboratory support and combine the strengths of syndromic and specific surveillance. [20]

Analysis

Due to their design, both surveillance systems analyzed here cannot operate as a near-real-time surveillance system. To improve user compliance, the two systems should be integrated into the primary health care medical recording, where the needed data could be automatically captured and transferred for epidemiological analysis and feedback. As seen above, NATO can complement national situational awareness through surveillance, intelligence-sharing, and risk assessments vital for NATO biodefense.[21]

Robust disease surveillance is a key factor for the early detection of an outbreak, regardless of whether deliberated or naturally occurring. During the COVID-19 pandemic, the lack of an early-warning system for early infectious disease outbreak detection was again visible and addressed by different national bodies and experts. Since the above-mentioned meeting of NATO in 2002, armed forces have begun to develop syndromic surveillance systems on a national level, with their own objectives and procedures. They all have been tailored to the main objectives of early detection of potential epidemics, evaluation of their potential impact on operational capacity, and the provision of information to facilitate the medical response for the representative nation. Many studies showed the value of syndromic surveillance within the military.[22] A mandated NATO solution for a near-real-time surveillance tool that will

[18] Andres G. Lescano et al., "Statistical Analyses in Disease Surveillance Systems," *BMC Proceedings* 2, no. 7 (November 14, 2008), https://link.springer.com/article/10.1186/1753-6561-2-s3-s7.

[19] Axel A. Bonačić Marinović et al., "Speed Versus Coverage Trade Off in Targeted Interventions during an Outbreak," *Epidemics* 8 (September 2014): 28–40, https://www.sciencedirect.com/science/article/pii/S1755436514000358?via%3Dihub.

[20] S. Arunmozhi Balajee, Ray Arthur, and Anthony W. Mounts, "Global Health Security: Building Capacities for Early Event Detection, Epidemiologic Workforce, and Laboratory Response," *Health Security* 14, no. 6 (December 1, 2016), https://www.liebertpub.com/doi/10.1089/hs.2015.0062.

[21] "New RD Publications – COVID-19: NATO in the Age of Pandemics," NATO (website), May 25. 2020, https://www.ndc.nato.int/news/news.php?icode=1440.

[22] Jean-Baptiste Meynard et al., "Value of Syndromic Surveillance within the Armed Forces for Early Warning during a Dengue Fever Outbreak in French Guiana in 2006," *BMC Medical Informatics and Decision Making* 8, no. 29 (July 2, 2008), https://bmcmedinformdecismak.biomedcentral.com/articles/10.1186/1472-6947-8-29.

cover the whole theatre, including the reporting from all deployed nations, is not available at the present time.

Therefore, the NATO Centre of Excellence for Military Medicine (NATO MILMED COE) started the development of a fully automated, early-warning system that may help prevent the mentioned lessons identified, including misclassifications, doubling of workload, and especially delivering up-to-date health status information to the commander in mission, as described in the next section.

Table 7-2. Main characteristics of the two systems used for public health surveillance in case study

(Original by author)

Surveillance Characteristics	GSfND	EpiNATO-2
Nationality	National	Multinational
Year implemented	2006	2013
Activation period	Permanent	Permanent
Periodicity of surveillance	Weekly	Weekly
Geographic scope	National Armed Forces mission	NATO, EU, single nations
Participating units	All national MTFs in missions	Specified NATO nations MTFs, depending on national contribution
Population monitored	Active-duty national military personnel in mission	Deployed NATO/EU forces
Recorded data for patients	ICD10 code, weekly FHP reports	14 specific disease and injuries events and 4 nonspecific disease and injuries events
Syndrome for recorded data	Acute respiratory tract infection, flu symptoms and pneumonia, other respiratory tract infection	Upper respiratory tract infection, influenza-like illness, and lower respiratory tract infection
Person responsible for data input	Military general practitioner or nurses	Military general practitioner or nurse
Support for input	PC – Word and Excel	PC – Excel
Person responsible for data collecting and sending to experts	National hygiene inspector	CJMed, PREVMed
Data transmission	National intranet (secured network)	Internet unclassified
Automatization of data analysis	Not automated	Automated

Surveillance Characteristics	GSfND	EpiNATO-2
Methods of data analysis	No data analysis	Crude rates and statistical process control, u-Chart, EWMA, funnel plot
Syntheses for commander	No indicators	Narrative in feedback
Feedback for actors	No feedback	Weekly
Dissemination to user	No dissemination	To CJMed, LSO, MTFs
Evaluation program	No evaluation	Regular side surveys to conduct audit and evaluation during deployment

Near-Real-Time Surveillance Project of the NATO MILMED COE

Timely detection and countermeasures are critical in mitigating the effects of natural outbreaks and biological attacks. Due to the exponential nature of the diseases causing major outbreaks, countermeasures introduced early can fundamentally change the impact on society as a whole and, more specifically, our military and medical support systems. Furthermore, such a system may provide data to inform force health protection and overall disease control and a quantified database on the health of the surveyed population that can help planning, stockpiling of resources, and evidence-based decision-making and reforms.

Brief Overview of Real-time Surveillance Efforts in NATO

The idea to establish a NATO-wide disease surveillance system has been a declared goal of the Alliance for the last 20 years. As referenced in the previous section, at the 2002 Prague NATO Summit of Heads of State and Government, decisive capability gaps in NATO's abilities to react to asymmetric threats were identified. Among these capability gaps was the lack of an early-warning disease surveillance system to detect naturally occurring or deliberately caused outbreaks of infectious disease.

By 2005, several national medical surveillance capabilities had been identified and tested concerning their ability to serve NATO's requirements. Finally, two syndromic surveillance systems were identified, which could possibly close the early-warning gap: the British (GBR) Portable Remote Illness and Symptoms Monitor (PRISM) system and the French (FRA) system *Alert et Surveillance en temps Reel* (ASTER). After multiple international testing phases and a live deployment to KFOR, the concept was solid enough to be implemented in the form of an institution, and so, NATO's highest medical decision-making body, the Committee of the Chiefs of Medical Services in NATO (COMEDS), supported the establishment of a deployment health surveillance capability (DHSC) for NATO in Munich, which came to realization in 2010.

Since then, there have been several high-level initiatives to create an all-encompassing logistical and medical information system, which has manifested in the medical communications and information systems (MEDCIS) development initiative, and later in the NATO Enablement Support Services (ESS) Medical Suite (MEDSUITE) development. The latter is currently in development, with the disease surveillance function being one of the planned modules for deployment in 2026 at the earliest.

In 2011, to integrate the DHSC into NATO better and to utilize an obvious synergy between these organizations, the DHSC was integrated into the NATO MILMED COE as a satellite branch. For the next 11 years, the DHSC branch deployed and tested the ASTER system and provided force protection advice to nations, and finally expanded into being a provider of a broader, force health protection function.[23]

This role change, which has been reflected in the branch taking up the name "Force Health Protection Branch" (FHPB), and the regular activities of the branch with such systems, ensured that they had the broadest possible experience in the field of disease surveillance and its importance in NATO. This need was further reinforced by the fact that the branch has taken custodianship of the NATO Standardization Agreement "Deployment Health Surveillance," which is a template and set of requirements for an effective disease surveillance system in NATO.[24] This seemingly simple administrative role and its overall background positioned the branch ideally to take up the long-dormant initiative of a near-real-time medical surveillance system for NATO.

Since neither the PRISM nor the ASTER system has proven to be a perfect and stable solution for this issue, mainly due to national

[23] Hans-Ulrich Holtherm, "Development of a Multinational Deployment Health Surveillance Capability (DHSC) for NATO," Worldwide Military-Medicine (website), January 31, 2019, https://military-medicine.com/article/3650-development-of-a-multinational-deployment-health-surveillance-capability-dhsc-for-nato.html.

[24] NATO, *Deployment Health Surveillance*, Allied Medical Publication (AMP)-4.1, ed. A, ver. 2 (Brussels: NATO Standardization Office, January 2017), https://coemed.org/files/stanags/03_AMEDP/AMedP-4.1_EDA_V2_E_2535.pdf.

restrictions and having no control over the development of these tools, the FHPB, with the support of subject matter experts (SMEs) of the NATO MILMED COE, has decided to develop a prototype system based on a widely available software development environment: Microsoft Office 365 Apps and Azure Cloud.

Development of a Working Near-real-time Surveillance Tool

In 2019, the NATO MILMED COE successfully migrated its information systems to the cloud. This step opened previously unavailable options for system and process integration and short development cycles for new capabilities and has been especially useful during the lockdown and remote-work periods that came in early 2020, as the COE could transition to remote-work immediately. The measures against the pandemic also meant a great number of COE courses, events, and other planned activities were canceled or postponed, resulting in a higher availability of funds for experimental projects and a more available staff to work on such an initiative. Moreover, the FHP Branch has been very active with organizing an important forum for the military-medical staff involved in the fight against COVID-19. These forums have been reinforced with additional SMEs joining the ranks and seconded experts from within the MILMED COE, which include an epidemiologist and an information management expert with experience in designing field data collection systems. The first concept to be proven was technical viability, while keeping the development platform in-house. The tool had to meet multiple key requirements to be considered a success:

1. Modular setup. The three distinct modules (see description of system below) can function without each other and allow external partners to choose which functions they use from the COE's tool and which ones they solve on their own. Practically, this means that a nation can decide only to use the analysis tool or only to send data to the database, but not use the COE's data-entry solution. Data entry must not require any preexisting medical training, and it must focus on symptoms that can be collected during a simple primary-care visit.

2. Interoperability and compatibility. The tool must run on the widest possible spectrum of hardware devices and operating systems. It must be able to receive and display data from other medical databases as background or for common analysis.

3. Scalability. The tool must be able to work with a virtually unlimited number of medical treatment facilities.

4. Security. While the current system runs on open Internet, it has to offer encrypted communication through the entire process and be portable to secure networks.

5. Easily modifiable/short development cycles. The tool should be built in a way that it is easily modifiable, as it will always be under development, and it will probably be tailored for specific missions to enhance precision.

6. Eases the work of the SMEs. The tool should provide clear and well-established quantitative analysis with visual aides to ease the work of the epidemiologists and provide tailored feedback to MTFs and other users.

The system can be divided into three distinct parts:

1. Data entry module/API. Data can be submitted via MILMED COE's custom-made application running on Android, IOS, Mac, or Windows and in practically any modern browser or directly to the database from national systems or databases via API calls, automated e-mails or specific workflows. Customized, remotely managed tablets are being tested live in the Bundeswehr's Military Hospital in Munich.

2. Database. The main, live fact tables are stored in SharePoint lists until archived. The support data, such as a list and location of treatment facilities, population figures, and camp locations are stored in separate lists with easy maintainability by the administrative staff. The database can be shared easily if required.

3. Data analysis, visualization, and alert module. The data is fed to a PowerBI report and dashboard, which analyses and visualizes the specific symptom groups as determined by the underlying algorithms. The system fetches data every working hour automatically but can be updated at any moment manually. A larger frequency of automated updates is possible, and it can generate e-mail–based alerts for special parameters and thresholds.

The first version of the tool was completed within three months between September and November 2020 and was demonstrated live at the COMEDS Plenary in December, where the nations noted its development and lauded the NATO MILMED COE's proactive stance on the issue. The limited goals of the prototype were also stated as the following:

1. Proof of concept. Such a tool can be developed easily with modern software solutions, and the end product's capabilities and versatility far outpace previous attempts.

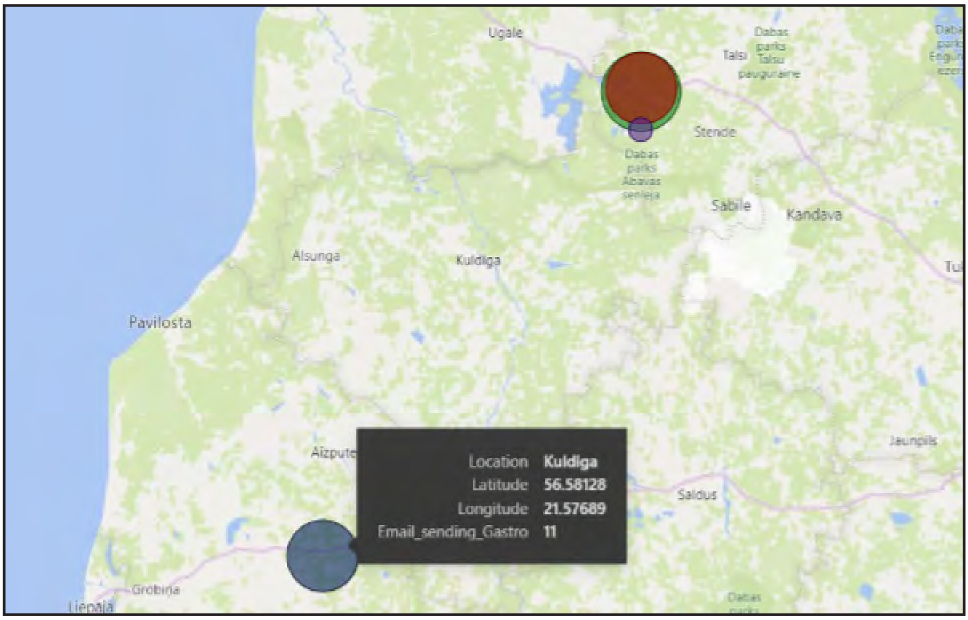
2. Possibility to test syndromic algorithms. The most important intellectual property in such a tool is the precision of the algorithms and the know-how of data collection with standardized symptom lists, thresholds, and diagnoses that one can program for the tool to provide a precise analysis. These algorithms have to be tested by dummy and live data determine their precision.

3. Capturing data. The tool, even in a work-in-progress version, has to collect as much live data as possible. Currently, a great portion of syndromic data is not recorded properly in missions, which leaves important benchmark data unrecorded.

The Committee of Chiefs of Military Medical Services in NATO was also informed that the tool would participate in the Coalition Warrior Interoperability Exercise, CWIX 2021, where it would interface with other national and NATO-wide systems to provide further proof of its viability. The member states noted the tool's development and lauded the NATO MILMED COE's proactive stance. Some expressed a deeper interest in the project. During the months after, the COE's SMEs introduced the tool to several COMEDS working groups and at Allied Command Transformation (ACT) events. They started to build the scientific community behind the tool to develop the algorithms and syndromes for it, while at the same time initiating changes and improvements to the tool's modules. These developments were put to the test at the CWIX'21, where a biological threat caused by an attack on critical infrastructure was simulated. The next subsection analyzes how the tool performed during the exercise and informed further development.

Case Study: NATO MILMED COE Near-real-time Surveillance Tool in Practice

The real-time surveillance tool produced a simulated attack on critical infrastructure resulting in biological threats. The CWIX in 2021 was mainly a virtual event, due to the pandemic, but this did not hamper the deployment of the NRTS tool. The MILMED COE team established connections to the national and NATO systems being tested and performed a comprehensive mapping of how NATO's and the participating nations' systems communicate and what message standards are being applied. The team also created translation/mapping tables that transformed the incoming data to the NATO format. The scenario included a cyberattack on a water treatment plant that supplied multiple units on the field with potable water. The units were colocated and organized in the same higher unit but had their own ROLE-1 level treatment facilities (basic primary care) reporting in, so we could also monitor and process data coming from different sources at about the same location (see figure 7-3).

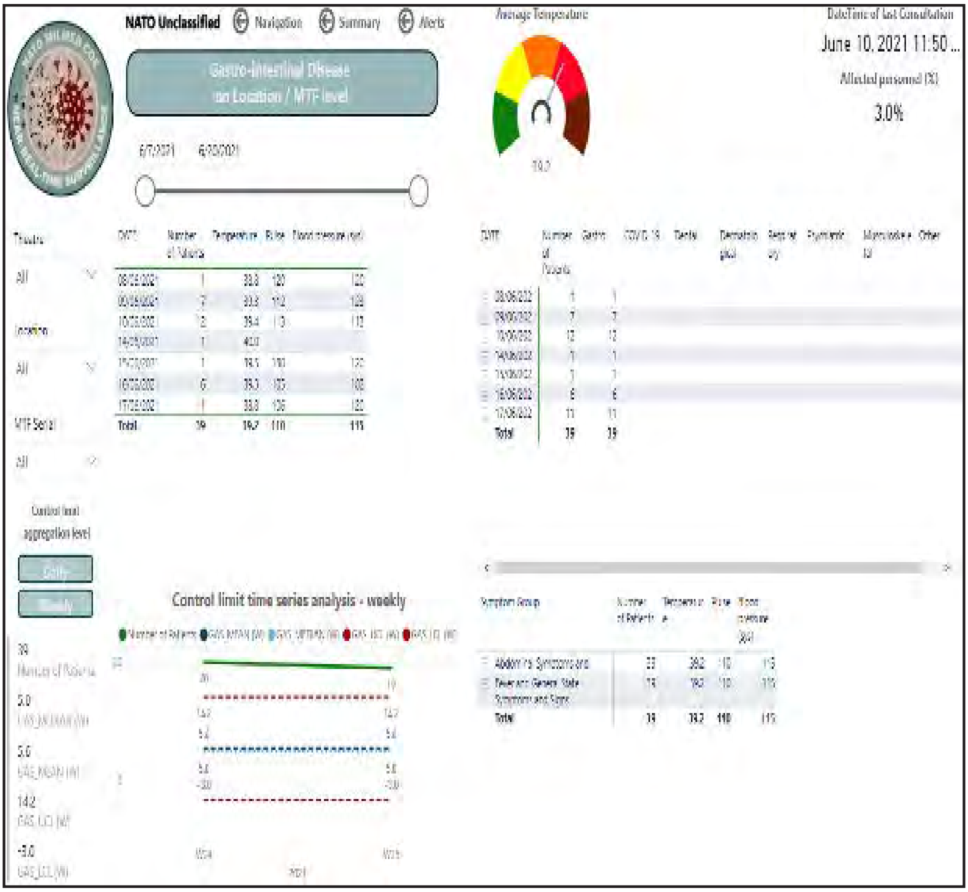


Location Kuldiga
Latitude 56.58128
Longitude 21.57689
Email_sending_Gastro 11

Figure 7-3. The quick map reference of cases. The overlapping circles show multiple units reporting from the same camp, and the size of the circle refers to the number of cases

(Original by author)

In the meantime, the team monitored the messages in JCHAT, the text-based chat in NATO's missions, where they could see the alert of the cyberattack and connect it to the outbreak of a gastrointestinal disease, so the FHPB could run an analysis and provide advice to the commander on countermeasures. The tool could receive, process, and feed data back into these systems, including NATO's Integration Core (INTCORE), which automatically transformed the alerts into JCHAT messages and made it available with key data to a wide range of systems in the mission. During the three days of simulations and running the entire scenario twice, the system recorded 320 visits and alerted for gastrointestinal disease for 39 patients, triggering an early alarm on the first day (see table 7-3).



June 10, 2021 11:50...

Affected personnel (%)

3.0%

6/7/2021 6/20/2021

Theatre
All

Location
All

MTF Serial
All

Control limit aggregation level

Daily

Weekly

39
Number of Patients

5.0
GAS_MEDIAN (W)

5.6
GAS_MEAN (W)

14.2
GAS_UCL (W)

-3.0
GAS_LCL (W)

DATE	Number of Patients	Temperature	Pulse	Blood pressure (sys)
08/06/2021	1	38.8	120	122
09/06/2021	7	38.8	112	128
10/06/2021	12	39.4	113	113
14/06/2021	1	40.0		
15/06/2021	1	38.5	110	120
16/06/2021	6	39.3	105	108
17/06/2021	1	38.8	106	122
Total	39	39.2	110	115

DATE	Number of Patients	Gastro	COVID-19	Dental	Dermatological	Respiratory	Psychiatric	Musculoskeletal	Other
08/06/2022	1	1							
09/06/2022	7	7							
10/06/2022	12	12							
14/06/2022	1	1							
15/06/2022	1	1							
16/06/2022	6	6							
17/06/2022	11	11							
Total	39	39							

Symptom Group	Number of Patients	Temperature	Pulse	Blood pressure (sys)
Abdominal Symptoms and	33	39.2	110	115
Fever and General State Symptoms and Signs	19	39.3	110	115
Total	39	39.2	110	115

Figure 7-4. Analysis dashboard of the gastrointestinal disease cases
(Original by author)

It also picked up alerts for possible COVID-like diseases, and some other, less critical illnesses. The patient profiles were built by the FHPB and distributed to the exercise audience, who made their inputs either via their national systems or using the COE's data-entry module. The processed data and alerts were reviewed by FHPB staff and verified, in the end, that while certain improvements in message standards and communication protocols will be necessary, the system worked as intended.

When evaluating the overall outcome, the criteria for success for the entire system were:

1. Modular setup. The modules have been used separately from each other successfully, as the training audience could enter data via its normal medical dataflow, ensuring that no duplicate data entry was needed.

2. Interoperability and compatibility. The tool imported data from external databases and the entry module was run on phones, tablets, and PCs with multiple operating systems and browsers.

3. Scalability. The tool received the data without issue when receiving the entries of the three simulated days within a span of a few hours. Data refresh remained consistent within a few minutes.

4. Security. The tool ran on MILMED COE's secure cloud and data entry only happened from verified sources and with authenticated users.

5. Easily modifiable/short development cycles. The tool has since been further developed based on user feedback from the exercise. The development, which added new functionality of storing and sending the data onward when Internet coverage is not stable, was completed in a few days. Since then, the tool has been deployed for a real-life test in Munich.

6. Eases the work of the SMEs: The analysis of whether the first alerts are merited was done in minutes, and the corresponding messages to the commanders and warnings to the deployed forces were sent soon afterward, with automatically collated data to verify them. It also offers a simplified graphical interface, which can be overlaid with various Common Operational Picture (COP) maps and data.

Table 7-3. Simplified, automated export to NATO INTCORE data lake and transmission service on suspected COVID-19 cases
(Original by author)

Theatre	MTF Serial	ID	Syndrome	Latitude	Longitude	Date and Time of Admission
SKOLKAN	Kuldiga-NLD-R2	NRTSP-69	COVID-19	56.58128	21.57689	09/06/2021
Iraq	Mosul-US-R1	NRTSP-72	COVID-19	36.201	43.7133	09/06/2021
SKOLKAN	COE-DEU-R1	NRTSP-99	COVID-19	57.1989	22.3531	09/06/2021
Congo/Mali	Gao-BEL-R1	NRTSP-107	COVID-19	0.01293	16.14742	09/06/2021
Congo/Mali	Gao-BEL-R1	NRTSP-112	COVID-19	0.01293	16.14742	09/06/2021
Congo/Mali	Gao-BEL-R1	NRTSP-116	COVID-19	0.01293	16.14742	09/06/2021
SKOLKAN	Talsi-NLD-R1	NRTSP-70	COVID-19	57.1488	22.35243	10/06/2021
SKOLKAN	Latvia-FIN-R1	NRTSP-83	COVID-19	57.20349	22.35391	10/06/2021
Iraq	Mosul-US-R1	NRTSP-68	COVID-19	36.201	43.7133	10/06/2021
Iraq	Mosul-US-R1	NRTSP-78	COVID-19	36.201	43.7133	10/06/2021
SKOLKAN	Kuldiga-NLD-R2	NRTSP-88	COVID-19	56.58128	21.57689	10/06/2021
SKOLKAN	Latvia-FIN-R1	NRTSP-110	COVID-19	57.20349	22.35391	10/06/2021
SKOLKAN	Talsi-NLD-R1	NRTSP-108	COVID-19	57.1488	22.35243	10/06/2021

Conclusion

In recent decades, it has become clear that the protection of critical infrastructure requires a wide spectrum of capabilities, many of which are outside the scope of regular military tasks. The effects of climate change and the change in the volume of migration can substantially increase the chance of transmission of contagious diseases and highlight the need for functional, fast, and easy-to-use monitoring systems in areas such as the arctic or new military deployment theaters around the world. This will require flexible, rugged, and easily scalable systems with a short turnaround in development to meet the ever-changing mission parameters. The systems introduced here play a role, but truly functional preventive measures will rely on timely information. The advancement in technology, especially in data collection and analysis, and the accessibility of this technology means data can be collected more easily than a few years ago, giving NATO an important tool to protect against the devastating effects of an unmitigated pandemic or biological attack. Therefore, national and NATO assets that collect syndromic patient data should be pooled to provide the widest possible reach for data collection while keeping all necessary privacy and data protection rules. NATO MILMED COE's surveillance tool could serve as a model for a NATO-wide, near-real-time disease surveillance system.

Select Bibliography

Abat, Cédric et al. "Traditional and Syndromic Surveillance of Infectious Diseases and Pathogens." *International Journal of Infectious Diseases* 48 (July 2016). https://www.sciencedirect.com/science/article/pii/S1201971216310384?via%3Dihub.

Balajee, S. Arunmozhi, Ray Arthur, and Anthony W. Mounts. "Global Health Security: Building Capacities for Early Event Detection." Epidemiologic Workforce, and Laboratory Response. *Health Security* 14 (December 1, 2016). https://www.liebertpub.com/doi/10.1089/hs.2015.0062.

Frickmann, Hagen et al. "Infectious Diseases during the European Union Training Mission Mali (EUTM MLI) – a Four-year Experience. *Military Medical Research* 5, no. 19 (2018). https://doi.org/10.1186/s40779-018-0166-5.

Jefferson, Henry et al. "Evaluation of a Syndromic Surveillance for the Early Detection of Outbreaks among Military Personnel in a Tropical Country." *Journal of Public Health* 30, no. 4 (2008). https://academic.oup.com/jpubhealth/article/30/4/375/1508419.

Meynard, Jean-Baptiste et al. "Value of Syndromic Surveillance within the Armed Forces for Early Warning during a Dengue Fever Outbreak in French Guiana in 2006." *BMC Medical Informatics and Decision Making* 8, no. 29 (July 2, 2008). https://bmcmedinformdecismak.biomedcentral.com/articles/10.1186/1472-6947-8-29.

NATO. *Allied Joint Doctrine for Medical Support*. Allied Joint Publication (AJP)-4.10. ed. C, ver. 1. Brussels: NATO Standardization Office. September 2019. https://www.coemed.org/files/stanags/01_AJP/AJP-4.10_EDC_V1_E_2228.pdf.

NATO. *Deployment Health Surveillance*. Allied Medical Publication (AMP)-4.1, ed. A, ver. 2. Brussels: NATO Standardization Office. January 2017. https://coemed.org/files/stanags/03_AMEDP/AMedP-4.1_EDA_V2_E_2535.pdf.

— Section 3 —

Countering the Terrorist Threat to Energy, Climate Change, and Supply Chains

— 8 —

Terrorist Threats to the Energy Sector in Africa and the Middle East

Aleksander Olech

ABSTRACT: Energy security plays an increasingly important role in the common security of NATO Allies. Energy facilities such as pipelines, oil and gas terminals, and even oil fields have become targets of attacks by various terrorist groups. By taking over energy-sector infrastructure, terrorists can manipulate state actors and obtain significant revenues to develop their military capabilities. In such circumstances, NATO countries and their troops must consider the harmful activities of terrorist groups to protect NATO's energy resources and ensure future supplies to Alliance members.

Keywords: terrorism, energy, fuel, Africa, oil

Introduction

Energy security plays a critical role in the common security of the NATO Alliance. NATO's role in energy security was first defined in 2008 at the Bucharest Summit and has since been strengthened.[1] Disruption of energy supplies has a significant impact on the safety of NATO members and partner countries and may affect the implementation of military operations. While these topics are primarily the responsibility of the member states, NATO member countries regularly hold consultations on energy security to increase their strategic awareness of energy security and provide the military

[1] "NATO's Role in Energy Security," NATO (website), n.d., accessed October 12, 2021, https://www.nato.int/cps/en/natohq/topics_49208.htm.

with a reliable energy supply. Crude oil, as well as gas, are currently the main sources for the production of goods, health care, transport, and investment in new technologies. Moreover, fuel is indispensable for the sustainment of military operations. The high fuel demand of combat forces must be fulfilled to ensure the effectiveness and safety of the alliance.

This chapter will discuss the increasing number of terrorist groups and rebel cells that interfere with global energy supplies and carry out terrorist attacks on energy facilities. As many European countries strongly rely on imports from Africa and the Middle East and at the same time aim to reduce energy dependence on Russia, it is crucial to indicate the main pillars and actions that jeopardize the extraction and transport of natural resources.

In this chapter, the author initially indicates threats to the energy sector that have evolved since 2003 because of terrorist attacks. Afterward, the most significant strikes on energy infrastructure in the last decade are distinguished. Subsequently, the emphasis is put on terrorist organizations that are acquiring and transporting energy resources. Finally, the author offers recommendations that NATO could implement due to the current terrorist threats to the energy sector in Africa and the Middle East. Fundamental sources include reports from think tanks, national authorities, press releases, scientific articles, and historical analyses.

Research on this scale, focused on terrorist threats to the energy sector, has been conducted to a very limited extent. This study will show that primarily terrorist organizations from Africa and the Middle East impede supplies to NATO members.

The following chapter is vital for NATO military and policy practitioners due to several factors. Energy supplies are crucial to any military activity. The majority of NATO countries are partially dependent on Russian supplies and therefore need diversification. Many regions in Africa and the Middle East are many rich in energy resources but vulnerable to terrorist threats. This vulnerability will need to be considered regarding future NATO missions in the region. In order to sustain current technological development, it is crucial to provide vital energy from a secure and constant source. The involvement of terrorists in seizing energy supplies, the international crisis, and the increasing role of Russia and China in the energy market should be a cornerstone for future research on threats to the energy sector.

Notable drivers that impact the energy supplies to NATO include the outbreak of the COVID-19 pandemic in 2020, an unstable internal situation of many states in Africa and the Middle East, aggressive Russian energy policy, and the Russian invasion of Ukraine. These phenomena have led governments to introduce numerous measures affecting the economic situation and fuel demand and supply worldwide. Complicated relations between the elements influencing fuel supply make it necessary to pursue the efficient use of fuels to ensure an uninterrupted supply chain.

The energy sector is a fundamental part of every baseline requirement defined by NATO as crucial to sustaining the resilience of the Alliance. Energy supplies and their use are strongly connected with supporting the continuous work of critical government services, maintaining the supply of raw materials, controlling the inflow of people, providing water and food, sustaining the electricity to deal with mass casualties, offering constant communication, and maintaining means of transport.[2]

The energy sector is vital on the civilian and military levels. Without energy supplies, no NATO members could use tanks or planes. The disruption of energy supplies would cause insecurity in the societies of member and partner countries of the Alliance and adversely affect NATO military operations. Energy security is a key resilience factor and has become more important since the emergence of cyber and hybrid threats to infrastructure. As the energy transition has begun globally, armed forces must adapt to new challenges and maintain operational efficiency by diversifying sources of supplies. Moreover, combat forces have significant fuel needs, and this dependence can affect their performance, increase their vulnerability, and force them to reassign part of their personnel to the protection of supply lines.[3]

The operability of NATO and allied states' troops in Africa and the Middle East using the energy infrastructure of states in the region requires access to the deposits, pipelines, and transmission routes. To fulfill its potential, NATO needs energy for standard mobility. Using local resources, NATO can carry out operations more easily in a sustained and efficient manner.

The Russian invasion of Ukraine is also triggering true NATO cohesion and demonstrating reliance of the Alliance on energy imported from Russia. However, differing approaches toward sanctioning and boycotting

[2] Jamie Shea, "Resilience: A Core Element of Collective Defence," NATO Review (website), March 30, 2016, https://www.nato.int/docu/review/articles/2016/03/30/resilience-a-core-element-of-collective-defence/index.html.

[3] "Energy Security," NATO (website), updated July 11, 2022, https://www.nato.int/cps/fr/natohq/topics_49208.htm.

energy supplies undermine the internal cooperation of NATO and show its vulnerabilities. Although some countries decided to ban gas and oil from Russia, others are unwilling to cut the supplies. Moreover, Russian actions, such as attacks on nuclear power plants and the destruction of pipelines in Ukraine, must be considered as such war tactics could be used by terrorists and other malign actors. Adding to their gray warfare tactics of plausible denial, during the period when Russia halted energy exports to some countries, the Nord Stream 1 and 2 pipelines were sabotaged, causing the single largest release of methane in history.[4]

Russia holds leverage over some European countries because it produces roughly 30 percent of Europe's natural gas supply. Notwithstanding, in 2019, there were 12 countries exporting liquefied natural gas (LNG) to NATO (including Alliance members Norway and the United States). Qatar, the largest trader of LNG to European NATO members, is responsible for over a quarter of LNG imports, which means more than 25 percent of LNG imports are transported through the important straits of Hormuz and Bab el-Mandeb and the dangerous waters of the Gulf of Aden.[5] Other important exporters are Algeria, accounting for 13.5 percent, and Nigeria, constituting 13 percent; both countries are struggling with terrorist organizations that want to control energy supplies.[6] Furthermore, some LNG that could be rerouted to Europe is exported from Africa and then sold to Asia, the main importer. In December 2021, as much as 2.73 metric tons of LNG was delivered from Africa to Europe in comparison with Russia, which supplied 1.44 metric tons to Europe.[7] Some NATO countries mainly rely on the imports of Russian gas (for example, the Czech Republic and Hungary). At the same time, other countries (such as Belgium, the United Kingdom, and France) are only

[4] Richard Valdmanis, "Nord Stream Rupture May Mark the Biggest Single Methane Release Ever Recorded, U.N. Says" Reuters (website), September 30, 2022, https://www.reuters.com/world/europe/nord-stream-rupture-may-mark-biggest-single-methane-release-ever-recorded-un-2022-09-30/.

[5] "From Where Do We Import Energy?," Eurostat (website), n.d., https://ec.europa.eu/eurostat/cache/infographs/energy/bloc-2c.html.

[6] International Group of Liquefied Natural Gas Importers (GIIGNL), *GIIGNL Annual Report 2020: The LNG Industry*, https://giignl.org/wp-content/uploads/2021/08/giignl_-_2020_annual_report_-_04082020.pdf; and Nina Howell and Adam Quigley, "LNG in Europe 2020: Current Trends, The European LNG Landscape and Country Focus" (New York: Bracewell, 2020), https://bracewell.cld.bz/LNG-in-Europe-2020-Current-Trends-The-European-LNG-Landscape-and-Country-Focus.

[7] Nikos Tasafos (@ntsafos), "LNG flows in December 2021," Twitter, January 23, 2022, 4:34 PM, https://twitter.com/ntsafos/status/1485274819109212164.

dependent on the Russian supplies for about 15 percent or less of their supply, and the Baltic States stopped importing gas from Russia.[8]

Therefore, the maintenance and protection of energy supplies are crucial to the Alliance and its development. The Alliance's dependency on fossil fuels and its continuous search for diversification will continue to pose a significant challenge.

Defining the Phenomenon of Terrorist Attacks on Energy Infrastructure

From 1970–2018, there were almost 2,000 terrorist incidents in which gas or oil facilities were the primary targets.[9] Various African and Middle Eastern countries rely economically on the extraction and processing of crude oil and natural gas. However, production and distribution depend on critical infrastructures such as pipelines, refineries, processing plants, terminals, oil rig substations, pumping stations, ships, and tankers. At the same time, several countries struggle with internal wars and terrorist organizations that attempt to destroy critical infrastructure, threaten to make it their target, or seize it for their purposes and benefits. Between 1999–2012, more than 200 attacks on critical infrastructure related to Africa's oil and gas industry occurred.[10] Between 2014–16, al-Qaeda and Daesh alone were responsible for over 70 attacks on the energy sector in North Africa (Algeria, Libya, and Egypt).[11]

Despite being significantly enfeebled in recent years, Daesh has persisted in striking oil and gas industry-related facilities. Instances include attacks on Libya's al-Ghani oil field in 2015, in which 11 guards were killed, and the Zillah oil facility in 2019, which caused the death of five people. Similarly, energy facilities in the Middle East have also been frequent targets

[8] "Russia 'Earned' $98bn in Fuel Exports in 100 Days of Ukraine War," *Al Jazeera* (website), June 13, 2022, https://www.aljazeera.com/news/2022/6/13/russia-earned-98bn-from-fuel-export-in-100-days-of-ukraine-war; and "Baltic States Become First in Europe to Stop Russian Gas Imports," Euractiv (website), April 4, 2022, https://www.euractiv.com/section/energy/news/baltic-states-become-first-in-europe-to-stop-russian-gas-imports.

[9] Chia-yi Lee, "Why Do Terrorists Target the Energy Industry? A Review of Kidnapping, Violence and Attacks against Energy Infrastructure," *Energy Research & Social Science* 87 (May 2022): 5.

[10] Lord Aikins Adusei, "Terrorism, Insurgency, Kidnapping, and Security in Africa's Energy Sector," *African Security Review* 24, no. 3 (2015): 332–59, https://doi.org/10.1080/10246029.2015.1072967.

[11] Lukáš Tichý and Jan Eichler, "Terrorist Attacks on the Energy Sector: The Case of Al Qaeda and the Islamic State," *Studies in Conflict & Terrorism* 41, no. 6 (2018): 450–73, https://doi.org/10.1080/1057610X.2017.1323469.

of terrorist organizations. Analogous incidents have occurred with the gas and oil pipeline in Yemen and the Sinai Peninsula in Egypt, Syria, and Iraq. One meaningful example would be the failed al-Qaeda attack on the Saudi giant Abqaiq oil processing plant in February 2006, the first incident of this type in the world's top oil provider country.[12]

Terrorism targeting the energy sector is a growing worldwide phenomenon. In 2003, such strikes accounted for 25 percent of terrorist attacks, rising to 35 percent in 2005.[13] In 2016, there was a 14 percent increase in terrorist attacks targeted at the oil and gas industry, which comprised almost 42 percent of all attacks.[14] Not limited to physical attacks on power plants, refineries, and gas or oil pipelines, they include other illegal activities (such as theft of oil or gas from pipelines, extortion, or selling raw materials) to finance and support groups carrying out the physical attacks.[15] Nevertheless, funding mechanism characteristics remain unknown, as the only transparent and reliably verifiable money transfers are those from kidnapping and extortion.[16] Refineries, platforms, and factory workers' abductions are not uncommon. Such actions are aimed at obtaining a ransom, drawing attention to terrorist organizations, destabilizing the activities of corporations from countries considered to be enemies by harming them economically, or lastly, undermining the credibility of a given country as it becomes unable to ensure the safety of companies and employees.

Moreover, oil terrorism has been proven to have negative repercussions on the country's internal social situation as the related human rights violations perpetrated by terrorists have amplified popular grievances and multiplied terrorist and criminal activity as a consequence.[17] Furthermore, quantitative studies have shown that this kind of domestic terrorism is directly responsible

[12] Simon Henderson, "Al-Qaeda Attack on Abqaiq: The Vulnerability of Saudi Oil," Washington Institute (website), February 28, 2006, https://www.washingtoninstitute.org/policy-analysis/al-qaeda-attack-abqaiq-vulnerability-saudi-oil.

[13] Jennifer Giroux, "Targeting Energy Infrastructure: Examining the Terrorist Threat in North Africa and its Broader Implications (ARI)" (Madrid: Elcano Royal Institute, February 13, 2009), https://www.files.ethz.ch/isn/145554/ARI25-2009_Giroux_Energy_Infraestructure_Terrorist_Threat_North_Africa.pdf.

[14] "Terrorist Attacks and Political Violence: How Oil Is Impacted," One Brief (website), n.d., accessed November 18, 2021, https://theonebrief.com/terrorism-political-violence-risk-impact-to-oil-energy-industry.

[15] Lukáš Tichý, "The Islamic State Oil and Gas Strategy in North Africa," *Energy Strategy Reviews* 24 (2019): 254–60, https://doi.org/10.1016/j.esr.2019.04.001.

[16] Chia-yi Lee, "Oil and Terrorism: Uncovering the Mechanisms," *Journal of Conflict Resolution* 62, no. 5 (May 2018): 903–28, https://doi.org/10.1177/0022002716673702.

[17] James A. Piazza, "Oil and Terrorism: An Investigation of Mediators," *Public Choice* 169 (2016): 251–68, https://doi.org/10.1007/s11127-016-0357-0.

for the increase in oil prices, which may lead to the worsening of social and economic instability. Such a scenario becomes even more pressing and alarming in particularly fragile countries, mainly in Africa and the Middle East, which often must deal with terrorism in the energy industry.[18] It is also a challenge for NATO countries importing from insecure regions. A cessation of energy supplies could strongly impact the majority of European countries and create an inability to use military forces that rely on gasoline.

Most Significant Terrorist Attacks on Energy Infrastructure in the Last Decade

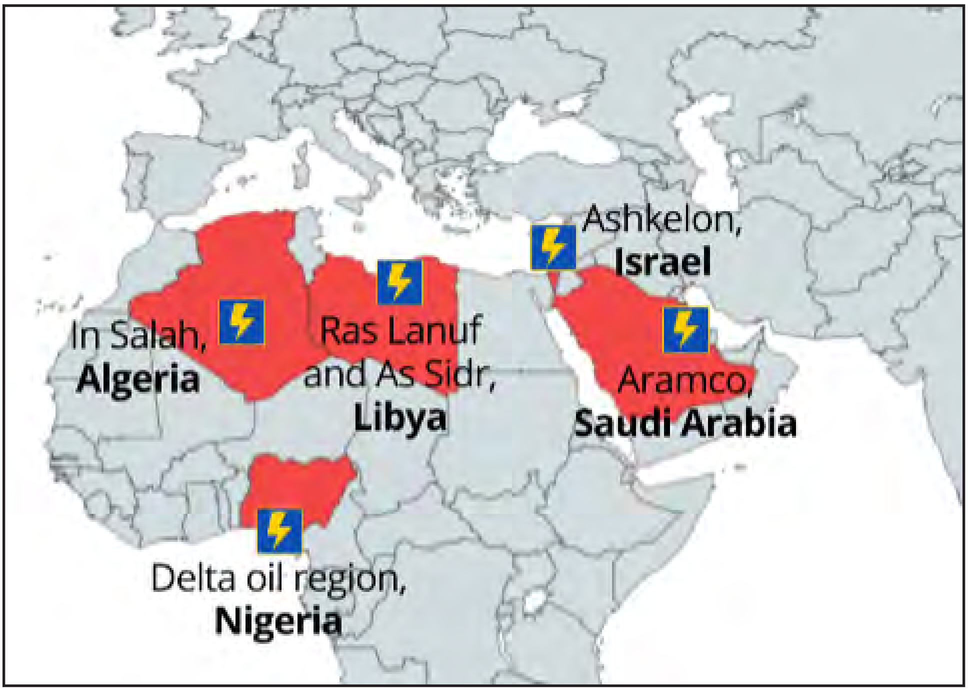


Figure 8-1. The most significant terrorist attacks on energy infrastructure in the last decade
(Original map by author)

Aramco, Saudi Arabia

Saudi Arabia is one of the largest energy suppliers in the world and closely cooperates, frequently on a military basis, with many NATO countries (for example, the United States and France). Aramco is a Saudi Arabian

[18] Dillon F. Farrell, "Oil & Terrorism: How Terrorism Affects Oil Rents" (master's thesis, Ridge College of Intelligence Studies and Applied Sciences/Mercyhurst University, 2016).

oil company based in Dhahran and is the biggest oil producer worldwide, as it is responsible for providing 10 percent of the global supply.[19] In 2016, Saudi Arabia ranked as the second country in the world as far as oil reserves are concerned, constituting 16.2 percent of the global oil reserve.[20] Such conditioning makes this region crucial for NATO energy security. Moreover, the Saudi economy itself is highly dependent on the oil industry. Being a critical point of the energy sector, Aramco has been the target of aggression, including two significant cyberattacks in 2012 and 2017 and a drone attack in 2019.[21]

The 2012 attack, executed with the Shamoon virus, damaged 10,000 company computers. The virus, malicious malware classified as a wiper, erases the hard drives of the computers it infects. According to former US Defense Secretary Leon Panetta, it was the most destructive cyberattack on the private sector to that date.[22] The attack occurred on August 15, 2012. Consequently, all significant internal networks were shut down for almost a month. It is acknowledged that the attack aimed not to seize data but to eliminate the greatest possible number of systems.[23] The attack raised concerns regarding the company's cybersecurity, as there are claims that it might have been performed by someone who had physical and direct access to a computer on the Aramco network.[24] Following the attack, the company isolated its electronic systems from the outside world to prevent the situation from happening again.

Five years later, in August 2017, Aramco faced another attack performed with a new malware version—namely Shamoon 2.0.[25] In this case, the attack aimed at erasing data and sabotaging the company's functions. Furthermore, all investigators acknowledged that the attack was meant to trigger an explosion and cause the loss of lives. According to experts,

[19] Dahlia Nehme, "Saudi Aramco: The Oil Colossus," Reuters (website), November 3, 2019, https://www.reuters.com/article/us-saudi-aramco-ipo-factbox-idUSKBN1XD03T.

[20] "Saudi Arabia Oil," Worldometer (website), https://www.worldometers.info/oil/saudi-arabia-oil/.

[21] Marwa Rashad, "Saudi Aramco Sees Increase in Attempted Cyber Attacks," Reuters (website), February 6, 2020, https://www.reuters.com/article/saudi-aramco-security/saudi-aramco-sees-increase-in-attempted-cyber-attacks-idUSL8N2A6703.

[22] Reuters Staff, "'Shamoon' Virus Most Destructive Yet for Private Sector, Panetta Says," Reuters (website), October 11, 2012, https://www.reuters.com/article/us-usa-cyber-pentagon-shimoon/shamoon-virus-most-destructive-yet-for-private-sector-panetta-says-idUSBRE89B04Y20121012.

[23] Sahar Alshathry, "Cyber Attack on Saudi Aramco," *International Journal of Management & Information Technology* 11, no. 5 (2017): 3037, https://doi.org/10.24297/ijmit.v11i5.5613.

[24] Rashad, "Saudi Aramco Sees Increase."

[25] Salem Alelyani and Harish Kumar, "Overview of Cyberattack on Saudi Institutions," *Journal of Information Security and Cybercrimes Research* 1, no. 1 (2018): 1–9.

the strike's goal was to keep Saudi Arabia from diversifying its economy and creating new employment opportunities for the young people of the country.[26] The strike raised concerns regarding the global safety of energy facilities. Furthermore, the incident represented a powerful and unique example of this emerging threat, as the hackers could cause significant physical damage.

The most recent physical attack on the Aramco facilities on September 14, 2019, was a knife in the heart of the Saudi economy. It targeted Abqaiq and Khurais, the two strategic Aramco facilities responsible for processing most of the Saudi crude oil. The strike was executed with 10 drones aimed at the facilities. The incident provoked an increase in oil prices and caused significant damage and a shortage of more than 5 percent of global oil supply.[27] Despite Yemeni Houthis claiming responsibility for the attack, Saudi Arabia, along with Western powers, accused Tehran.[28] A 2020 UN report ruled out the possibility that the drones could have been launched from Yemeni territory.[29]

The economic damage caused by the 2019 drone strike was significant, followed by an upsurge in oil prices. The Saudi petrochemical industry recovered due to its oil reserves and met the requirement for oil exports with a slight delay. Moreover, the drone attack prompted Aramco to reconsider its comprehensive security measures.

Strikes against the energy industry continue to raise concerns in the international community. Saudi Arabia has long been considered a great stabilizer of the oil market. However, recent incidents have revealed the inner vulnerability of systems and structures, evidenced by the inexpensive access to technology relative to the extent of the damage they caused. Although the country reacted immediately, its apparent vulnerability may discourage purchasers from relying on Saudi oil to a certain extent. Furthermore, there is no conclusive reason to believe comparable attacks

[26] Nicole Perlroth and Clifford Krauss, "A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try," *New York Times* (website), March 15, 2018, https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html.

[27] "Aramco Attack: Worst Disruption Ever Sends Oil Prices Soaring," *Al Jazeera* (website), September 16, 2019, https://www.aljazeera.com/economy/2019/9/16/aramco-attack-worst-disruption-ever-sends-oil-prices-soaring.

[28] Bill Chappell, "Saudi Arabia Says Iran 'Unquestionably Sponsored' Attack On Oil Facilities," NPR (website), September 18, 2019, https://www.npr.org/2019/09/18/761985624/saudi-arabia-says-iran-unquestionably-sponsored-attack-on-oil-facilities.

[29] *Final Report of the Panel of Experts on Yemen* (New York: UN Security Council, April 28, 2020), https://reliefweb.int/sites/reliefweb.int/files/resources/S_2020_326_E.pdf.

will not recur in the future, as terrorists have shown interest in developing new techniques and technologies between attacks. Shortly after the latest strike, and not coincidentally, the United States, European countries, the UN, and the International Energy Agency sent experts to Saudi Arabia to investigate the attack. Thus, they showed a common interest in obtaining additional information and developing joint preventive measures for the future.[30]

Ras Lanuf and As Sidra, Libya

In 2011, a NATO-led coalition initiated a military intervention in Libya. However, the Alliance's involvement was insufficient, and the country is still suffering, unable to recover after the civil war. Libya's rich natural resources make its economy strictly dependent on gas and oil sales. This branch makes up 94.4 percent of Libya's total income from export.[31] In particular, Ras Lanuf and As Sidra, located in the Gulf of Sirte, are the two most substantial oil terminals, with a combined export capacity of around 600,000 barrels per day. Numerous groups have targeted both locations to acquire control of Libya's largest economic branch.[32] Terrorists understand that the region's economy is strictly dependent on energy production. Therefore, this sector constitutes a significant target of their activities and provides a chance to attain political influence. Moreover, attacking pipelines and other energy facilities allows them to gain additional income to fund their operations.

One of the most significant attacks occurred in January 2016, when four oil storage tanks at the Ras Lanuf terminal were set on fire. Moreover, the assaulters targeted the pipeline, the biggest one on the Libyan coast, leading to the As Sidra terminal. The Islamic State executed the attack. The aftermath of the strike was considerably worse than the previous ones. Military actions have targeted both terminals since 2011, as affected facilities were equipped with the infrastructure necessary for oil refinement and

[30] Michelle Nichols and Humeyra Pamuk, "Saudi Arabia Consults Allies on Oil Attack, Awaits Result of Investigation: Official," Reuters (website), September 25, 2019, https://www.reuters.com/article/us-saudi-aramco-attacks-un-idUSKBN1WA1T9.

[31] Lukas Tichy, "The Islamic State Oil and Gas Strategy in North Africa," *Energy Strategy Reviews* 24 (2019): 254–60, https://doi:10.1016/j.esr.2019.04.001.

[32] Mahmoud Barakat, "Libya Resumes Oil Exports at Sidra, Ras Lanuf Ports," Anadolu Agency (website), September 16, 2019, https://www.aa.com.tr/en/energy/oil/libya-resumes-oil-exports-at-sidra-ras-lanuf-ports/33615.

export. Also, terminals remained closed for a longer period. Overall, Daesh's energy-related attacks have continued.[33]

The financial loss was immense. The attack caused a significant shortage in oil production, which fell to nearly 325,000 barrels per day in 2016, which was previously about 1.7 million barrels per day. It directly affected gas and oil exports, decreasing to 260,000 barrels per day in 2016 alone.[34] The terminals remained closed for a longer period. In May 2019, for example, Daesh claimed responsibility for the attack on the Zella oilfield, belonging to the Zueitina Oil Company, which did not result in significant physical damages to the infrastructure but constituted another significant demonstration of the actual threat of terrorist organizations on the Libyan energy sector.[35]

Regardless of the internal situation in Libya, Western countries, including the EU, whose energy security is dependent on imports from Libya for about 3.4 percent of oil and 2 percent of gas, have also been affected.[36] Moreover, being a country rich in natural resources, Libya remains essential for the European market. Any incident concerning oil security in Libya affects NATO countries, given the country's immense reserves. NATO, particularly France, the United States, and Italy, were actively engaged in the country's transformations, surfacing during the Arab Spring, to secure their interests regarding the energy sector.[37]

In Salah, Krechba Oil Fields, Algeria

Algeria, a vital NATO partner, joined the Mediterranean Dialogue in 2000 and can help reduce NATO's dependence on Russian oil and gas. Salah Gas, a joint venture formed by Sonatrach, BP, and Equinor, began gas production in the three northern fields of Krechba, Teguentour, and Reg in 2004. In 2016, the other four southern gas fields of Gour Mahmoud, In Salah, Garet el Befinat, and Hassi Moumene were included.

[33] "Islamic State Militants Attack Lybia's Ras Lanuf Oil Terminal," Africa News (website), January 21, 2016, https://www.africanews.com/2016/01/21/islamic-state-militants-attack-lybia-s-ras-lanuf-oil-terminal/.

[34] Tichý, "Islamic State Oil and Gas Strategy," 258.

[35] Ayman al-Warfalli, Ahmed Elumami, and Ahmed Eljechtimi, "Three Killed in Suspected Islamic State Attack outside Libyan Oilfield," Reuters (website), May 18, 2019, https://www.reuters.com/article/us-libya-oil-attack-idUSKCN1SO0CP.

[36] "Trade – Libya: EU Trade Relations with Libya: Facts, Figures and Latest Developments," European Commission (website), n.d., https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/libya_en.

[37] Milad M. Elharathi, "Humanitarian Intervention: Morals versus Realism: The Use of Force in the Defence of Human Rights in Libya," *World Affairs: The Journal of International Issues* 18, no. 1 (2014): 76, https://www.jstor.org/stable/48504954.

In March 2016, the Krechba oil field was attacked by an explosive detonated from a long distance. Consequently, it had to be closed for safety reasons.[38] Targeting the Sonatrach facilities could have immense consequences as it is Africa's largest oil and natural gas company, making Algeria the seventh largest natural gas exporter in the world. Any threats to block production could result in a shortage of supply and a significant increase in prices. For this reason, Algeria, one of Europe's leading gas suppliers, represents a critical point in NATO's strategy to combat terrorism and cyber threats.[39]

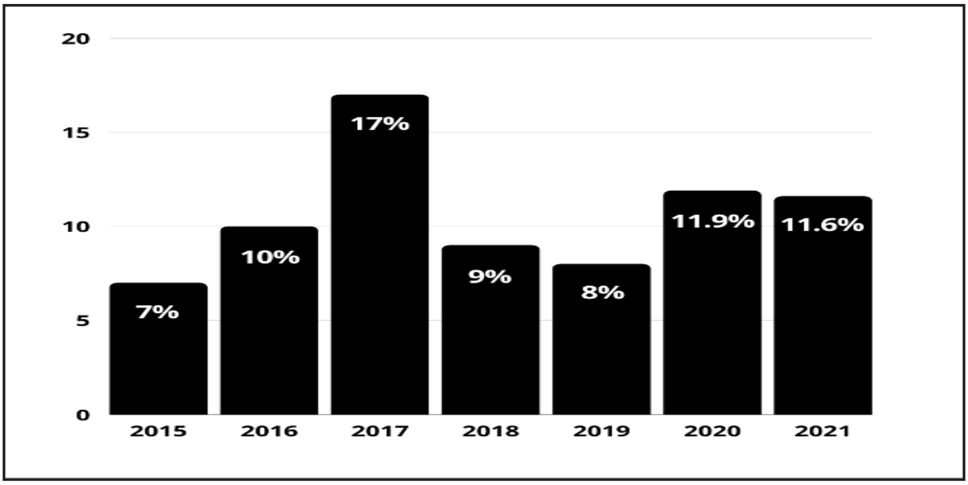


Figure 8-2. The share of Algerian gas in total gas imports by EU countries
(Original chart by author)

Ashkelon, Israel

Israel has been a crucial NATO partner for more than 20 years and an active member of NATO's Mediterranean Dialogue. The Trans-Israel pipeline, also known as Eilat-Ashkelon or the Europe-Asia Pipeline, was constructed to transport Iran-originated crude oil from Israel to Europe. The pipeline operator, the Eilat Ashkelon Pipeline Company (EAPC, also known as Europe Asia Pipeline Company), has main infrastructures in the cities of Eilat, Beersheva, and Ashkelon. The Ashkelon infrastructure is the largest and belongs to the EAPC. Additionally, Ashkelon serves as the base for various other independent oil storage tanks operated by different international companies.

[38] Associated Press, "Gas Facility in Algeria Is Attacked with Rockets," *New York Times* (website), March 18, 2016, https://www.nytimes.com/2016/03/19/world/africa/algeria-bp-statoil-gas-facility-attack.html.

[39] James Thorpe, "NATO and Algeria Strengthen Counter-terror Partnership," *International Security Journal* (website), May 27, 2021, https://internationalsecurityjournal.com/nato-and-algeria-partnership/.

On May 11, 2021, Hamas attacked the coastal city of Ashkelon, and, as a result, the Israeli oil refinery and pipelines, including the Eilat-Ashkelon pipeline, were destroyed. On May 12, after the assault, which resulted in a fire of the Trans-Israel pipeline, the US public energy corporation Chevron shut down its platform on the Israeli shore.[40]

Delta Oil Region, Nigeria

Nigeria is currently an LNG supplier to several NATO countries. In addition, Abuja has strong ties with Moscow, which the Alliance should monitor. The Niger Delta region is oil-rich and, at the same time, concentrates most of the oil production. Therefore, this region is crucial for the energy security of NATO countries, as both Europe and the United States are experiencing an increase in demand for imported energy. However, the instability that has characterized the territory since the beginning of the twenty-first century resulted in the blocking of a quarter of Nigeria's supplies.[41]

In 2016, the Chevron CVX.N platform in the Niger Delta region became the target of an attack. According to Chevron, the largest oil exporter in Africa, the attack was executed on May 4, and the Niger Delta Avengers (NDA) militant group immediately claimed responsibility for the incident. In the days following the attack on the platform, the group continued destructive activities and attacked other significant facilities, such as gas lines and crucial installations. The NDA operation transformed into a three-month series of attacks. The motivation behind the aggression was purely economic, as the group released a statement demanding a more considerable share of crude oil sales.[42]

Similar to other groups that emerge in politically unstable countries, the NDA was created in February 2016 following political tensions in the country after the 2015 presidential election. Besides the fight for the profit from oil exports, NDA claims to fight for the people of the Delta region

[40] Elza Turner and Eklavya Gupte, "Rocket Hits Crude Oil Storage Tank at Trans-Israel Pipeline: Reports," S&A Global (website), May 12, 2021, https://www.spglobal.com/platts/en/market-insights/latest-news/oil/051221-rocket-hits-crude-oil-storage-tank-at-trans-israel-pipeline-reports.

[41] Jamie Shea, "Energy Security: NATO's Potential Role," NATO Review (website), September 1, 2006, https://www.nato.int/docu/review/articles/2006/09/01/energy-security-nato-s-potential-role/index.html.

[42] Tife Owolabi, "Militants Attack Chevron Platform in Nigeria's Oil-rich Niger Delta," Reuters (website), May 5, 2016, https://www.reuters.com/article/us-nigeria-oil-delta-idUSKCN0XW1PL.

suffering due to "divisive and exclusive" politics. Simultaneously, the group aspires to form an independent Niger Delta Republic.[43]

Indeed, since the discovery of the oil fields in 1950, the Delta region has struggled with violence and instability. The country's development and viability depend on natural resources, whereas control over them belongs to the government and oil multinationals. Thereby, entire communities are disregarded due to the lack of social and infrastructural development, while Nigeria is facing numerous violent clashes and the emergence of militant groups like NDA.[44] Oil terrorism has harmful consequences for the suppliers and affects the country's internal situation at the same time. For example, terrorist attacks on Nigerian pipelines in 2016 resulted in a 36 percent decrease in oil production, resulting in a 50 percent reduction in government revenue.[45]

Terrorism in the Energy Sector as the Instrument of Geopolitical Pressure

Currently, Africa and the Middle East contain the highest number of terrorist organizations. Several different groups and their affiliates, which are lethal not the countries in which they operate and to others, including all NATO member states. The concentration of extremists in the region is strongly related to the ongoing armed conflicts, unstable situation in failed states (such as Yemen, Somalia, and Syria), and the competition of terrorist groups for land, money, and arms and drug trafficking. All these circumstances allow terrorists to carry out activities and plan future attacks, often jeopardizing energy stability. Thus, NATO countries and their troops must consider the harmful activities of terrorist groups, including their attempts to destroy key energy centers, which have become one of their main targets.

Based on recent terrorist incidents in Africa and the Middle East strongly related to energy security, it is essential to know which terrorist groups carry out operations that could affect NATO allies, armed forces, and energy

[43] *Resurgence of Militancy in the Niger Delta: Update on the Niger Delta Avengers* (Askoro Abuja, NG: Foundation for Partnership Initiatives in the Niger Delta, June 2016), https://fundforpeace.org/wp-content/uploads/2018/08/PIND-Briefing-Niger-Delta-Avengers-June-2016.pdf.

[44] Mercy Erhi Makpor, "The Niger Delta Avengers: An Assessment of the Causes, Agitation, Major Challenges for OMNCs and Suggestions for Tackling Insurgency in the Niger Delta Region of Nigeria," *International Journal of Research in Humanities and Social Studies* 4, no. 10 (2017): 16–26.

[45] "Terrorist Attacks and Political Violence."

supplies. There are at least a dozen significant terrorist groups—with cells and affiliates in nearby countries—that should be mentioned. The largest organizations that operate with the intention of destroying or exploiting energy resources will be emphasized in the following sections.

Daesh

Daesh has long been considered the wealthiest terrorist organization in the world. Between 2014–15, oil production in controlled areas constituted its most important, if not primary, source of revenue. This terrorist organization controlled 8 out of 114 oil production sites in Iraq, such as the Ajil field, the oil wells in the Hamrin Mountains, the Qayara and Najma fields, and the Baiji refinery. In Syria, out of 75 sites in total, there were 34 spots located in the eastern governorates of Dayr al-Zawr, Hassaka, and Raqqa under its supervision.[46] When it comes to Daesh's approach to the energy issue, three components can be distinguished.

1. Efficient development of oil and gas fields in Syria and Iraq.

2. Increasing oil and gas production to secure financing for the organization.

3. Seizure of new oil and gas fields and destruction of critical infrastructure in the countries Daesh considers hostile to weaken the economy in those countries.[47]

The Daesh Shura Council identified oil and gas as key survival instruments.[48] In 2014, Daesh controlled over 60 percent of Syria's and nearly 10 percent of Iraq's oil production. According to the World Bank Group, the organization was produced up to 86,000 barrels per day in the first half of 2014 and 56,000 barrel's per day in the year's second half. However, the production level dropped significantly to 35,000 barrels per day in 2015 and 16,000 barrels per day in 2016. This noticeable production

[46] Quy-Toan Do et al., *How Much Oil Is the Islamic State Group Producing?: Evidence from Remote Sensing*, Policy Research Working Paper, no. 8231 (Washington, DC: World Bank, 2017), https://openknowledge.worldbank.org/handle/10986/28617.

[47] Jessica Lewis McFate, *The ISIS Defense in Iraq and Syria: Countering an Adaptive Enemy*, Middle East Security Report, no. 27 (Washington, DC: Institute for the Study of War, May 2015), https://www.understandingwar.org/report/isis-defense-iraq-and-syria-countering-adaptive-enemy.

[48] Tichý and Eichler, "Terrorist Attacks on the Energy Sector."

decrease, reflected in the overall revenue decline, has been accompanied since 2015 by territorial and financial losses for the organization.[49]

Moreover, compared with previous production trends, Daesh could not exploit the seized fields efficiently to use their full production potential. Nevertheless, Daesh's appropriation and utilization of any energy facility are to be treated as a severe threat regardless of whether the terrorists can use the production potential. The oil production was directly managed by Daesh, while the oil distribution network in the area under its supervision was not its immediate concern.[50] Oil sold to independent distributors was purchased either by small local refineries or other intermediaries transferring it further. According to the official reports, Daesh may have charged from $15 to $45 per barrel, depending on oil quality and local market conditions.

Before the establishment of the Global Coalition against Daesh, testimony to the US Senate Committee on Energy and Natural resources estimated the organization could have earned between $1 and $1.5 million US dollars on oil sales.[51] Moreover, despite the lack of knowledge on the exact numbers regarding production or revenue, it is estimated that between 2014–15, weekly revenue generated from oil sales amounted to several million US dollars. Although the fight against Daesh claimed to be victorious, the organization still exists and continues operations in the Middle East and Africa. It constantly exercises physical control over smaller regions, including those producing crude oil and natural gas. Moreover, Daesh continues to launch attacks against critical infrastructure. The latest assault on a Syrian gas pipeline occurred on September 17, 2021.[52] Taking the above information into consideration, terrorist organizations can take over critical infrastructure and profit from it, making the risk of the occurrence of such situations possible in the future.

[49] "Islamic State Territory Down 60 Percent and Revenue Down 80 Percent on Caliphate's Third Anniversary, IHS Says," IHS Markit (website), June 29, 2017, https://news.ihsmarkit.com/prviewer/release_only/slug/aerospace-defense-security-islamic-state-territory-down-60-percent-and-revenue-down-80.

[50] "How Much Oil Is the Islamic State Group Producing?: Evidence from Remote Sensing," World Bank Group (website), n.d., https://openknowledge.worldbank.org/handle/10986/28617.

[51] *Testimony before the US Senate Committee on Energy and Natural Resources: Hearing to Examine Terrorism and the Global Oil Markets*, 114th Cong. (2015) (statement of Peter Harrell, adjunct senior fellow, Center for a New American Security), https://www.cnas.org/publications/congressional-testimony/peter-harrell-before-the-senate-committee-on-energy-and-natural-resources.

[52] Daniel Onyango," ISIS Claims Responsibility for Pipeline Attack and Power Blackout in Syria," Pipeline Business (website), September 21, 2021, https://www.pipeline-journal.net/news/isis-claims-responsibility-pipeline-attack-and-power-blackout-syria.

Boko Haram

Boko Haram frequently carries out terrorist activities in the energy sector, especially in Nigeria. In 2017, Nigerian President Muhammad Buhari's administration began exploring the northeastern region of Nigeria and the Lake Chad Basin.[53] The discovery of new sources of natural resources would have allowed the country to diversify its supplies. The pressing menace of Boko Haram's entrenched presence in the territory did not initially deter the state from attempting to create a new source of revenue and boost the economy of a region whose poverty is also attributable to terrorists' activities.[54] However, Boko Haram's attack on a convoy escorting surveyors in the northeastern state of Borno hindered these plans. The attack resulted in dozens of killings, including Civilian Joint Task Force members supporting armed forces in combating the terrorist group. Moreover, four oil workers were kidnapped, and at least one was killed, while Boko Haram appeared to be asking for ransom for the remaining three. Consequently, E. Ibe Kachikwu, the Nigerian minister of state for petroleum resources, immediately halted the exploration until security clearance was granted.[55] Nevertheless, it has been made clear that the Nigerian government remains eager to conduct future exploration activities in the Borno state.

Boko Haram has never ceased targeting energy infrastructure. In January 2021, it blew up Maiduguri's power tower, plunging the capital city of the Borno state into darkness. In February 2021, it launched explosives toward the same city, killing at least 10 people and injuring about 50.[56] The constant presence of Boko Haram makes it impossible to explore the northern areas for raw materials exploitation. The establishment of new energy infrastructure in areas under its control may lead to the interception of extracted oil, providing the group with an additional source of income. Furthermore, there are more terrorist groups in the Sahel region and Nigeria

[53] "Nigeria: du pétrole bientôt exploité sur les terres de Boko Haram?," France TV Info (website), July 27, 2017, https://www.francetvinfo.fr/monde/afrique/politique-africaine/nigeria-du-petrole-bientot-exploite-sur-les-terres-de-boko-haram_3057249.

[54] John Campbell, "Boko Haram Blocks Oil Exploration in Northeast Nigeria," Council on Foreign Relations (website), August 1, 2017, https://www.cfr.org/blog/boko-haram-blocks-oil-exploration-northeast-nigeria.

[55] Ludovica Iaccino, "Boko Haram's Fatal Ambush Destroys Hope of Boost to Nigeria's Economy with Borno Oil," International Business Times (website), July 28, 2017, https://www.ibtimes.co.uk/boko-harams-fatal-ambush-destroys-hope-boost-nigerias-economy-borno-oil-1632401.

[56] Blessing Tunoh, "Boko Haram Blows Up Power Tower, Throws Maiduguri into Darkness Again," Channels TV (website), March 27, 2021, https://www.channelstv.com/2021/03/27/boko-haram-bombs-power-tower-throws-maiduguri-into-darkness-again/.

itself that can be directly engaged in attacking energy infrastructure in the Middle East and North Africa region.[57]

Nigeria remains the biggest energy producer in Africa, having immense natural-gas reserves. In 2018, it was the fifth largest exporter of LNG in the world, producing up to 2 million barrels per day.[58] Additionally, Nigeria remains the largest economy and most populous country in Africa and within OPEC, making the country a truly impactful actor in the regional security scenario.[59] However, Nigeria's extraction and production capacity has been affected by the presence of terrorist organizations in its territory. It was estimated that, in 2014, an average of 75,000 to 150,000 barrels of crude oil were stolen each day in the Delta region, causing tremendous economic damage since the Nigerian economy is highly dependent on oil and gas export.[60]

Taking into consideration the area of Boko Haram's activities, which are concentrated mainly in northeastern Nigeria, this terrorist organization has not yet posed a regular threat to the state energy sector, given that Nigeria's oil and gas fields are located mostly in the south. Nevertheless, the state's revenue from natural resources could provide for a more effective fight against rebels, as it would make it possible to boost investment in developing military and anti-terrorist capabilities. On the other hand, an economy that relies on natural resources in energy production and export for 70 percent of state revenue is a victim of fluctuations in oil prices. Indeed, the poor economic situation translates into increased uncertainty on the political scene, which could serve as a crucial factor in the further destabilization of the country.

There are well-grounded concerns regarding the future of the oil industry in the Lake Chad region. Boko Haram will regularly attack critical infrastructure (such as oil pipelines and production sites) and try to seize

[57] Alan Lis and Aleksander Ksawery Olech, "The Activity of Jihadist Terrorist Organizations in the Region of Sahel," Institute of New Europe (website), June 21, 2021, https://ine.org.pl/en/the-activity-of-jihadist-terrorist-organizations-in-the-region-of-sahel.

[58] *BP Statistical Review of World Energy 2019*, 68th ed. (London: BP, 2019), https://www.bp.com/contenta/dam/bp/business-sites/en/global/corporate/pdfs/energy-economics/statistical-review/bp-stats-review-2019-full-report.pdf.

[59] "Energy and Security – Nigeria," Robert Strauss Center for International Security and Law (website), n.d., https://www.strausscenter.org/energy-and-security-project/nigeria/.

[60] "Threats and Opportunities for Energy Sector in West Africa," International Peace Institute (website), September 9, 2014, https://www.ipinst.org/2014/09/threats-and-opportunities-for-energy-sector-in-west-africa.

it to sell oil and generate a steady source of income.[61] For this reason, countries around Lake Chad should strengthen their internal anti-terrorism policies to protect citizens, secure critical energy installations, and cooperate on a transnational level to fight terrorists.

Niger Delta Avengers

The Niger Delta Avengers (NDA), which emerged in 2020, is another group that directly threatens and accounts for most of the attacks on the Nigerian energy sector. Their actions, including the oil installation bombing in the Niger Delta, demonstrate opposition to the government's negligence toward the region. Moreover, they objected to its alliance with foreign energy multinationals, who are accused of extracting and exploiting indigenous natural resources while failing to improve the social and economic conditions of Nigerian citizens.[62] Activities of the NDA pushed the president of Nigeria to initiate an amnesty program for the group members to maintain peace in the southern regions. Although the program has been in force since 2009, it failed to dissuade the NDA from launching widespread attacks in 2016, thus plunging the country into recession.

In the summer of 2016, the NDA threatened to declare the independence of the southern oil-rich region as an extreme act of defiance against the Nigerian government. The groups indicated that the region's richness in natural resources did not translate into an increase in the standard of living of its citizens. Between February and August 2016, the NDA reported at least 14 attacks on oil fields and terminals in the states of Delta (9 attacks), Bayelsa (three attacks), and Akwa Ibom (two attacks), reducing the country's production to merely 1.4/1.5 million barrels per day.[63] Such a situation was particularly challenging for Nigeria, as the attacks took place concurrently with the drop in the value of the Naira, the Nigerian currency. Immediately after the 2016 attacks, Nigeria lost its primacy as Africa's largest oil exporter, surpassed by Angola. This scenario corresponds precisely with the purpose of the terrorist strategy designed and

[61] J. Tochukwu Omenma, "Untold Story of Boko Haram Insurgency: The Lake Chad Oil and Gas Connection," *Politics and Religion* 13, no. 1 (2020): 180–213, https://doi.org/10.1017/S1755048319000166.

[62] Michael Fitzpatrick, "France Creates Agency to Fight Foreign Fake News Aiming to Undermine the State," RFI (website), June 5, 2021, https://www.rfi.fr/fr/afrique/20160526-nigeria-sont-vengeurs-delta-niger-rebelles-mend-installations-petrolieres.

[63] "Nigeria: les Vengeurs du Delta du Niger menacent de déclarer l'indépendance de la région pétrolifère," Jeune Afrique (website), October 19, 2016, https://www.jeuneafrique.com/350315/politique/nigeria-rebelles-menacent-de-declarer-lindependance-delta-niger/; and Eklavya Gupte, "Niger Delta Militants Threaten to Resume Attacks on Nigeria's Oil Installations," SP Global (website), June 28, 2021, https://www.spglobal.com/platts/en/market-insights/latest-news/oil/062821-niger-delta-militants-threaten-to-resume-attacks-on-nigerias-oil-installations.

implemented by the NDA: to destabilize and weaken the Nigerian economy to such an extent that the country's central government could no longer be ignore its claims. The 2016 attack was swiftly followed by negotiations between the Buhari government and the terrorist group and a ceasefire in August, which implied the threat was relatively contained. However, in June 2021, the rebels announced a resumption of attacks as part of Operation Humble, aimed at "humbling" the Nigerian economy, driving it into a prolonged recession.[64]

There is also another danger in the country that needs to be highlighted. In 2020, the Movement for the Emancipation of the Niger Delta (MEND) launched attacks on gas and oil pipelines in the Bayelsa state.[65] This small rebel group continues operations of a movement that emerged around 2004 and whose activity was based on attempts to stop oil production in the Niger Delta region and environmental devastation, including polluting gas flaring and oil spills, deforestation, and desertification. Their methods included kidnappings of oil workers for ransom, armed attacks on production facilities, pipeline destruction, and theft of oil that was later sold on the black market.[66] The MEND activity demonstrates the increase of terrorist threats in Nigeria and the possible involvement of other rebel groups in the energy sector.

al-Qaeda

Energy infrastructure components, such as oil pipelines, are easily accessible and constitute a target that can cause significant economic damage if attacked. As early as 2002, al-Qaeda began exploring the possibility of attacks on natural resources when it attacked the French-flagged *Limburg* tanker carrying 397,000 barrels of oil off the coast of Yemen. In April 2008, after the attack on a Japanese tanker that took place in the same place, oil price soared to a record $117 per barrel. Meanwhile, when al-Qaeda attempted to attack the Abqaiq refinery in Saudi Arabia in February 2006, the attempt caused oil prices to rise by $2 per barrel.[67]

Attacks in Algeria have been less frequent since the civil war ended in 2002, but groups such as al-Qaeda in the Islamic Maghreb (AQIM) and

[64] Gupte, "Niger Delta Militants."

[65] Rayyan Alhassan, "Niger Delta Militants who Bombed Oil Pipelines in Bayelsa Make 5 Demands to Nigerian Government," *Daily Nigerian* (website), November 27, 2020, https://dailynigerian.com/niger-delta-militants-bombed/.

[66] "Nigeria's Shadowy Oil Rebels," *BBC News* (website), April 20, 2006, http://news.bbc.co.uk/2/hi/africa/4732210.stm.

[67] "Saudis Foil Oil Facility Attack," *BBC News* (website), February 24, 2006, http://news.bbc.co.uk/2/hi/middle_east/4747488.stm.

fighters allied with Daesh remain active. In 2006 and 2007, AQIM militants bombed a gas pipeline, which was temporarily taken out of service as a result.[68] Other related attacks involved the bombing of coaches carrying oil workers.

Algerian oil and gas infrastructure has been heavily safeguarded by the national army, especially since the 2013 attack on the In Amanas gas plant operated by BP and Statoil, during which 40 workers were killed.[69] At that time, Algeria could not transport energy supplies and lost almost all international contracts. Moreover, it demonstrated the strength of terrorist organizations that may not threaten national security and affect all recipients of supplies, including many NATO countries.[70] In 2016, another attack on an Algerian gas power plant caused no loss of life or damage. However, as a precautionary measure, the facility was temporarily shut down, which negatively affected the importing countries and national interests.

As global demand grows, the Algerian energy sector's vulnerability to all threats may increase, which will be reflected in costs. Furthermore, non-state armed groups (such as AQIM) will continue to evolve, innovate, and prove their ability to circumvent security measures by conducting asymmetric attacks. The number of terrorist groups in the Sahel region, either affiliated with al-Qaeda or Daesh, is growing. In this case, the risk of new strikes on energy facilities is relatively higher.

State Terror and the Use of Terrorist Groups in the Energy Sector

Oil and natural gas could also become state governments' political tools, especially when they are influenced by organizations recognized as terrorists. One such example is the Islamic Revolutionary Guard Corps (IRGC). In 2008, the IRGC commander Mohammad Ali Jafari stated that "the enemies know that we could easily block the Strait of Hormuz indefinitely."[71] Hormuz is one of the most important places for transporting natural

[68] Giroux, "Targeting Energy Infrastructure."

[69] Joachim Dagenborg and Lamine Chikhi, "Algeria's In Amenas Gas Plant Returning to Normal after Attack," Reuters (website), September 1, 2014, https://www.reuters.com/article/us-statoil-bp-algeria-idUSKBN0GW2N820140901.

[70] Tomasz Kijewski, "Atak terrorystyczny na kompleks gazowy Tiguentourine w In Amenas w Algierii w styczniu 2013 r. jako przykład nowych zagrożeń dla energetycznej infrastruktury krytycznej i bezpieczeństwa wewnętrznego państwa," *Przegląd Bezpieczeństwa Wewnętrznego* 9, no. 13 (2013): 202–23.

[71] Keith Crane et al., "Oil Revenues, Rogue States, and Terrorist Groups," in *Imported Oil and U.S. National Security* (Santa Monica, CA: RAND Corporation, 2009): 43–58, https://www.rand.org/pubs/monographs/MG838.html.

resources worldwide. If Iran did block the strait, oil prices worldwide would rise significantly. Although Jafari's statement was delivered 13 years ago, it is still very relevant.

Indeed, terrorism on energy supplies affects the security of strategic chokepoints. Four of the routes particularly at risk are located in the Middle East—the Strait of Hormuz at the mouth of the Persian Gulf, the Bab el-Mandeb Strait at the southern entrance to the Red Sea, the Suez Canal and the Sumed pipeline connected to the Red Sea of the Mediterranean, and the Turkish straits linking the Mediterranean and the Black Sea. These vital energy trade corridors have been repeatedly targeted by terrorist organizations, especially in the context of the numerous conflicts in the region. In 2013, for example, al-Qaeda–affiliated groups damaged two ships using grenades in the Suez Canal. Similarly, in 2014, Daesh attacked and sabotaged the primary Iraq-Türkiye export line from Kirkuk to Ceyhan.[72] Almost all territories close to the most significant chokepoints were the aim of attack from terrorist organizations. The possible additional terror from transit states could heavily affect the situation in the energy supply market.

Recommendations

Energy security has been a crucial strategic factor since the early twentieth century. In an era increasingly dominated by hybrid warfare, it has become one of the main challenges for NATO and the European Union. Terrorist attacks conducted by extremist groups against energy infrastructure can have disastrous consequences. To combat the growing threat to the energy security environment, countries must adopt a multifaceted approach. NATO and EU countries should undertake joint efforts aimed to diversify their energy sources, develop national infrastructure, and invest in alternative energy sources so they are not compelled to rely heavily on oil and gas supplied from unstable regions.

Oil and gas importing countries could allocate funds to help support the native communities affected by the oil and gas production in Sudan, Nigeria, or Algeria. These funds could help provide military training, police funding, community patrols, and strengthen critical infrastructure. For instance, in Iraq, the United States helped fund 14,000 security guards,

[72] Robin Mills, "Risky Routes: Energy Transit in the Middle East," Brookings Doha Center Analysis Paper, no. 17 (Doha: Brookings Institution, April 2016), 1–37, https://www.brookings.edu/wp-content/uploads/2016/07/en-energy-transit-security-mills-2.pdf.

who were placed at critical locations along major pipelines. The United States also supplied monitoring equipment, including electronic motion sensors.[73] The French Republic also uses its soldiers to protect Africa's key transit routes and energy facilities.[74]

NATO should concentrate on securing the world's most important chokepoints to ensure the continued flow of volumes of natural resources. Moreover, the cooperation between NATO countries, which are recipients of energy, and their main extractors and exporters should be strengthened. NATO's involvement could take various forms—from military presence for counterterrorism to education. NATO can also assist with education and training for countries struggling with terrorism and attacks on energy infrastructure. Securing the supply chain in the most sensitive regions is also in the interest of NATO countries. It is a NATO duty to develop security measures to protect the Alliance from physical terrorist attacks and terrorist cyberspace intrusions that threaten energy supplies.

In addition, the future growth in gas demand should be directed toward Africa, which will witness a 40 percent growth in production between 2018–30. In contrast, production is expected to decline in the EU (-8 percent).[75] Helping to diversify European energy supplies has been part of the US response, alongside NATO defense and diplomatic efforts. For this reason, to diversify and secure energy supplies, NATO should strengthen counterterrorist cooperation with African and Middle Eastern countries. The next step is to develop an effective anti-terrorist strategy to secure energy supplies in Africa and the Middle East to ensure successful energy delivery, verification of dangers, and tools to eliminate the threats to energy consumers and suppliers.

Conclusion

Terrorism, cyberattacks, infrastructure sabotage, attacks on oil tankers and pipeline installations, and attacks and killings of people associated with the

[73] "New Technology Can Help Fight Pipeline Sabotage," Institute for the Analysis of Global Security (website), March 31, 2004, www.iags.org/n033104t1.htm.

[74] Aleksander Olech, *International Military Involvement of the French Republic* (Warsaw: Institute of New Europe, 2021), https://ine.org.pl/wp-content/uploads/2021/07/International-Military-Involvement-of-the-French-Republic.pdf.

[75] Rim Berahab, *Global Trends in the Energy Sector and Their Implication on Energy Security in NATO's Southern Neighbourhood* (Madrid: Elcano Royal Institute,September 8, 2020), 5, https://media.realinstitutoelcano.org/wp-content/uploads/2021/10/ari103-2020-berahab-global-trends-energy-sector-and-implication-on-energy-security-in-natos-southern-neighbourhood.pdf.

energy companies represent a shift in the nature of war. It is not necessarily the state's territory that is threatened by military aggression, but critical infrastructures, such as oil, gas, and pipeline installations. Such activities may significantly impact the NATO member states importing natural resources from the Middle Eastern and African countries. The actions mentioned above might temporarily halt the flow of crude oil and liquefied natural gas. In the future, one can expect an increased cyber and kinetic attacks.

Special attention should be given to places strategically crucial for energy supply, such as the Strait of Hormuz and Bab el-Mandeb Strait, which have become targets of terrorist organizations. In 2018, several Saudi tankers crossing the Bab el-Mandeb Strait were attacked by the Yemeni Houthi fighters, resulting in the suspension of supplies. Any blockage in the flow of goods brings enormous financial losses for numerous countries and organizations.

In 2018, as many as 6.2 million barrels per day of refined crude oil were transported through the Bab el-Mandeb Strait, to Europe, the United States, and Asia, accounting for approximately 9 percent of all oil transported by sea.[76] Meanwhile, in 2020, about 18 million barrels of crude oil and LNG passed through the Strait of Hormuz daily. With the exploitation of resources in new maritime areas and tankers traversing uncertain waters, external support from NATO will remain essential in securing supplies located in unstable regions. At the same time, transport from Nigeria has been regularly interrupted for many years, damaging for deliveries from the Gulf of Guinea.

Under the aggressive energy policy pursued by Russia, NATO has a limited range of maneuver and must concentrate on supplies from other sources. From 2015–21, African and Middle Eastern countries, led by Saudi Arabia, were in the top 10 countries supplying oil to NATO members.

In 2020, Nigeria, one of Africa's important oil producers, championed oil importation, striking more than 466,000 barrels per day, followed by Morocco with 240,000 barrels per day. Petroleum imports accounted for 17 to 20 percent of imports in Nigeria, Kenya, Egypt, and Ghana in 2019. This ratio tends to increase as the oil price rises. We expect current account deficits to come under pressure and widen in oil-importing countries. Africa can turn the Russia-Ukraine war oil price

[76] Justine Barden, "The Bab el-Mandeb Strait Is a Strategic Route for Oil and Natural Gas Shipments," US Energy Information Administration (website), August 27, 2019, https://www.eia.gov/todayinenergy/detail.php?id=41073.

chaos into an opportunity for competitive oil producers (such as Niger, Algeria, Libya, and Angola) to cash in with more crude oil exports.[77]

The energy sector is a vital part of critical infrastructure, and its vulnerabilities must be taken into account. Without a stable energy supply, health and welfare are threatened, and a country's economy cannot function. Critical infrastructure is as complex as it is vulnerable, and terrorist groups have been able to carry out attacks on its most fragile structural components in the oil and gas sector. These attacks have often generated significant losses in human lives, the economy, and national security. Prediction studies based on game-theory methodology have demonstrated that strategies aimed at improving the robustness of critical infrastructures may be an instrumental protection solution.[78] Interestingly, terrorism in the energy sector does not seem to target oil and natural gas exclusively. More recently, serious concerns have been rising in Europe. These concerns include the terrorist threat to the Desertec renewable energy project for the Middle East North Africa region, which is expected to become one of Europe's crucial energy sources.[79]

Terrorist attacks on the oil and gas infrastructure harm the suppliers and the country's internal situation by reducing government revenue. Such incidents have an immediate impact on local economies, which in the long term can lead to social unrest and potentially result in more people willing to join the ranks of hostile groups carrying out attacks. Furthermore, for any organization involved in oil production, gas, or any other industry directly linked to energy supply, disruptions can directly impact the demand for their products and services and the ability to deliver them. Subsequently, this can affect local inflation, cost of living, employment rates, and over time the development of terrorism. The need for NATO countries' involvement may become essential, but most critical infrastructures may have already been seized or destroyed. NATO members may participate in many foreign missions in the Middle East and Africa under the EU or UN mandate and carry out their military and nonmilitary operations. If countries such as Algeria, Libya, Nigeria, and Saudi Arabia lose capacity to export energy resources and Russia sustains an aggressive energy policy,

[77] Padili Mikomangwa, "Russia Oil Chaos Should Push Africa to Be Energy Self-reliant," Exchange (website), March 9, 2022, https://theexchange.africa/africa/russia-oil-chaos-should-push-africa-to-be-energy-self-reliant.

[78] Xijun Yao et al., "Assessment of Terrorism Risk to Critical Infrastructures: The Case of a Power-Supply Substation," *Applied Sciences* 10, no. 20 (2020): 7162, https://doi.org/10.3390/app10207162.

[79] Karen Smith Stegen, Patrick Gilmartin, and Janetta Carlucci, "Terrorists versus the Sun: Desertec in North Africa as a Case Study for Assessing Risks to Energy Infrastructure," *Risk Management* 14, no. 1 (February 2012): 3–26.

there will be a breakdown in the market, and NATO will lose capacity to operate fully.

In the future, terrorists may attack not only regions that are rich in natural resources but also transport infrastructure. To undermine NATO countries and their allies carrying out missions in the Middle East and Africa, terrorists will seek to cut off energy sources. Moreover, by taking control of the sale of energy resources, they will be able to finance terrorist activities, manipulate the market through overpricing, and cut off certain consumers from resources. The provision of training and logistics support and a gradual move toward cooperation with countries with a smaller share of the energy market but a large potential is crucial for NATO members. The main objective is to sustain military activity and ensure the development of countries that rely on imports. Therefore, eliminating terrorist attacks in the energy sector should provide the basis for developing anti-terrorist strategies and increasing the Alliance's resilience.

Select Bibliography

Alelyani, Salem, and Harish Kumar. "Overview of Cyberattack on Saudi Institutions." *Journal of Information Security and Cybercrimes Research* 1, no. 1 (2018).

Berahab, Rim. *Global Trends in the Energy Sector and Their Implication on Energy Security in NATO's Southern Neighborhood*. Madrid: Elcano Royal Institute, September 8, 2020. https://media.realinstitutoelcano.org/wp-content/uploads/2021/10/ari103-2020-berahab-global-trends-energy-sector-and-implication-on-energy-security-in-natos-southern-neighbourhood.pdf.

Lee, Chia-yi. "Why Do Terrorists Target the Energy Industry? A Review of Kidnapping, Violence and Attacks against Energy Infrastructure." *Energy Research & Social Science* 87 (2022).

Shea, Jamie. "Energy Security: NATO's Potential Role." NATO Review (website). September 1, 2006. https://www.nato.int/docu/review/articles/2006/09/01/energy-security-nato-s-potential-role/index.html.

Stegen, Karen Smith, Patrick Gilmartin, and Janetta Carlucci. "Terrorists versus the Sun: Desertec in North Africa as a Case Study for Assessing Risks to Energy Infrastructure." *Risk Management* 14, no. 1 (February 2012).

Tichý, Lukáš. "The Islamic State Oil and Gas Strategy in North Africa." *Energy Strategy Reviews* 24 (2019). https://doi.org/10.1016/j.esr.2019.04.001.

— 9 —

Climate Change as a Defining Factor in Allied Military and Counterterrorism Operations

Sabrina Schulz and Marcus Mohlin

ABSTRACT: This chapter addresses the challenges posed by the direct and indirect impacts of climate change on Allied military and counterterrorism operations and the implications of a transition away from fossil fuels for NATO Armed Forces. It explores three dimensions of how climate change impacts military and counterterrorism operations. The focus is on Article 3 (operations), crisis management, cooperative security, and humanitarian aid and disaster relief. The evidence is produced from the existing body of research on climate and security. The findings help NATO military and policy practitioners identify climate risks and design strategies to meaningfully respond to them.[1]

Keywords: climate change, climate security, climate resilience, renewable energy, decarbonization

Introduction

Consensus in academic research and in the security community has emerged over the fact that climate change will affect national, international, and human security in various ways. An increasing body of literature covers the geopolitical, geo-economic and security and social ramifications of the direct and indirect impacts of climate change, including the risks for critical infrastructure. As NATO's 2030 Factsheet, dated June 2021, confirms, "[c]limate change is the defining challenge of our time. The security

[1] The authors would like to extend a thank you to Ms. Linnea Berkhahn-Lindholm and Mr. Edvard Björk, interns at Swedish Armed Forces Headquarters, who helped research and draft parts of the chapter.

implications of climate change are being felt in NATO's neighborhood, be it in the Sahel,Middle East and North Africa, or the Arctic, and within NATO Allied territory. By understanding this challenge and adapting and mitigating, where possible, NATO will be better positioned to fulfill its three core tasks."[2]

Climate change is often described as a "threat multiplier" and destabilizing factor that increases the risk of conflict with direct and indirect impacts on security, critical infrastructure, and military operations.[3] Despite this vulnerability, there are still few studies on the impacts of climate change on military infrastructure and operations.[4] An increase in military operations is expected in regions where climate impacts add to an already fragile context. These operations include counterterrorism and humanitarian aid and disaster relief (HA/DR) operations, which will have consequences for military planning, operations, and the role of the Armed Forces.[5] As NATO's Climate Change and Security Action Plan (June 2021) confirms, "[c]limate change is one of the defining challenges of our times. It is a threat multiplier that impacts Allied security in the Euro-Atlantic area and the Alliance's broader neighborhood."[6] The term "threat multiplier" applies both to Article 3 (national security and civil preparedness) and Article 5 (collective defense) of the North Atlantic Treaty. This chapter focuses on Article 3 challenges.

The risks and threats of climate change have been made clear by science. According to the most recent Sixth Assessment Report: Climate Change 2022 (AR6) by the International Panel on Climate Change (IPCC), "[c]limate change is a threat to human well-being and planetary health. Any further delay in concerted anticipatory global action on adaptation and mitigation will miss a brief and rapidly closing window of opportunity

[2] "Factsheet: NATO 2030" (Brussels: NATO, June 2021), https://www.nato.int/nato_static_fl2014/assets/pdf/2021/6/pdf/2106-factsheet-nato2030-en.pdf.

[3] Kathleen A. Mahoney-Norris and Derek S. Reveron, "Climate Change and Environmental Security," in *The Oxford Handbook of U.S. National Security*, ed. Derek S. Reveron, Nikolas K. Gvosdev, and John A. Cloud (New York: Oxford University Press, 2017), 1–2, https://academic.oup.com/edited-volume/28069.

[4] "Department of Defense (DoD) Climate Risk Analysis" (Washington, DC: DoD, Office of the Undersecretary for Policy, 2021), 8, https://media.defense.gov/2021/Oct/21/2002877353/-1/-1/0/DOD-CLIMATE-RISK-ANALYSIS-FINAL.PDF.

[5] Kate Cox et al., A *Changing Climate: Exploring the Implications of Climate Change for UK Defence and Security* (Santa Monica, CA: RAND Corporation, 2020), 8–11, https://www.rand.org/content/dam/rand/pubs/research_reports/RRA400/RRA487-1/RAND_RRA487-1.pdf.

[6] "NATO Climate Change and Security Action Plan," NATO (website), June 14, 2021, https://www.nato.int/cps/en/natohq/official_texts_185174.htm.

to secure a livable and sustainable future for all." Many of these threats referred to by the IPCC apply to human security.[7]

Based on the IPCC's report, various climate impacts also directly relate to military security, infrastructure security, and operations, including counterterrorism operations. Accordingly, science clarifies that "[k]ey infrastructure systems including sanitation, water, health, transport, communications and energy will be increasingly vulnerable if design standards do not account for changing climate conditions."[8] This vulnerability also applies to military infrastructure and NATO's seven baseline requirements. Climate impacts will make infrastructure more vulnerable to attacks by non-state armed groups and terrorists. Adapting military infrastructure and operations to climate risks will be decisive in maintaining the operability and readiness of the armed forces.

This chapter goes beyond the direct impacts of climate change and examines its indirect and cascading effects in an operational and a strategic sense. The authors argue that Allied security and operations are affected by the impacts of climate change along three dimensions.

Three Dimensions of Climate Change Impacting Allied Security and Operations

The first dimension of how climate change affects military security and operations, including counterterrorism operations, concerns the direct impacts of climate change (for example, changing weather patterns and the increased frequency and severity of extreme weather events). Changing weather patterns, rising air and water temperatures, rising sea levels, hurricanes, increased precipitation, flooding, and drought and related levels of dust will require new approaches to ensure the resilience of military and civilian critical infrastructure and maintain the operability and readiness of the armed forces. This problem also applies to situations where non-state armed groups and terrorists may try to take advantage of weather-related instability and chaos. Weather impacts on military operations (WIMO) will affect armed forces beyond infrastructure and require new approaches in doctrine, training, equipment, and organization.

[7] United Nations Development Programme (UNDP), *2022 Special Report: New Threats to Human Security in the Anthropocene: Demanding Greater Solidarity* (New York: UNDP, 2022), https://www.un-ilibrary.org/content/books/9789210014007/read.

[8] "Climate Change 2022: Impacts Adaptations and Vulnerability, Summary for Policymakers" in *IPCC Sixth Assessment Report* (Cambridge, UK: Cambridge University Press, 2022), 12–13.

The second dimension of the impacts of climate change on Allied security and operations covers the indirect impacts and the cascading second- and third-order effects of climate change. This dimension is, first, about conflict in regions of the world most affected by climate change. For example, because of sea level rise or drought-related harvest failures, people in the affected regions might be displaced and forced to migrate. Migration and the increase of climate refugees, who migrate to new locations due to the effects of climate change in their home region, can add to instability in already fragile geographies. Further, climate impacts social unrest due to food insecurity and hunger when agricultural land is no longer arable. The failure of governments to address these challenges can lead to political instability and violent conflict, especially when large parts of the population lose their income and property. The emerging governance vacuum can also make it easier for armed criminals and extremist groups, including terrorists, to radicalize parts of society and recruit fighters.

An additional cascading effect of climate change is the long-term impacts on the natural physical environment. For example, when ice shields in the Arctic melt at an accelerated pace, access to resources at the seabed becomes possible, which can trigger conflict over access rights. In addition, new sea routes that emerge as the sea ice melts create new opportunities for terrorist activities, trafficking, and other criminal activities, as policing these areas is nearly impossible. These examples illustrates that climate change will add further complexities to national security, including defense against terrorism.

The third dimension of the impacts of climate change on Allied security and operations concerns the possible future requirements when Allied forces "go green." This phase starts when NATO troops transition from traditional fossil fuels to alternatives to reduce their carbon footprint and strengthen their strategic and tactical independence from fossil fuels. Such a requirement to decarbonize—likely driven by markets and government regulation—will affect Allied forces and operations in terms of logistics and capabilities. This foreseeable shift will cause implications for tactical and operational capabilities.

Another strategic implication of climate change impacting the military is the shift away from fossil fuels toward renewable sources of energy (RES). This transition has implications for the economic model of fossil-fuel exporting states, as state revenues will be at risk when the global demand for fossil fuels decreases. The destabilization of governments in the wake of a possible economic crisis can have significant ramifications for regional geostrategic balance and Allied security. At the same time, the demand for new raw materials (such as selenium, gallium, and polysilicon for solar-PV modules or cobalt and lithium for lithium-ion batteries) to produce infrastructure for RES and batteries for electric vehicles (EVs) raises strategic challenges as access to these markets for raw materials needs to be secured. It entails a shift from one set of resources to another, inevitably leading to competition over controlling the new geographies where the raw materials are located. The energy security chapter in this handbook deals with these challenges in depth.

This chapter, instead, dedicates a case study to the strategic entanglements and security threats created by the dependence on imported fossil fuels, in this case, natural gas from Russia. The Russian war of aggression on Ukraine in 2022 showed that only a swift transition from fossil fuels to RES in Europe could reduce the energy security risks emerging from the dependence on Russian gas.

From Climate Change as a Threat Multiplier to a Threat Response

The notion of climate change as a threat multiplier is not new. It has been recognized in literature and political discourse since the early 2000s. Only now is the strategic community starting to study the implications for Allied armed forces in depth and develop concepts to prepare for and adapt to the new security environment. In 2007, the European Council called on High Representative for the Common Foreign and Security Policy Javier Solana to consider the issue. His report concluded that climate change should be seen as "a threat multiplier which exacerbates existing trends, tensions and instability."[9] In March 2008, the UK's National Security Strategy referred to climate change as "potentially the greatest threat to global stability and security, and therefore to national security."[10] Moreover in an October 2009 speech, NATO Secretary General Anders Fogh Rasmussen emphasized that "the security implications of climate change need to be better integrated into national security and defense strategies."[11] Today, the United States and the UK armed forces are among those Allies with the most advanced concepts and doctrines when it comes to dealing with the security implications of climate change.

[9] *Climate Change and International Security: Paper from the High Representative and the European Commission to the European Council* (Luxembourg: Publications Office of the European Union, 2008), https://data.europa.eu/doi/10.2860/50106.

[10] UK Ministry of Defence, *The National Security Strategy of the United Kingdom: Security in an Interdependent World* (London: UK Ministry of Defence, 2008).

[11] "The National Security Implications of a Changing Climate," White House (website), May 2015, https://obamawhitehouse.archives.gov/sites/default/files/docs/National_Security_Implications_of_Changing_Climate_Final_051915.pdf.

During the last decade, climate security became a fringe topic among the defense, foreign, and development policy communities. International institutions largely failed to act on climate change. Foreign and security policymakers were instead focused on such issues as events in the Middle East and North Africa (MENA) region following the Arab Spring uprisings in 2011, the advance of ISIS in Iraq and Syria in 2014, Brexit, and Donald J. Trump's victory in the 2016 US presidential election. It was only in 2019 that climate change returned to the global security agenda when the Dominican Republic Presidency of the UN Security Council organized a full-day debate on the UN Security Council, with over 80 member states speaking. As UN Under Secretary General for Political Affairs Rosemary A. Di Carlo made clear, "[m]ost important, for all of us, is the recognition that deeds must follow words. Major armies and businesses have long recognized the need to prepare for climate-related risks, rightfully assessing climate change as a threat multiplier. We cannot lag behind."[12]

As the IPCC's 2022 report confirms, "[w]idespread, pervasive impacts to ecosystems, people, settlements, and infrastructure have resulted from observed increases in the frequency and intensity of climate and weather extremes, including hot extremes on land and in the ocean, heavy precipitation events, drought and fire weather."[13] Climate change is already affecting every region of the Earth. However, its impacts are experienced differently depending on the exposure of humans, infrastructure, and arable land to new climactic conditions and the ability of a region to adapt. While urban areas are particularly exposed to heat waves, flooding, and rising sea levels, their ability to adapt is usually weak. The situation is worse in many developing countries that tend to be the most affected by climate impacts but have the least resources to cope with the effects.

The most recent scientific data suggests that the climate system can potentially run out of control. For example, the planet's poles are exposed to increasing temperatures, which can lead to knock-on effects in the climate system. As sea ice melts with its high albedo effect, it exposes the darker surface of the water, which will absorb heat much more quickly than ice contributing to warmer ocean temperatures and the further destabilization of the ice sheets. The West Antarctic and Greenland ice sheets are melting at an accelerating rate. Future generations might, therefore, already be committed to sea-level rises of around 10 meters, though that would happen over several

[12] "Momentum Builds for UN Security Council Action on 'Multitude' of Climate-related Threats," Planetary Security Initiative (website), January 21, 2019, https://www.planetarysecurityinitiative.org/news/momentum-builds-un-security-council-action-multitude-climate-related-threats.

[13] "Climate Change 2022: Impacts Adaptations and Vulnerability, Summary for Policymakers," 11.

hundred years. As the rate of melting sea ice accelerates, this process may be sped up. In March 2021, scientists registered record high temperatures in Antarctica of more than 70 degrees Fahrenheit (40 degrees Celsius) warmer than average, which is unprecedented. Simultaneously, the Arctic was more than 50 degrees Fahrenheit (30 degrees Celsius) warmer than average.[14] A case study on the Arctic in section 3 of this chapter will elaborate on the security implications of this development.

Thus, climate change is no longer solely an environmental challenge. On the contrary, climate change has become a high-priority security risk for many countries, including those in NATO. Consequently, NATO, as well as some countries, are developing strategies and concepts on how to integrate climate change into operations. The concluding section of this chapter on "threat response" will summarize the recommendations across the three dimensions mentioned above and briefly present NATO's Climate Change and Security Action Plan.

Direct Impacts of Climate Change on the Resilience of Military Forces and on Critical Infrastructure

The following section deals with the direct impacts of climate change (such as extreme temperatures and the increasing frequency of extreme weather events that have affected, and will increasingly affect, the resilience of military and civilian critical infrastructure and the performance of the armed forces, including in counterterrorism operations and defense against terrorism. Climate change will not wait until we are ready for its impacts. Therefore, new required measures will be described in more detail in the next section. Syncing the policies of NATO member states and their respective armed forces with the Alliance's seven baseline requirements will make each country's military more resilient and able to operate in a climate-altered world.

Sections 1 and 3 in this handbook cover the role of critical infrastructure (CI) and critical energy infrastructure (CEI) in depth and demonstrate that protecting CI and CEI is a core national security task. A breakdown or malfunction of CI would create long-term supply bottlenecks, the disruption of public safety, and potentially the inability of armed forces to operate. Critical infrastructure and CEI are vital for the functioning of a state and an economy and have, therefore, always been a potential target for adversaries.

[14] Caitlin Kaiser and Angela Fritz, "Extraordinary Antarctica Heatwave, 70 Degrees above Normal, Would Likely Set a World Record," *CNN* (website), March 28, 2022, https://www.cnn.com/2022/03/28/weather/antarctica-world-record-high-temperature-anomaly-climate/index.html.

They play a key role in contemporary warfare and when dealing with terrorist threats.[15] This chapter addresses the implications of climate impacts for CI and CEI. Many of the insights generated apply to the vulnerability of infrastructure to terrorist attacks.

As the UK's Ministry of Defence (MoD) recognizes in its 2021 Climate Change and Sustainability Strategy, climate change has an impact on armed forces as it will "affect the way we protect, operate and fight—from the warming of our oceans through to the increased requirement for humanitarian and disaster relief."[16] It clearly acknowledges that "the way we conduct defense and the tasks we are called on to carry out will be forced to change as we adapt to new environmental conditions."[17] Thus, the UK military is aligning itself with the most recent scientific findings by the IPCC.

Weather Impacts on Military Operations and Climate-altered Operations

Scientific findings require armed forces operating in a climate-altered world to increase their resilience and adapt to climate change. Weather impacts on military operations (WIMO) affect mission performance, and climate change–induced extreme weather events will increase in frequency and severity in the future. Many of these challenges apply to theaters characterized by terrorist threats or in counterterrorism operations. For example, with extreme weather events such as flooding, Allied forces' ability to use existing infrastructure on the ground and mobility could be severely limited. Other areas likely to be affected are intelligence gathering, surveillance, target acquisition, and tactical reconnaissance due to the increase of relative humidity and cloudiness in the atmosphere. Many satellites depend on visual wavelengths, but the ability to detect objects under the cloud cover decreases naturally in dense cloudiness. Air and naval assets are particularly weather sensitive. For example, high wind speed or high wave height impair the ability to operate from certain types of platforms.

[15] Arnold C. Dupuy, "Energy Security in the Era of Hybrid Warfare," NATO Review (website), January 13, 2021, https://www.nato.int/docu/review/articles/2021/01/13/energy-security-in-the-era-of-hybrid-warfare/index.html; and Heiki Jakson et al., *Energy in Irregular Warfare*, 2017 Energy in Conflict Series (Vilnius, LT: NATO Energy Security Centre of Excellence, 2017), https://enseccoe.org/data/public/uploads/2017/05/irregular_warfare_176x250mm_20170526.pdf, 12–13.

[16] "Ministry of Defence Climate Change and Sustainability Strategic Approach (Accessible Version)," UK Ministry of Defence (website), March 30, 2021, https://www.gov.uk/government/publications/ministry-of-defence-climate-change-and-sustainability-strategic-approach/ministry-of-defence-climate-change-and-sustainability-strategic-approach-accessible-version.

[17] "Ministry of Defence Climate Change."

The resilience of armed forces will have to be defined in a new way, go beyond definitions around civilian preparedness, and include the entire range of measures armed forces must introduce to adapt to a new operating environment. NATO's seven baseline requirements for national resilience are key guidelines for a new definition of resilience against the background of the challenges posed by climate change and its impacts:[18]

- Assured continuity of government and critical government services
- Resilient energy supplies
- Ability to deal effectively with uncontrolled movement of people
- Resilient food and water resources
- Ability to deal with mass casualties
- Resilient civil communication systems
- Resilient civil transportation systems

These baseline requirements for national resilience make changes in the following areas necessary: concepts and doctrine, training, personnel, infrastructure, equipment, information, organization, logistics, and interoperability.

Concepts and doctrine must include guidelines on mainstreaming climate change in decision-making processes and minimizing climate risk to military infrastructure and operations. Climate risk must become an integral to concepts and doctrine to enable armed forces to operate in a climate-altered world. For instance, concepts and doctrines will have to define how the military can best support the government when responding to extreme weather events in the context of counterterrorism and humanitarian assistance and disaster relief (HA/DR) operations. With an increasing occurrence of weather extremes, demands on already exhausted forces to assist civilian authorities and emergency services with manpower, niche capabilities, and vehicles will rise.

[18] "Resilience, Civil Preparedness and Article 3," NATO (website), September 20, 2022, https://www.nato.int/cps/en/natohq/topics_132722.htm.

As the next section in this chapter will show, there is also a link between climate impacts and violent conflict in fragile contexts and low-income and developing countries. The connection between environmental factors and armed conflict will increasingly have to be considered when planning future peacekeeping and peace enforcement operations. For example, climate impacts such as drought can enable criminal activities like illegal logging, which might require a focus on constabulary operations.[19]

As Russia's war of aggression in Ukraine shows, food can easily become the most important commodity that needs to be protected along sea lines, especially when crop failures increase worldwide due to climate change. Therefore, securing supply chains for food and other vital goods will require more attention, changed assumptions about the reach and sustainability of defense capabilities, and a shift in the focus of national interest and doctrines.[20]

Training is vital to prepare for a world impacted by natural disaster and extreme weather events. The armed forces must understand how future combat and noncombat operations will be affected by climate change. Training must continually evolve to prepare servicemembers for climate impacts and enable them to operate in extreme conditions.[21] The same applies to medical and first-aid training, engineering, search and rescue, and evacuation skills. At the same time, military training can become more challenging as severe weather events may impact the timing and location of training activities. Moreover, challenging and prolonged operations due to climate impacts constitute a risk to physical security, which also needs to be addressed in a training context.[22]

Personnel may need to work in altered environmental conditions and climate-degraded areas more often, which may affect physical and mental health.[23] For example, higher temperatures due to climate change can affect the transmission, spread, and geographical reach of vector-borne infectious diseases. The growing spread and geographical reach of infectious diseases, in turn, can put increased pressure on personnel, decrease the armed forces'

[19] Clive Murgatroyd, "Defence in a Changed Climate," *RUSI Journal* 153, no. 5 (November 25, 2008): 30–31, https://www.tandfonline.com/doi/full/10.1080/03071840802521895.

[20] Murgatroyd, "Defence in a Changed Climate," 30.

[21] Department of the Army (DA), *United States Army: Climate Strategy* (Washington, DC: Office of the Assistant Secretary of the Army for Installations, Energy and Environment, February 2022), 14–16, https://www.army.mil/e2/downloads/rv7/about/2022_army_climate_strategy.pdf.

[22] Cox et al., *Changing Climate,* 10.

[23] Cox et al., *Changing Climate,* 10–11.

operational ability, and increase the need for individual medical assistance, protective equipment, and vaccinations. Increased rainfall could expose service personnel to risks from waterborne diseases.

Infrastructure will be increasingly vulnerable to climate-related events (such as flooding, wildfires, storms, and hurricanes). The operational use of physical, digital, and communication infrastructure, vital for successful mission preparedness and readiness, will be increasingly at risk. The infrastructure of military bases, in particular, has to be adapted to climate impacts and become more resilient. Thus, investments in climate-resilient infrastructure will be essential for the success of military operations.[24]

Civilian infrastructure that supplies military operations can also indirectly put military operations at risk. Resilient infrastructure and supply chains, including for energy, which can withstand extreme weather events and the ability to operate in a climate-altered world will therefore be vital.[25] When climate impacts affect military installations, local communities that depend economically on these facilities may also experience knock-on effects.[26]

Equipment must be fit for an evolving operating environment, including in more extreme weather and HA/DR operations against the background of degraded infrastructure. Higher temperatures, increased wind speed, wave height, and cloudiness will increasingly affect equipment performance and may impair military operations.[27] For example, high temperatures during military operations in Afghanistan reduced the capacity of helicopters for airlift and the ability to transport essential equipment and supplies. Similar equipment failures are possible in theaters with exposure to dust, storms, and flooding and need to be addressed.[28] Investment in resilient equipment will be key in the future. Additionally, a potential expansion of security operations to fight terrorism while also supporting HA/DR operations might increase the need for engineering equipment, medical care, and helicopters or boats in the case of flooding.

[24] "DoD Climate Risk Analysis."

[25] DoD, *DoD Draft Climate Adaptation Plan*, *Report Submitted to National Climate Task Force and Federal Chief Sustainability Officer* (Washington, DC: Office of the Undersecretary of Defense, Acquisition and Sustainment, September 1, 2021), 12–13, https://www.sustainability.gov/pdfs/dod-2021-cap.pdf.

[26] Cox et al., *Changing Climate,* 11–12.

[27] *DoD Draft Climate Adaptation Plan*, 9–10.

[28] Cox et al., *Changing Climate*, 13.

Information, specifically more accurate, defense-specific meteorological forecasting, will be needed to understand better the impacts of climate change on military operations, personnel, equipment, and geographic regions. Data are also increasingly important to assess the risk of conflict or the need for HA/DR operations as a direct or indirect result of climate impacts. NATO members can then take action to prevent, stabilize, or contain a crisis. Data from hydrographic, geographical, and meteorological services could help forecast extreme weather events and their impacts, including for military theaters of operation.

Organization will probably have to be adjusted as new military activities and roles are defined as a response to climate impacts. A potential additional role for the armed forces could be increased support in HA/DR operations, though a clear division of labor with civilian forces would be necessary. Additional civil preparedness and resilience tasks would impact the conduct of military operations, so dedicated climate emergency forces throughout NATO could become an option.

Logistics and the maintenance of climate-resilient supply chains are vital functions and require resilient infrastructure and equipment. Weather extremes and rising temperatures will increase the need for reliable supply chains for critical goods, including water, medicine, and fuel. To increase resilience in theater, lowering energy use and optimizing logistical support requirements will be key.[29] Additionally, building resilient logistics requires a stress test of supply chains. Emergency plans are necessary to protect critical supply chains and components.[30]

Interoperability refers to the ability to act coherently and effectively to achieve tactical, operational, and strategic objectives. Climate-related emergencies requiring military support rely on a coordinated response by various military and civilian actors. At the same time, if Allies are affected by natural disasters and climate impacts, their ability to contribute to existing or emerging Alliance activities and operations might be affected.[31]

Climate change requires Allies to adapt missions, operations, and infrastructure and leverage all relevant information, methodologies, technologies, and approaches in close collaboration with multiple civilian and military actors. NATO's role could be to develop and agree to standards

[29] *DoD Draft Climate Adaptation Plan*, 16–17.

[30] Cox et al., *Changing Climate*, 13.

[31] Cox et al., *Changing Climate*, 15–16.

and technologies that enhance resilience, improve interoperability, and enable knowledge-sharing. Resilience requires civil preparedness and military capacity. There has been an increase in recent years of ownership of CI by the private sector. Thus, greater cooperation between public and private actors will be needed to maintain operability during disasters.

To conclude, NATO's seven baseline requirements for resilience, energy supplies, and transportation provide an excellent framework for developing a meaningful and effective response to the challenges of climate change for the armed forces, particularly counterterrorism operations. The armed forces must maintain the ability to operate in a climate-altered world, likely characterized by frequent HA/DR operations and widespread constabulary operations in support of international and national mandates, requiring new doctrines/concepts, training, capable personnel, resilient infrastructure, appropriate equipment, information on meteorological conditions, new organizational structures, reliable logistics, and interoperability with partners and Allies.[32] This goal requires a new framework and methodologies to optimize and adapt the lines of effort to mitigate and manage the risks of climate change and to create resilient armed forces.[33]

Case Studies on the Direct Impacts of Climate Change on the Resilience of Military Forces and Critical Infrastructure

The following examples illustrate how resilience needs to be improved across various types of civilian and military infrastructure to withstand the effects of climate change on civil preparedness and military capacity.

Hurricane Sandy

Hurricane Sandy, which struck the United States in October 2012, was one of the most expensive storms on record, and its intensity has become part of a "new normal." To date, infrastructure has been designed based on the assumption that a future climate would be much the same as today.

[32] Murgatroyd, "Defence in a Changed Climate," 30–31.

[33] Murgatroyd, "Defence in a Changed Climate," 32–33.

This assumption no longer holds as "climate bands are becoming outdated, leaving infrastructure operating outside of its tolerance levels."[34]

Consequently, CI assets are facing direct physical threats with significant cascading effects for those relying on their services. According to a study by the McKinsey Global Institute, "[a] failure to adapt by not taking climate change into account in the design, construction, and maintenance of infrastructure assets will not only cause costs to owners and operators but will leave entire communities exposed and vulnerable. Adaptation can deliver a strong return both by reducing costs from climate-related damage to the infrastructure itself and by avoiding significant knock-on effects in wider society."[35] Thus, investing in new and retrofitting existing infrastructure will be essential building block sin enhancing CI resilience. The vulnerability of CI to attacks by irregular forces and terrorists increases in situations where severe weather events create chaos, which adversaries can easily exploit.

Hurricane Florence

In 2018, Hurricane Florence caused catastrophic damage to the Carolinas and exemplified the wider operational risks of natural disasters. The storm heavily impacted many military installations, and beyond the cost of climate-related damages, it delayed the certification of the 22nd Marine Expeditionary Unit for overseas deployment.[36] The time required for repair degraded the military's combat power for some time. This problem demonstrates that more frequent extreme weather events might make it too expensive and impractical to maintain military installations and infrastructure in certain areas (such as on vulnerable coastlines). At the very least, their resilience needs to be increased to maintain operational readiness.[37] Consequently, climate resilience and contingency plans need to be developed for every military installation to prevent major damage and enable the continuity of operations in case of extreme weather events.

[34] Jonathan Woetzel et al., "Will Infrastructure Bend or Break Under Climate Issues?," McKinsey Global Institute (website), August 19, 2020, https://www.mckinsey.com/business-functions/sustainability/our-insights/will-infrastructure-bend-or-break-under-climate-stress.

[35] Woetzel et al., "Will Infrastructure Bend or Break under Climate Issues?," 9.

[36] Bruce A. Stein et al., *Climate Adaptation for DoD Natural Resource Managers: A Guide to Incorporating Climate Consideration into Integrated Natural Resource Management Plans* (Reston, VA: National Wildlife Federation, May 17, 2019), 9.

[37] Cox et al., *Changing Climate*, 9.

Hurricane Michael

Hurricane Michael exemplifies the need to prepare for climate impacts on military training. After the hurricane, Tyndall Air Force base lost the premier simulator for the F-22, and the training facility was unusable for several months. As recovery efforts began, the F-22 fleet redistributed Tyndall personnel, aircraft, and equipment to other locations. The hurricane affected the training of F-22 pilots, which exemplifies the need to prepare for climate impacts to military training. Damages to the base amounted to billions of dollars. During the rebuild, the design wind speed was based on the Florida building code for a high-velocity hurricane zone. The extent of the damage caused and the decision in favor of a more resilient base reconstruction show the importance of preparing for climate impacts on military infrastructure.[38]

2011 Earthquake and Tsunami

The 2011 earthquake and tsunami east of Honshu Island exemplified the need for interoperability and concept considerations. The earthquake created a tsunami that devastated Japan's eastern coast. Although this natural disaster was not linked to climate change, similar impacts could also occur due to climate-related extreme weather events. In addition, the case study demonstrated the vulnerabilities created by nuclear power as a high-risk energy source and the need to consider a renewables-based energy system from a security, public safety, and resilience point of view.

An estimated 1.4 million households lost access to water, and 1.25 million homes were cut off from electricity. The number of displaced citizens amounted to over 500,000.[39] The destruction of communications infrastructure inhibited an accurate estimation of the extent of the damage. Other infrastructure was severely damaged, which, together with cold weather and snow, paralyzed transportation, and relief efforts. The reactor cooling systems at several units of the Fukushima Daiichi nuclear power plant failed, resulting in several explosions and evacuations. The earthquake and the tsunami killed almost 16,000 people and injured over 5,000. Japan estimated the reconstruction cost to be around $300 billion.[40] US armed forces played an important role and cooperated with other US government agencies,

[38] *DoD Draft Climate Adaptation Plan*, 11.

[39] "Millions without Food, Water, Power in Japan," *NBC News* (website), March 1, 2011, https://www.nbcnews.com/id/wbna42044293.

[40] Yasufumi Saito, "Japan's Tsunami and Nuclear Disaster Unleashed a $300 Billion Effort to Rebuild a Hinterland," *Wall Street Journal* (website), March 10, 2021, https://www.wsj.com/articles/japans-tsunami-and-nuclear-disaster-unleashed-a-300-billion-effort-to-rebuild-a-hinterland-11615377375.

particularly the State Department and the Department of Energy. At the peak of the operation, approximately 24,000 personnel, 189 aircraft, and 24 Navy vessels were deployed.[41]

This disaster response effort illustrated the array of capabilities the military can bring to complex disasters. As discussed earlier, more frequent weather extremes will force the armed forces to operate in disaster-stricken areas. Japan is a key ally of the United States, with considerable capabilities of its own, which made it easy for the United States to take a supporting role. Existing concepts were not tailored to supporting a technologically advanced ally, as most HA/DR operations take place in developing countries and create some problems given different operating cultures. This disaster demonstrated the need for resilient energy supply, how to deal with the uncontrolled movement of people, resilient water resources, resilient civil communications systems, and resilient transportation systems, which are part of NATO's seven baseline requirements. The operation also highlighted the ability to cooperate with a non-NATO ally during crises, which creates a greater need for concept development and interoperability.[42]

Climate Change as a Threat Multiplier: Indirect Impacts of Climate Change Impacting (Human) Security

This section deals with the far-reaching indirect impacts or second- and third-order effects of climate change that severely undermine human security, particularly the Global South. NATO armed forces must be prepared for HA/DR, counterterrorism, and peace and stability operations in regions in its immediate vicinity where climate impacts shape the physical, operational, and wider strategic and political environment. The geographical occurrence of most impacts of climate change will primarily concentrate on the Global South. In response, the focus of academic research and policy debates on the so-called climate-security nexus has mostly been on fragile contexts and low-income and developing countries. Figures by the Stockholm International Peace Research Institute (SIPRI) illustrate the complex interlinkages between climate change and threats and risks to human and military security. Accordingly, "as of December 2020, 10 out of 21 ongoing United Nations (UN) peace operations were located in countries ranked as most exposed to climate change. Six of the 10 biggest

[41] Jennifer D. P. Moroney et al., *Lessons from Department of Defense Disaster Relief Efforts in the Asia-Pacific Region* (Santa Monica, CA: RAND Corporation, 2013), 86–88, https://www.rand.org/pubs/research_reports/RR146.html.

[42] Moroney et al., *Lessons*, 86–88, 97–98.

UN peace operations (by total international personnel) were in countries ranked most exposed to climate change."[43]

Thus, the challenges and recommendations for HA/DR operations in the previous section mainly apply to these regions of the world. This short section illustrates the logic of violence and conflict in these climate-exposed regions. According to the 2022 United Nations Development Program (UNDP) Special Report on Human Security, "[v]olatility in weather patterns, shocks to food supply and distribution, and land and resource scarcity—typically interacting with horizontal inequalities and contestation of political power—have all been linked to heightened conflict risks."[44] This point implies that the climate-conflict nexus applies in particular to countries depending on rain-fed agriculture and with low economic diversification.[45]

With their large share of employment in the agricultural sector, Ghana and Ethiopia illustrate how climate variability has reduced income and increased food insecurity.[46] Research studies illustrate how climate impacts such as the destruction of crops as a consequence of extreme weather events—drought and desertification of farmland as well as flooding—lead to higher food prices and food insecurity.[47] Food insecurity, in turn, can lead to increased displacement and migration from rural regions to cities. As pressure on natural resources, basic infrastructure, housing and the job market at the destination rises, the risk of community-based violence and conflict increases, too, because migrants compete with the local population over access to scarce resources.[48]

Increasing parts of the population may also become more vulnerable to radicalization through extremist groups. Local armed and criminal groups, including extremists and terrorists, may make strategic and tactical use of these circumstances. For instance, they may attempt to gain more control over natural resources and arable land to exploit these, or they may expand their recruitment pools as the population struggles with hunger and loss

[43] Florian Krampe, "Why United Nations Peace Operation Cannot Ignore Climate Change," Stockholm International Peace Research Institute (SIPRI) (website), February 22, 2021, https://www.sipri.org/commentary/topical-backgrounder/2021/why-united-nations-peace-operations-cannot-ignore-climate-change.

[44] UNDP, *2022 Special Report,* 54.

[45] UNDP, *2022 Special Report,* 55.

[46] UNDP, *2022 Special Report,* 52.

[47] Krampe, "United Nations Peace Operation."

[48] Rafael Reuveny, "Climate Change-induced Migration and Violent Conflict," *Political Geography* 26, no. 6 (August 2007): 656–73, https://www.sciencedirect.com/science/article/abs/pii/S0962629807000601?via%3Dihub.

of livelihood.[49] As a recent UNDP report on the interplay between climate change and violent extremism states, “fragile and natural-resource constrained contexts can provide fertile ground for violent extremist groups to flourish and extend their reach, particularly, where governance and institutions are weak and may not be able to respond, the COVID-19 pandemic serving also to highlight gaps in response.”[50]

Importantly, the inability of governments to address climate impacts adequately (such as food and water security) can undermine a government’s legitimacy and lead to governance vacuums that these groups can easily exploit. For the same reason, climate impacts can undermine peace and stability operations and disarmament, demobilization, and reintegration (DDR) efforts in post-conflict situations, which can reignite a conflict and generate power vacuums.[51]

It is not climate change triggering conflict, but the “interlinkage with structural development challenges, socioeconomic-political conditions and horizontal inequalities with attendant power imbalances that tends to trigger conflict,” as the UNDP Special Report on Human Security points out.[52] This logic is well illustrated by the UN Multidimensional Integrated Stabilization Mission (MINUSMA) in Mali, where climate impacts have affected natural resource-based livelihoods and severely undermined human security in a context of conflict and weak governance. These complex interactions between climate change, weak governance, low levels of economic development, and inequality hinder MINUSMA’s efforts to support peace and stability in Mali.[53] The UN Multidimensional Integrated Stabilization Mission addresses climate-related security risks (such as natural resource-related conflicts). These efforts, however, are limited by an absence of prioritization, limited capacity within the mission, and coordination challenges between the mission and the UN Country Team.[54]

[49] Florian Krampe and Pernilla Nordqvist, “Climate Change and Violent Conflict: Sparse Evidence from South Asia and South East Asia,” *SIPRI Insights on Peace and Security* 2018, no. 4 (September, 2018), https://www.sipri.org/sites/default/files/2018-09/sipriinsight1804.pdf.

[50] Catherine Wong and Nika Saeedi, *The Climate Security Nexus and the Prevention of Violent Extremism: Working at the Intersection of Major Development Challenges*, United Nations Develoment Programme (UNDP) Policy Brief (New York: UNDP, October 12, 2020).

[51] Nordqvist and Krampe, “Climate Change and Violent Conflict.”

[52] UNDP, *2022 Special Report*, 14, 24.

[53] Farah Hegazi, Florian Krampe, and Elizabeth Smith, “Climate-related Security Risks and Peacebuilding in Mali,” SIPRI (website), April 2021, https://www.sipri.org/publications/2021/sipri-policy-papers/climate-related-security-risks-and-peacebuilding-mali.

[54] Hegazi, Krampe, and Smith, “Climate-related Security Risks.”

Mali is fertile ground for the rise of terrorist groups as they can exploit the security vacuum, the plight of the civilian population, and the fragility of neighboring countries for their purposes. The Sahel is characterized by irregular migration, frequently organized by illegal trafficking rackets promising a safe journey to Europe via Algeria, Tunisia, and Morocco. The cause of migration includes conflict (Mali), political oppression (Eritrea), terrorism (Nigeria), hunger, and extreme poverty across the Sahel. Climate and environmental impacts exacerbate the situation and lead to internal climate displacement and climate migration to other countries.[55]

Another example of the destabilizing effects of climate change is the Lake Chad Basin region, as mentioned in the chapter on energy. The security crisis in the region is characterized by competition over scarce water resources and increased human migration. Continuous terrorist and violent extremist attacks and ethnic, religious, and farmer-herder conflicts drive migration.[56] It affects the riparian countries of Cameroon, Chad, Niger, and Nigeria. The Multinational Joint Task Force (MNJTF) was established in 2012 to combat Boko Haram and other terrorist insurgencies in the basin. Its difficulties in stabilizing the region are not least due to the fact that "terrorists and other violent extremist groups continue to adapt to conditions and exploit vulnerabilities to increase the spread of violence in the Lake Chad Basin."[57] Thus, climate change constitutes an enabling element that terrorists can exploit to their advantage. Terrorist attacks on farms contribute to the existing food insecurity and exacerbate the security situation.[58]

Climate impacts also contribute to the destabilization of other regions on the African continent, including southwest neighborhoods of NATO, comprising West Africa and the adjacent sea areas (and island states) of the Gulf of Guinea and Macaronesia (the marine biogeography of archipelagos from the Azores via the Madeira Group, the Savage Islands,

[55] Serigne Bamba Gaye, *Connections between Jihadist Groups and Smuggling and Illegal Trafficking Rings in the Sahel* (Dakar-Fann, SN: Friedrich Ebert Foundation and Security Centre of Competence Sub-Saharan Africa, 2018), https://library.fes.de/pdf-files/bueros/fes-pscc/14176.pdf; and Kira Vinke, "Sturmnomaden – Wie der Klimawandel Uns Menschen die Heimat Raubt," Bayerische StaatsBibliothek, January 1, 2022.

[56] Osei Baffour Frimpong, *Climate Change and Violent Extremism in the Lake Chad Basin: Key Issues and Way Forward* (Washington, DC: Wilson Center, July 2020), https://www.wilsoncenter.org/sites/default/files/media/uploads/documents/Climate%20Change%20and%20Violent%20Extremism%20in%20the%20Lake%20Chad%20Basin%20Key%20Issues%20and%20Way%20Forward_0.pdf.

[57] Frimpong, *Climate Change and Violent Extremism*, 4.

[58] Frimpong, *Climate Change and Violent Extremism*, 3.

the Canary Islands to Cape Verde).[59] The region exemplifies the cascading effect of climate change, including extremely high risks of drought (particularly across Sierra Leone, Guinea, other coastal areas, and Nigeria), extreme temperatures, flooding, wildfires (particularly in southern Nigeria and Mali), and storm surge in coastal areas.[60] Against the background of accumulating and aggravating security risks in the region, including illegal, unregulated, and unreported (IUU); excessive fishing; transatlantic trafficking of animals and plants, drugs, guns, and humans; and migration from Africa to the Canaries and also across the Atlantic.[61]

Thus, NATO will increasingly have to deal with political instability in regions in its vicinity characterized by the direct or indirect impacts of climate change. These situations may require HA/DR operations or multilateral peace and security operations with a UN mandate in the future, and NATO armed forces have to be equipped for these challenges.

Case Study on Emerging Security Risks and Threats at NATO's Northern Border: Climate Impacts in the Arctic

A different case where the impacts of climate change bring about new security risks and threats is the Arctic. Ice shields are melting at an accelerated pace, opening new unsecured sea routes and creating opportunities for trafficking and other criminal activities, as policing these areas is nearly impossible. In addition, thawing permafrost poses a direct physical threat to military and civilian infrastructure in the Arctic region, including military bases.[62] Infrastructure damage will undermine transport—mainly ice roads, railroad systems, ports, and airfields—communications, logistics, and other essential services, and cost millions of dollars. Moreover, access to resources at the seabed becomes possible, which may lead to a contestation of rights of access.

The opening of new shipping lanes and the construction of seaports in the Arctic region do not increase geopolitical tension. However, in the absence

[59] R. Andreas Kraemer and Ashley McIlvain Moran, "Emerging Theatres: West Africa and Macaronesia," in *NCWES: Sustainable Peace & Security in a Changing Climate: Recommendations for NATO 2030. A Report for the NATO Secretary General from the North-Atlantic Civil-Society Working-Group on Environment and Security*, ed. Ronald A. Kingham and Olivao Lazard (Brussels: Environment and Development Resource Center, 2021), 34–38.

[60] Kraemer and Moran, "Emerging Theatres," 34–38.

[61] Kraemer and Moran, "Emerging Theatres," 34.

[62] Olivia Wynne Houck, "Infrastructure in the Arctic: The Arctic Institute Infrastructure Series," Arctic Institute (website), March 22, 2022, https://www.thearcticinstitute.org/infrastructure-arctic-the-arctic-institute-infrastructure-series/.

of clear and enforceable regulations under international law, particularly the United Nations Convention on the Law of the Sea (UNCLOS), issues such as the rite of passage are not yet resolved. Since policing the new sea routes will be challenging, transnational criminal activities (such as trafficking) will likely increase.

However, new geopolitical tensions can arise from increased military presence and China-Russia cooperation in projects for the Northern Sea Route (NSR).[63] Russia's war of aggression on Ukraine might further contribute to an accelerating militarization of the region.

A military target of choice in the Arctic region could be underwater cables, with their crucial economic significance and function for Allied defense and security. In January 2022, a fiber-optic cable enabling communications between the Norwegian mainland and the Svalbard archipelago was cut. The cable supports the Svalbard Satellite Station, one of two ground stations collecting data from polar-orbiting satellites. While the cause for the disruption is unclear, it demonstrates the vulnerability of cables and other infrastructure undersea. The loss of a single cable could have a disproportionate impact on a country's information warfare capabilities, thereby posing an asymmetric threat.[64]

Going Green: Effects on Operations in Transition Away from Fossil Fuels

This section covers the increasing pressure on armed forces to "go green" against the background of NATO member governments to decarbonize their economies. Many issues covered in this section are elements of NATO's Climate Change and Security Action Plan. They align with the NATO 2030 agenda that commits Allies to reduce GHG emissions from military activities and installations significantly. NATO is also assessing the feasibility of reaching net-zero emissions by 2050. NATO will reflect these issues in its new strategic concept. As the NATO 2030 Factsheet confirms, "[g]reening militaries offers real win-wins, by decreasing dependence on fossil fuel supplies, to improve operational effectiveness."[65]

Such a transition away from fossil fuels will have significant impacts at the operational level. Armed forces must ensure resilient energy

[63] Houck, "Infrastructure in the Arctic."

[64] Alan Cunningham, "Underneath the Ice: Undersea Cables, the Arctic Circle, and International Security," Arctic Institute (website), March 29, 2022, https://www.thearcticinstitute.org/underneath-ice-undersea-cables-arctic-circle-international-security/.

[65] "Factsheet: NATO 2030."

supplies and reliable fuel logistics while lowering their energy use to maintain an operational effect. Against the background of these challenges, joint planning and implementation of an energy transition among NATO Allies and partners would constitute a major advantage. At the same time, the risks and opportunities of an energy transition in the armed forces must be carefully analyzed.

Given the efforts of NATO members to decarbonize their economies, the pressure on armed forces to "go green" is increasing, and regulation may follow. So far, most militaries have not been involved in wider efforts to cut greenhouse gas emissions and achieve climate neutrality, but this is likely to change soon.[66] An energy transition away from fossil fuels in the military will significantly impact tactical and operational capabilities. Thus, it is crucial to understand the risks and opportunities of such a transition.

The energy transition's possible impacts must also be considered in defense planning. Capability planners must assess the potential effects on operational effectiveness. When analyzing the IPCC's scenarios from a defense perspective, it becomes clear the short-term risks of the transition will decrease, and opportunities will increase in the medium and long term.[67] The main challenge for Allied forces during this transition will be maintaining tactical and operational impact. NATO must acknowledge the vulnerabilities of new energy systems toward armed attack and make them more resilient to maintain both national security and the operability of armed forces.[68]

Energy Resilience in Military Operations

Energy resilience is the ability to anticipate, prepare for, adapt, withstand, respond to, and rapidly recover from energy disruption.[69] Greater energy resilience with more energy produced on-site during military operations would make missions more self-sufficient and resilient. Much less fuel will have to be transported to the zones of military operations in the future as the reliance on renewable energy, in particular electricity,

[66] "A Beginner's Guide to Climate Neutrality," United Nations Climate Change (website), February 26, 2021, https://unfccc.int/blog/a-beginner-s-guide-to-climate-neutrality.

[67] Murgatroyd, "Defence in a Changed Climate," 32.

[68] Arnold Dupuy et al., "Energy Security in the Era of Hybrid Warfare," NATO Review (website), January 13, 2021, https://www.nato.int/docu/review/articles/2021/01/13/energy-security-in-the-era-of-hybrid-warfare/index.html.

[69] Alex Beehler and J. E. Jack Surash, "Cutting the Cord to Test Energy Resilience," US Army (website), April 13, 2020, https://www.army.mil/article/234514/cutting_the_cord_to_tst_energy_resilience.

will increase.[70] The potential advantage is that the energy demands of forward operating bases, HR/DR operations, and equipment can be met more easily and contribute to higher tactical and operational self-sufficiency and resilience.[71]

Military installations must have secure and reliable access to energy and water to achieve mission objectives. With rare exceptions, installations today rely on commercial utilities for energy and water. A number of vulnerabilities, both man-made and natural, are associated with dependence on electric grids, gas pipelines, and water systems, which can jeopardize operational and tactical capabilities. Moreover, military installations and their infrastructure and suppliers are known targets for terrorists.[72]

Sources and distribution of electricity supply and logistics and charging capacities also constitute bottlenecks in military operations.[73] The reliance on uninterrupted power supplies might lead to new solutions (such as on-site renewable energy generation, large-scale energy storage, and smart microgrids). Microgrids can operate independently from the regular grid and are, in theory, less vulnerable to terrorist attacks or cyberattacks. However, appropriate cybersecurity protection is currently lacking, ruling out solar PV for microgrids. It is clear, however, that relying on locally produced RES would reduce the need for risky and costly fuel convoys and rear logistics whose vulnerability can be exploited by adversaries and result in many casualties. Reducing dependence on fossil fuels and electrical grids can make military operations more resilient and needs to become an integral part of defense planning.[74]

Energy Logistics and Smart Energy

Fuel logistics and security have been a concern in military operations throughout history.[75] Logistical challenges with energy supplies have negatively affected military operations, as illustrated by General Patton's

[70] DA, *Climate Strategy*, 6-7.

[71] DA, *Climate Strategy*, 13.

[72] Beehler and Surash, "Cutting the Cord."

[73] Joakim Nyman et al., "Planning and Analysis of Charging Infrastructure," RISE (website), n.d., https://www.ri.se/en/what-we-do/expertises/planning-and-analysis-of-charging-infrastructure.

[74] Constantine Samaras, William J. Nuttall, and Morgan Bazilian, "Energy and the Military: Convergence of Security, Economic, and Environmental Decision-making," *Energy Strategy Reviews* 26 (November 19, 2019): 3–6, https://www.sciencedirect.com/science/article/pii/S2211467X19301026?via%3Dihub.

[75] Samaras, Nuttall, and Bazilian, "Energy and the Military," 3.

US 3rd Army running out of fuel during World War II. Patton's Army had pushed across France in a remarkable demonstration of maneuverability, but it was stopped just before the critical West Wall defenses guarding the German border due to a fuel shortage. There is no known example of fuel shortages due to inadequate stocks in France. The problem was fuel distribution.[76]

The security of fuel supplies also heavily affected NATO's operation in Afghanistan. The fuel was delivered mainly by fuel convoys through Pakistan. After the Ṣalālah incident in which 28 Pakistani soldiers were killed, the border was closed, and supply lines had to shift to the Northern Distribution Network, a rail link from Latvia to Uzbekistan, where the fuel was offloaded on trucks and transported across the border to Afghanistan. This change in distribution lines demonstrates the vulnerabilities and difficulties of fuel logistics in military operations.[77]

The vulnerability of rear logistics can be exploited by enemy fighters and terrorist forces and result in many casualties. In 2007, on average, there was one casualty for every 24 fuel convoys in Afghanistan. Reducing energy requirements through innovative technologies represents a significant opportunity to reduce the strategic vulnerability associated with fuel supplies.[78]

NATO exercise Capable Logistician (CL), in 2019, tested innovative solutions to reduce fossil fuel consumption and wastage in military installations and demonstrated the benefits of smart energy in military operations. This exercise showed how innovative energy technologies based on RES could improve operational effectiveness. The exercise drew on several scenarios requiring a smart energy response (such as power cuts, pollution of primary water sources, and diesel contamination). During the exercise, a smart microgrid, constructed to supply energy to camp tents, connected RES to diesel generators that would power up when renewable power was unavailable. The exercise showed how the management and planning of energy flows can be improved in a highly effective manner.[79]

[76] G. W. Berragan, "Higher Command and Staff Course Staff Ride Paper: Who Should Bear Primary Responsibility for the Culmination of Patton's US Third Army on the Moselle in 1944? Are There Lessons for Contemporary Campaign Planning?," *Defence Studies* 3, no. 3 (October 19, 2007): 161, 165, https://www.tandfonline.com/doi/abs/10.1080/14702430308405084.

[77] Samaras, Nuttall, and Bazilian, "Energy and the Military," 5.

[78] Samaras, Nuttall, and Bazilian, "Energy and the Military," 5.

[79] "NATO Tests Smart Energy Technologies at Exercise in Poland," NATO (website), June 3, 2019, https://www.nato.int/cps/en/natohq/news_166827.htm?selectedLocale=en#:~:text=NATO%20tested%20new%20energy%2Dsaving,interoperability%20between%20national%20armed%20forces.

A test deployment of portable solar-power generation systems at several US Marine forward operating bases in Afghanistan during 2010 also reduced the need for diesel generators by more than 90 percent.[80] Diesel generators can operate during harsh conditions without compromising an operation; however, they can also hinder military operations due to the need for fuel supply lines. Hybrid solutions with increased renewable energy generation at forward operating bases can reduce the need to rely on fuel convoys to ensure energy supply.[81] They can decrease reliance on diesel generators and lower the number of fuel convoys, a common target for adversaries. Decreasing the reliance on convoys can also free up personnel accompanying and protecting the convoys and therefore increase the operational effect.[82]

Joint Implementation

It is not clear yet what the most viable long-term options for the "green transition" of the armed forces could be. Russia's war of aggression in Ukraine brought home the fact that a transition away from imported fossil fuels toward RES is urgent. While the short-term transition to alternative fuels, in particular synthetic liquid fuels, is considered technically feasible, it is challenging from a financial and logistical point of view. Therefore, it requires large-scale planning and joint implementation. Allies and relevant partner nations should unanimously decide how to reduce energy use and substitute fossil fuels with RES.

Interoperability is key during the transition. Ideally, infrastructure, new energy sources, and fuel could be used by all NATO members and partners. A shared view on the need for a transition from fossil fuels, a coordinated approach, joint planning, implementation, and the development of intra-alliance standards and common processes is required.[83] Decisions on future sources of power and electricity in the Alliance will likely become politicized as different countries have different energy transition strategies. This decision also applies to a common technology for vehicles (for example, electric vehicles versus fuel cells).[84]

[80] Spencer Ackerman, "Afghanistan's Green Marines Cut Fuel Use by 90 Percent," Wired (website), January 13, 2011, https://www.wired.com/2011/01/afghanistans-green-marines-cut-fuel-use-by-90-percent/.

[81] Samaras, Nuttall, and Bazilian, "Energy and the Military," 4–6.

[82] "NATO Tests Smart Energy."

[83] DA, *Climate Strategy*," 7–11.

[84] Jutta Lauf, Wsewolod Rusow, and Reiner Zimmermann, "Nitrogen Based Propellants as Substitute for Carbon Containing Fuels," in *Energy Highlights,* no. 16 (Vilnius, LT: NATO Energy Security Centre of Excellence, 2021), 5–6, https://www.enseccoe.org/data/public/uploads/2021/11/d1_energy-highlights-no.16.pdf.

Compatibility between Civilian and Military Solutions

In addition to the need for more resilient energy supplies and joint implementation of the relevant solutions, armed forces also need to ensure the operability and readiness of traditional fossil fuel-based technologies. The transition to RES in the armed forces will likely be much slower than the civilian sphere and will rely on fossil-fuel technologies (such as the internal combustion engine) for much longer. It will be crucial that the armed forces maintain the necessary degree of technical competence among engineers, technicians, and mechanics to maintain operational capability. At the same time, the relevant staff needs to be trained to service new types of operational vehicles as different competencies and resources are required.

Case Study on Offshore Wind Power

The expected increase in offshore wind power development requires sound management of the risks offshore wind farms pose to military operations. Offshore wind farms reduce the capacity of radar systems and affect air traffic control and weather forecasting, which impacts national security and defense missions. Offshore wind farms may also adversely impact the quality of data obtained from primary surveillance radars (PSR). Maintaining PSR's capability is vital to obtain a recognized air picture; impaired capacity might reduce the possible range and the time to identify and act on potential aggression, which risks undermining security and military operations at sea and in the air.[85] Thus, the adverse side effects of offshore wind farms on the radar for military and civilian aviation have to be mitigated, so they do not constitute a risk to national security.[86]

[85] *Air Defence and Offshore Wind: Working Together towards Net Zero* (Air Media Centre/HQ Air Command/UK Ministry of Defense, Autumn 2021), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1021252/Air_defence_and_offshore_wind.pdf.

[86] Marju Kõrts, "Role of Wind Farms for National Grids: Challenges, Risks, and Chances for Energy Security," in *Energy Highlights* (Vilnius, LT: NATO Energy Security Centre of Excellence, 2020), 4–6, https://enseccoe.org/data/public/uploads/2021/04/role-of-windfarms-for-national-grids-2020-marju-korts.pdf.

Case Study on Renewable Energy Sources on Forward and Rear Operating Bases

Recent studies on the practicality of RES for expeditionary military operations showed that solar photovoltaic (PV) energy and wind power, on rare occasions, are the most promising renewable energies for use by armed forces. Implementing solar PV on forward-operating bases could reduce the reliance on fossil fuels. The technology has become modular, mobile, transportable, and deployable for remote operations. From a tactical perspective, solar PV provides military advantages as it helps armed forces become more energy self-sufficient, so remote operations could become independent of resupply. It reduces the logistical footprint due to its transportability and simple operational maintenance. It also has a low thermal signature and is much quieter than diesel generators. However, due to the need for direct solar radiation, these systems cannot be camouflaged. To produce renewable power for a bigger rear-operating base, a significant area of land would be required if the base is not connected to national electric grids. This requirement makes it challenging to create an independent hybrid electrical grid to meet the demand for bigger rear-operating bases.

Onshore wind power in the form of small wind turbines could also be a technology of choice since installation is technically manageable and maintenance is minimal. However, due to its intermittency, onshore wind requires energy storage systems. In addition, onshore wind farms are highly visible and could interfere with communication signals and sensors, reducing their functionality in an operational application.[87]

The main problem of RES is their intermittent quality, so wind and solar PV cannot be used independently. However, when combined with conventional generators, they add great value in forward-operating bases, which can work as a backup or energy storage. In rear-operating bases, the energy demand of a base is higher and more capacity needs to be installed. Hybrid solutions with RES are suitable for smaller bases and could provide the Armed Forces with more resilient energy supplies and greater operational effect.[88]

Solar PV and wind power are scalable, can be easily transported, and do not need a lot of infrastructure, so their increasing use by deployed military forces should be tested further. NATO and its partners should

[87] Guilia Signorelli, "Military Aspects of Energy Security with an Emphasis on Interdependencies between the Civil Energy Sector as a Supplier and Military as a Consumer," in *Energy Highlights* (Vilnius, LT: NATO Energy Security Centre of Excellence), 23, https://enseccoe.org/data/public/uploads/2021/10/d1_military-aspects-of-energy-security.pdf.

[88] Signorelli, "Military Aspects of Energy Security," 23.

be proactive in implementing new energy technology, so NATO can fully exploit the advantages.[89]

Case Study on Nord Stream 2: Security Risks and Threats Emerging from Dependence on Imported Fossil Fuels

Russia's war of aggression in Ukraine acutely exposed the dependence of key NATO countries on imports of fossil fuels—oil, gas, and coal—from Russia. For years, warnings by experts about the political ramifications of this dependence were ignored.[90] Instead, a new pipeline, Nord Stream 2, running parallel to Nord Stream, was built from 2018 onward to import high-emission natural gas from northwestern Russia to the northeast of Germany via the Baltic Sea. Just like Nord Stream 1, it circumvented transit countries in Eastern Europe, especially Ukraine. Had Nord Stream 2 become operational, it would have allowed Russia to bypass existing pipelines through Central Eastern Europe (CEE) and Ukraine altogether, cutting off government income from transmission charges and enabling Moscow to "turn off the tap" at a whim. Moreover, the pipeline would have increased the disproportionate dependence on Russia as a gas supplier and on fossil fuels at a time when domestic renewable energy constituted an affordable alternative to imported gas.

A miscalculation on the part of political decisionmakers relates to the risks emerging from the long-term lock-in created by European (and, in particular, German) dependence on imported fossil gas. Nord Stream 2 undermined the commitment of the European Union to a "net zero" economy by the year 2050, and, in particular, Germany's more ambitious commitment to become carbon neutral by 2045. Despite these risks, calls by the United States, Allies from CEE, and environmental activists to stop the construction of Nord Stream 2 were ignored by consecutive German governments.

Environmental groups took to the courts because of the violation of a range of laws and regulations during the construction process. In late 2021, the German Federal Network Agency for electricity, gas, telecommunications, post, and railway (*Bundesnetzagentur*, BNetzA) announced that Nord Stream 2 AG, the pipeline operator headquartered in Switzerland, had not yet met the regulatory conditions for the certification process. According to BNetzA, the operator had to have a legal presence in Germany for the German authorities to exercise oversight. Moreover, according

[89] Signorelli, "Military Aspects of Energy Security," 29–30.

[90] Sascha Müller-Kraenner, *Energy Security: Re-measuring the World* (Munich: Taylor and Francis, 2007).

to European Union law, the pipeline operators need to be independent of the fuel suppliers and grant nondiscriminatory access, which was not the case with Gazprom. In the EU's regulation of network industries (such as electricity and gas), unbundling refers to the separation of the activities potentially subject to competition, such as the production and supply of energy, from those where competition is impossible or not allowed. Transmission and distribution of electricity and gas are regulated monopolies in the EU. Unbundling is meant to prevent a situation where competitive and monopolistic activities are performed by the same company. The two different types of activities cannot be "bundled."[91] Therefore, the necessary unbundling would have had to happen before a license could be granted. A legal clearance by the European Commission would have been necessary, too. These legal requirements were largely ignored by key German government decisionmakers, at least until late 2021.

Nord Stream 2 was built on the assumption that the European demand for natural gas would increase during the transition to a renewables-based energy system. In this context, gas was portrayed as a "bridging fuel" that helps mitigate the effects of fluctuating renewables. Before Russia's war of aggression in Ukraine, the question of whether there was a need to increase natural gas supplies was a contentious issue. Germany, at least at the time, had significant gas import capacities with Russia, Norway, and the Netherlands. However, the Netherlands decided to stop its gas production as the main suppliers for the foreseeable future.

From a climate point of view, it needs to be emphasized that the fuel transported via Nord Stream 2 would have been a source of an additional 100 million tons of carbon dioxide per year. Environmental groups and scientists using satellite-based remote sensing also pointed out that, at the sites of production in Russia, there are significant amounts of the potent greenhouse gas methane emitted into the atmosphere, suggesting natural gas is not more climate-friendly than coal as an energy source.[92]

The case of Nord Stream 2 proves that reliance on fossil energy imports creates political and economic dependencies, thereby significantly restricting the political room for maneuver. Renewable sources of energy, on the contrary, can be produced in-country and shared with neighboring countries and Allies.

[91] "Unbundling in the European Electricity and Gas Sectors," Florence School of Regulation (website), July 20, 2020, https://fsr.eui.eu/unbundling-in-the-european-electricity-and-gas-sectors/.

[92] "Methane Emissions from the Energy Sector Are 70% Higher than Official Figures," International Energy Agency (website), February 23, 2022, https://www.iea.org/news/methane-emissions-from-the-energy-sector-are-70-higher-than-official-figures.

Renewable energy sources are also the main instruments to fight the mounting risks and threats of climate change.

Threat Response: Climate Change and Security Action Plan

Climate change will have severe ramifications for the planning and execution of all future Allied operations. NATO's response to the risks and threats from climate impacts must cover the three dimensions described in this chapter: the impacts of extreme weather events on military infrastructure and operations; the indirect impacts and the cascading effects of climate change, especially in fragile contexts that can lead to conflict and an increase of terrorist activity; and the implications of armed forces "going green" and switching to renewable energy. Many of the recommendations in this chapter relate to the priorities identified in NATO's Climate Change and Security Action Plan, especially when it comes to the need to adapt to Europe's committed-to climate change. Adaptation needs identified in the action plan cover resilience, civil preparedness, defense planning, capability delivery, assets and installations, standards, innovation, training, exercises, and disaster response.

Armed forces must maintain their ability to operate in a climate-altered world. When addressing the impacts of extreme weather events on military infrastructure and operations, NATO's seven baseline requirements for resilience, energy supply, and transportation provide an excellent framework for developing a meaningful and effective response. Specific changes are necessary for concepts and doctrine, training, personnel, infrastructure, equipment, information, organization, logistics, and interoperability. To improve CI resilience against climate impacts, NATO must invest in new infrastructure and retrofit existing infrastructure. Every military installation will require climate resilience and contingency plans to enable operational continuity in case of extreme weather events.

Significant challenges will arise for all operations in fragile contexts and regions disproportionately affected by climate impacts. The need for improvements along the seven baseline requirements is particularly critical in these situations. At the same time, the swift implementation of NATO's Climate Change and Security Action Plan will be key to making armed forces resilient in the face of climate impacts and maintaining operational effectiveness, including in HA/DR and counterterrorism operations.

The priority in the action plan to contribute to the mitigation of climate change, which includes mapping NATO's own GHG emissions and energy-efficient and sustainable technologies, is value-added. It also has implications for the conduct of military operations. As this chapter has shown, joint planning and the joint implementation of an energy transition among NATO Allies and partners will be vital. A cooperative effort will improve the chances of implementing on-site renewable energy generation, large-scale energy storage, and smart microgrids in the theater effectively and efficiently. It will make NATO armed forces and critical infrastructure more resilient and able to adapt effectively to a climate-altered and carbon-constrained world while reducing the military carbon footprint.

Select Bibliography

Air Defence and Offshore Wind: Working Together towards Net Zero. Air Media Centre/HQ Air Command/UK Ministry of Defense. Autumn 2021. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1021252/Air_defence_and_offshore_wind.pdf.

Beehler, Alex, and J. E. Surash. "Cutting the Cord to Test Energy Resilience." US Army (website). April 13, 2020. https://www.army.mil/article/234514/cutting_the_cord_to_test_energy_resilience.

Cox, Kate et al. *A Changing Climate: Exploring the Implications of Climate Change for UK Defence and Security*. Santa Monica, CA: RAND Corporation, 2020. https://www.rand.org/content/dam/rand/pubs/research_reports/RRA400/RRA487-1/RAND_RRA487-1.pdf.

Department of Defense, *Department of Defense Draft Climate Adaptation Plan*. Report Submitted to National Climate Task Force and Federal Chief Sustainability Officer. Washington, DC: Office of the Undersecretary of Defense (Acquisition and Sustainment). September 1, 2021. https://www.sustainability.gov/pdfs/dod-2021-cap.pdf.

Department of the Army. *United States Army: Climate Strategy*. Washington, DC: Office of the Assistant Secretary of the Army for Installations, Energy and Environment. February 2022. https://www.army.mil/e2/downloads/rv7/about/2022_army_climate_strategy.pdf.

Murgatroyd, Clive. "Defence in a Changed Climate." *RUSI Journal* 153, no. 5 (November 25, 2008). https://www.tandfonline.com/doi/full/10.1080/03071840802521895.

Samaras, Constantine, William J. Nuttall, and Morgan Bazilian. "Energy and the Military: Convergence of Security, Economic, and Environmental Decision-making." *Energy Strategy Reviews* 26 (November 19, 2019). https://www.sciencedirect.com/science/article/pii/S2211467X19301026?via%3Dihub.

Stein, Bruce et al. *Climate Adaptation for DoD Natural Resource Managers: A Guide to Incorporating Climate Consideration into Integrated Natural Resource Management Plans*. Washington, DC: National Wildlife Federation, May 17, 2019.

— 10 —

Terrorist Threats to Supply Chain and Logistical Resilience

Gabriel T. Raicu

ABSTRACT: The resilience of logistics and transport chains is imperative for an effective defense against classic or hybrid terrorist threats from previously known terrorist groups or malicious actors whose actions are difficult to attribute. Modern communications and digitization technologies are major logistics issues because practice has shown that current major military conflicts can be waged in the cyber realm, without formal declarations of war and can have disastrous military, political, and economic effects, with major disruption of supply chains at a global level. However, the Alliance must have the best logistical means to deal with any type of threat and must be able to scale up and expand its supply chain in line with international developments. The case studies in this chapter on coordinating logistics threats to cybersecurity and transport illuminate areas where NATO can be enriched through further training.

Keywords: logistics, supply chain, resilience, terrorism, cybersecurity

Introduction

There is an indissoluble link between criminal groups and terrorist networks that leads to a blurring of a clear line between national responsibility and the international response. From this perspective, there is an overlap between illicit trafficking patterns and proliferation activities versus illegal immigration routes and extended international crime centers. Thereby the prerogatives of sovereignty and border control policies act against the global nature of the terrorist threat. Undergoverned or even ungoverned areas from NATO's geographical boundaries from North Africa to the Balkans pose risks of infiltration by terrorist groups into Europe, many of them adapting their logistics to suit different legislative frameworks.

This chapter will provide logistics and supply chain definitions, examine the organizations handling logistics and supply chain in and for NATO and their efficiency, explain current case studies of areas where the security of the Alliance is being threatened through attacks on logistics and supply, and provide recommendations.

It is necessary to make a major distinction between the supply chain as a whole and the logistics itself, starting with the fact that the supply chain is responsible for overall sourcing, processing, and delivery to end users. Logistics is specifically focused on moving and storing goods between the various components of the supply chain. Given the above statements, logistics is a subsection of the supply chain and a part of the end-to-end supply chain process. Although the full efficiency of activities in modern society is dependent on supply chain and logistics flexibility, NATO's approach is to streamline national resources to meet the Alliance's common needs.

Logistics and Supply Chain in the NATO Context

Logistics is the science of planning, organizing, moving, and maintaining the forces at the Alliance's disposal. Without functional logistics, no operation is possible, as logistics is a key element of the success and achievement of the Alliance's extensive objectives. NATO defines *logistics* as a "science of planning and carrying out the movement and maintenance of forces. In its most comprehensive sense, the aspects of military operations logistics deals with include: (1) design and development, acquisition, storage, movement, distribution, maintenance, evacuation, and disposal of materiel; (2) transport of personnel; (3) acquisition or construction, maintenance, operation, and disposition of facilities; (4) acquisition or furnishing of services; and (5) medical and health service support."[1]

From an evolutionary point of view, logistics has risen over time through the perspective of the experience of the Alliance and the change in the geopolitical situation. NATO logistics were limited to the North Atlantic area during the Cold War, with a planned linear defense based on national support elements of Western Europe. Communication lines within Europe

[1] NATO, *NATO Glossary of Terms and Definitions*, AAP-06 (Brussels: NATO Headquarters, 2013), https://www.jcs.mil/Portals/36/Documents/Doctrine/Other_Pubs/aap6.pdf.

extended into the Channel and North Sea ports area.[2] Planning required that reinforcements and supplies be picked up at sea from the United States and Canada in the same ports and transported by air to European bases to use prepositioned equipment. Moving equipment like tanks across continents and through diverse terrain is a complex technical and political issue, completely different from airlifting supplies in the fastest way possible.

NATO followed the principle that logistics was a national responsibility before the 1990s. Consequently, its only focus "was the establishment of compliance with overall logistics requirements between members."[3] NATO's plans and actions were governed until the end of the Cold War based on this principle when it was largely accepted that the global situation had undergone a fundamental change that had underpinned this principle. This experience has changed the security environment and triggered a series of specific logistical challenges in the Partnership for Peace (PfP) and other cooperation programs with Central and Eastern Europe and other international organizations, where peace support operations in the Balkans generate a series of specific logistical challenges.

Complexity of the Supply Chain

The capabilities of the Alliance are sustainable when each of the components of the communication lines is functional. The weakest link endangers the efficiency of the entire system.

To improve the security of the Alliance's current lines of communication (LOCs) and transport routes, NATO must assess threats and establish efficient and cost-effective LOCs when needed.[4] Security of shipments is a main priority, as is the political approval to pass through a country that may have nothing to do with the conflict. Specifically, the exposure of each link will be considered here in the event of a conflict or in case the agents of influence of the aggressor state could act through proxy against the integrity of the communication lines.

The supply process can be considered as a system of systems aggregated activity where supplying the military with everything from food to equipment is a part of each NATO operation. It is a complex process, creating new

[2] NATO Logistics Committee, *NATO Logistics Handbook* (Brussels: NATO Headquarters, November 2012), https://www.nato.int/docu/logi-en/logistics_hndbk_2012-en.pdf.

[3] "Logistics," NATO (website), June 21, 2017, https://www.nato.int/cps/en/natolive/topics_61741.htm.

[4] "Civilian Expert Helps NATO Establish Communication Lines," NATO (website), January 27, 2012, https://www.nato.int/cps/fr/natohq/news_83812.htm?selectedLocale=en.

LOCs far more complex than finding roads, airports, rail networks, or ports to dock ships.

A major challenge in terms of supply chain security is its dependence on the private sector, which raises a number of risks for various reasons, ranging from a company's operational limitations to the related interest given by political affiliation or confusing geostrategic interest, which the owner of a logistics node may have. The owners or the main shareholders of the companies may take actions contrary to their direct economic interests due to their relationship of subordination or dependency with states that have geostrategic visions contrary to the values of the Alliance. This vulnerability can spread with cascading affects and has the potential to affect severely sectors not directly related to the supply chain segment. Although the example is not unique, we can cite the energy crisis that has affected Europe due to the major dependence on fossil resources from Russia. Moreover, dependence on mineral resources, physical production capacity, and energy resources belonging to states or blocs with geopolitical interests opposite to democratic values generates the possibility of affecting military mobility or altering operations at the Alliance level due to multiple disruptions along the supply chain or within intermediate logistics operations.

A comprehensive perspective here that distinguishes between the shortest and most efficient logistics chain and the politically possible one can be considered in the case of the Russia-Ukraine war. In the area of the eastern flank of the Alliance, in the case of countries that joined NATO after 1990, there are disparities in the development of the transport network due to the former policies of the Warsaw Pact which supported railway transport first with road transport having an auxiliary function. Consequently, the distribution of the road network is not efficient, and its density is four to five times lower than in Western Europe. The discrepancy is even more pronounced in the case of the newly acceded states in Eastern Europe.

Supply Chain and Collective Logistics

To understand the complexity of logistics at a NATO level, it would be necessary to approach each decision-making and operational layer in detail to identify ways to streamline the activity. A more effective approach is to study the issue as a system of dynamically interacting systems governed by individual principles, visions, and policies subject to a major common goal. Some defining elements and directions need to be considered in this approach.

NATO logistics can be understood by basic functions not limited to supply, maintenance, movement and transport, oil support, infrastructure engineering, and medical support. Multinational logistics reduces costs, streamlines processes, and increases the efficiency of logistics support at any time.

The important parts of the specific elements that give the dimension of systemic complexity are listed below:

- Sharing the provision and use of logistic capabilities between nations is one of the key logistics principles driving all related support in NATO.
- There must be a flexible ability to move forces in an efficient manner in and between operational theaters. The complete spectrum of NATO roles and missions also needs advanced logistical support.
- The Logistics Committee is the main committee that supports the North Atlantic Council and the Military Committee as the global coordinating authority for the full range of logistical functions within NATO.
- The general list of agencies, policy commissions, and organizations involved in NATO's logistics activities includes the:
    - Logistics Committee (LC)
    - Petroleum Committee (PC)
    - Committee of the Chiefs of Military Medical Services in NATO (COMEDS)

- Civil Emergency Planning Committee (CEPC)
- Committee for Standardization
- NATO Supply and Procurement Agency (NSPA)
    - Fuel Management, which includes the Central European Pipeline System (CEPS) Programme
    - Strategic Transport and Storage, which includes the NATO Airlift Management (NAM) Programme
    - Systems Procurement and Life Cycle Management
    - Logistics Services and Project Management
    - Support to Operations and Exercises
- Bi-SC Medical Advisory Group (Bi-SC MEDAG)
- Bi-SC Movement and Transportation Forum (Bi-SC M&T Forum)[5]

According to NATO, the "Bi-SC Movement and Transportation Forum (Bi-SC M&T Forum) was formed in 1996 and is the senior forum for coordinating Alliance-wide concerns for movement and transportation policy planning between Strategic Commanders, NATO members and designated agencies. Movement and transport matters of relevance to the forum are those that derive from the NATO commander's movement and transport responsibility and from concepts and policies developed by NATO Headquarters."[6]

To address the complexity and provide an effective framework for resolving subsequent issues arising from the need for continuous adaptation to ongoing geostrategic challenges (such as the Russia-Ukraine conflict), NATO Logistics Vision and Objectives 2015–24 set a framework in which NATO addresses the gaps in logistics capability. Following the first phase of the Russia-Ukraine conflict, at the 2014 Wales Summit, in response to Russia's challenges and the strategic implications, the heads of state and government agreed on the

[5] NATO, *Logistics Handbook*.

[6] NATO, *Logistics Handbook*.

Readiness Action Plan (RAP). The plan also addresses the risks and threats posed by the Middle East and North Africa. Through the RAP, the leaders of the Alliance agreed to reverse the downward trend in defense budgets and increase them over the next decade. NATO Logistics Vision and Objectives (V&O) have been revised in line with developments from the 2010 Strategic Concept, Political Guidance 2015, and the Readiness Action Plan.

The current strategic logistics guidance consisting of the revised vision statement provides effective logistical support and broadens the Logistics Vision to give NATO commanders the greatest flexibility in current and future missions promoting the pursuit of collective logistics within the Alliance. An important aspect of the revised vision is that it seeks to include broader civil responsibilities by taking a more comprehensive approach and is not limited to the Joint force commander. The Logistics Committee serves as the overarching coordinating authority across the spectrum of logistics functions within NATO and the main committee supporting the North Atlantic Council and the Military Committee.[7]

Supply Efficiency and Operational Consolidation

NATO has no direct access to the necessary supply-chain capabilities and logistics, even in its primary military defense responsibility. NATO's assets and capabilities belong to its member states, with few exceptions, most notably for political consultation and command and control. One of most important parts of its integrated military structure is the NATO Defense Planning Process (NDPP).

Through the NDPP, the main pillars of its integrated military structure, nations coordinate and distribute their capabilities at the Alliance level. The Transfer of Authority (ToA) mechanism allows national forces to fall under the control of NATO's Supreme Commander if needed. NATO's most recent operational experience and the development of a comprehensive approach to operations have expanded the NDPP to include selected nonmilitary capabilities, primarily in logistics, stabilization, and reconstruction. No provisions have been implemented due to concerns of possible transfer of these capabilities under NATO command should a situation warrant.

Civilian capabilities will always remain under national control if provided by national organizations. National contributions to NATO requirements

[7] NATO, *Logistics Handbook*.

require considerable effort and extend to counterterrorism assets.[8] While the political guidelines fail to establish important links between NATO and the organizations responsible for implementing national policies and asset control, it has been possible to establish a fundamental link between NATO's counterterrorism capabilities and the NDPP.

NATO's decades of multidisciplinary experience in civil defense, critical infrastructure protection, information sharing, air defense, airspace and maritime security, nonproliferation and CBRN response, special operations, and force protection bring consistency and consolidation to newly developed policies.

During conflicts and subsequent periods of austerity, it is essential to minimize the impact of adversary propaganda and disinformation spread. This spread can equate to, or even outweigh, the effects of classical terrorist attacks in affecting the logistics chains at the decision and operational levels. Depending on the intensity, estimated duration, and importance of a conflict, the main aim is to raise awareness of surface transport's benefits for long distance. In this case, air transport provides for rapid deployment, while rail or road transport offers a cost-effective method for prolonged sustainment in the longer term to counteract fears imposed by economic contraction due to war threats. Rail and road transport also bridges the gap between the military perspective and commercial reality. Thus, beyond political reasoning, it is about finding the most cost-effective and secure methods of military transportation. One significant example of this is the closure of the surface LOC via the Pakistan to Afghanistan surface into the north of Afghanistan, resulting in escalating cost of airlift support to the International Security Assistance Force.

Logistics and Supply Chain Threats Aspects

Threats Complexity and Their Interrelation

After the end of the Cold War, there was a tendency to reduce the military presence in Europe, leading to several current potential logistical problems that must be overcome now during the Ukraine conflict. For example, there is an increased need for semitrailers with a capacity of 70 tons, supplementing the number of rail cars with a minimum capacity of 90 tons, increasing the number of mobile rail ramps, modernizing and digitizing road infrastructure,

[8] "Resilience, Civil Preparedness and Article 3," NATO (website), March 23, 2021, http://www.nato.int/cps/en/natolive/topics_49158.htm?selectedLocale=en.

developing military electronic cargo tracking systems, and improving data interchange between transportation structures and military units.[9]

The real level of NATO armed forces capabilities in areas like military mobility and logistics is shown by military training and exercises such as Dragoon Ride, Sabre Strike or Atlantic Resolve in eastern flank countries, including Poland, Romania, Hungary, Bulgaria, the Czech Republic, Slovakia, and the three Baltic republics of Estonia, Latvia, and Lithuania. NATO and EU structures cooperation in security and defense led to the Permanent Structured Cooperation (PESCO) establishment in 2017. There was a need to create a "Military Schengen Zone" to streamline military mobility in the EU, especially in its eastern areas.

The new NATO logistics vision reflects top-down guidance by principles, with the deployment of NATO forces potentially requiring rapid movement of personnel in the current strategic environment. A large quantity of equipment and material must be deployed across NATO territory, considering the need for operational effectiveness versus considerations of efficiencies.[10]

Threats can come from state and non-state actors in the form of terrorist attacks, cyberattacks, or combined in the form of hybrid warfare, with faint delineations between conventional and unconventional forms of conflict.[11] Natural disasters and climate change can trigger floods, fires, and earthquakes or generate biohazards and pandemics (such as COVID-19) with an unpredictable effect on global logistics. The security environment was radically transformed due to the challenge of adapting and responding to these threats.

There is a Strengthened Resilience Commitment reiterated in 2021 by the Heads of State and Government of the North Atlantic Alliance: "We are addressing threats and challenges to our resilience, from both state and non-state actors, which take diverse forms and involve the use of a variety of tactics and tools. These include conventional, non-conventional and hybrid

[9] Wiktor Biernikowicz, *The Military Transport Challenges in Light of the NATO "Freedom of Movement" Policy on the Example of Poland* (Prague: CLC, 2018), https://www.confer.cz/clc/2018/read/2571-the-military-transport-challenges-in-light-of-the-nato-freedom-of-movement-policy-on-the-example-of-poland.pdf.

[10] NATO, *Logistics Handbook*.

[11] Urmas Paet, "Europe Needs a Military Schengen," *European Defence Matters* (2017), https://eda.europa.eu/webzine/issue12/cover-story/europe-needs-a-military-schengen; and David M. Herszenhorn, "Call for 'Military Schengen' to Get Troops Moving," *Politico* (website), August 4, 2017, https://www.politico.eu/article/call-for-military-border-schengen-to-get-troops-moving-nato-eu-defense-ministers/.

threats and activities; terrorist attacks; increasing and more sophisticated malicious cyber activities; increasingly pervasive hostile information activities, including disinformation, aimed at destabilizing our societies and undermining our shared values; and attempts to interfere with our democratic processes and good governance."[12] There has been a growing NATO commitment for at least five years "about the baseline requirements on resilience from infrastructure, from energy, from telecoms, now logistics and supply chain."[13]

How NATO can execute its commitment to resilience of logistics and supply chain in the face of cyber threats is the subject of the next section.

Nonphysical and Advanced (Cyber) Threats to Logistical Chain

The NATO Cooperative Cyber Defense Centre states that "the Tallinn Manuals have served [for a decade] as an essential tool for policy and legal experts on how international law applies to cyber operations," providing an academic analysis of international law applied to cyber conflicts, which cyberterrorists, as well as nation-states, can perpetrate.[14] Cyberterrorists are organized into groups that commit cyberattacks for political, religious, ideological, or social reasons to promote fear of targeted victims. Their actions are aimed at terrorists in real space, and they can act as individuals or organized groups or work as proxies for a nation-state interest.

Although strict adherence to these definitions is not mandatory for cyber defense planning, knowledge about attacker typologies provides insight into their motivation, resources, and determination. However, this can also have some very practical implications.

Any kinetic action in any field can involve attacks in cyberspace, although cyber warfare can exist mainly in virtual space. Escalation of conflicts and the potential to be used for terrorist purposes, if cyber conflicts escalate, inevitably attracts the targeting of railways, roads, airports, and sea and river ports, as well as connecting infrastructure such as bridges and ferryboats.

[12] "Strengthened Resilience Commitment," NATO (website), June 14, 2021, https://www.nato.int/cps/en/natohq/official_texts_185340.htm.

[13] "Newsroom: Building Transatlantic Resilience: Why Critical Infrastructure Is a Matter of National Security," NATO (website), December 10, 2020, https://www.nato.int/cps/en/natohq/opinions_180067.htm.

[14] "Talinn Manual," NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) (website), n.d., https://ccdcoe.org/research/tallinn-manual.

Railway cybersecurity challenges due to increased digitization create a novel threat derived from the complexity of new systems like the European Railway Traffic Management Systems (ERTMS), which have already improved cross-border interoperability throughout Europe by creating a single standard for railway signaling. The efficiency offered by ERTMS must be weighed against the inherent risk of increased vulnerability due to the extensive digitization that tends to focus the attackers' attention. There is an increased demand for a dedicated railway cybersecurity solution amid increasing threats.

Only solutions built with the railway's protocols, technologies, and systems can ensure reasonable safety, continuity, and reliable transport. Railways often become primary targets for cyberattacks during major events due to a country's leadership and delegations using railway transport and the media impact that increases with the disruption in event logistic.

Concerns about the cybersecurity of the railways have led to directives such as the Transportation Security Administration's December 2021 security directives "to fortify cybersecurity across all US critical infrastructure, including passenger railroads, rail transit agencies, and freight railroads."[15] Similarly, the European Committee for Electrotechnical Standardization (CENELEC), responsible for developing and defining voluntary electrotechnical standards in Europe, created CLC/TS 50701 in 2021 to guide all railway operators, system integrators, and product suppliers on managing cybersecurity in the context of the EN 50126-1 RAMS lifecycle process.[16]

There is a close logical connection within the civilian domains that can be constituted in real areas of disruption of the supply chain. Aviation, a major logistics component, has been subjected to multiple types of cyberattacks. There is a large variation between the types of attacks, ranging from the 2015 DDoS attack on Polish airline LOT that left 1,400 passengers stranded at a Warsaw airport to the 2016 and 2017 Black Energy malware and GoldenEye ransomware attacks at Boryspil airport

[15] Transportation Security Administration, *Enhancing Public Transportation and Passenger Railroad Cybersecurity*, Security Directive 1582-21-01 (Washington, DC: Department of Homeland Security, December 31, 2021), https://www.tsa.gov/sites/default/files/sd-1582-21-01_signed.pdf.

[16] "CLC/TS 50701: Railway Applications – Cybersecurity," European Standards (website), 2021, https://www.en-standard.eu/clc/ts-50701-2021-railway-applications-cybersecurity.

in Kyev.[17] In 2017, there were physical leaks of highly confidential data at Heathrow Airport, and in 2018, a hacked mobile application exposed the data of 20,000 Air Canada customers.[18] The 2018 massive personal data leak of over 400,000 customers of British Airways and the 2020 major data breach on EasyJet of over 9 million customers' leaked personal data are other examples.[19] In 2020, login portals (one reserved for employees, the other for partners and service providers) at San Francisco International Airport were compromised, and in 2020, the Prague airport foiled several attempted attacks, to name a few.[20]

While the direct effects of the attacks varied, the repercussions and hard- to-predict ripples generated systemic effects. They caused the destabilization of logistics systems over large areas, which impacted efficiency and trust.

Given the specific nature of port interconnection as a hub for rail, land, and air transport, the logistical risks posed by the impact of cybersecurity incidents requires the introduction of regulations related to the maritime industry. In March 2020, the US Coast Guard released Navigation and Vessel Inspection Circular (NVIC) 01-20, titled "Guidelines for Addressing Cyber Risks at MTSA Regulated Facilities." There are several organizations involved in guidance for cyber defense–related to ports, including the European Union

[17] Stephanie Prevost, "Ten Major Cyberattacks against the Airport Industry," Stormshield (website), August 16, 2021, https://www.stormshield.com/news/ten-major-cyberattacks-against-the-airport-industry; AFP News Agency, "Hackers Target Polish Airline LOT, Ground 1,400 Passengers," Security Week (website), June 21, 2015, https://www.securityweek.com/hackers-target-polish-airline-lot-ground-1400-passengers; Pavel Polityuk and Alessandra Prentice, "Ukraine Says to Review Cyber Defenses after Airport Targeted from Russia," Reuters (website), January 18, 2016, https://www.reuters.com/article/us-ukraine-cybersecurity-malware-idUSKCN0UW0R0; and Ellie Burns, "Chaos in Ukraine as Ransomware Cyber Attack Hits Airports, Banks & Government," Techmonitor (website), June 27, 2017, https://techmonitor.ai/technology/cybersecurity/chaos-ukraine-ransomware-cyber-attack-hits-airports-banks-government.

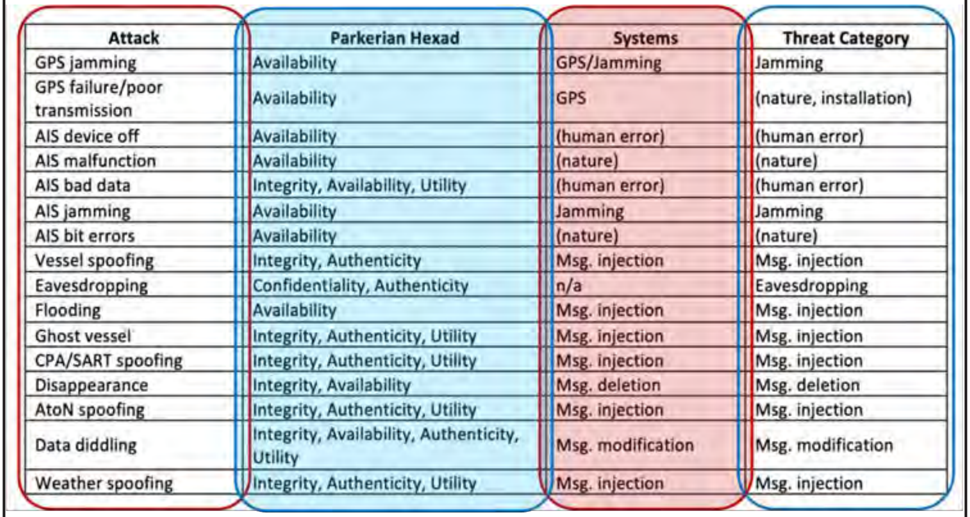
[18] Charlie Osborne, "Heathrow Airport Fined £120,000 over USB Data Breach Debacle," ZDNet (website), October 9, 2018, https://www.zdnet.com/article/heathrow-airport-fined-120000-over-usb-data-breach-debacle; and Jeremy Kirk, "Air Canada: Attack Exposed 20,000 Mobile App Users' Data," August 30, 2018, https://www.bankinfosecurity.com/air-canada-attack-exposed-data-on-20000-mobile-app-users-a-11441.

[19] John Bosnell, *British Airways Suffers Data Breach Compromising Information on over 429,000 Customer Cards* (Genève, CH: ORX News, December 21, 2018), https://managingrisktogether.orx.org/sites/default/files/public/downloads/2019/01/british-airways-suffers-data-breach-compromising-information-over-429-000-customer-cards.pdf; and "EasyJet Hacked; Details of 9 Mn Customers Compromised," CISO-MAG (website), May 20, 2020, https://cisomag.eccouncil.org/easyjet-hacked-details-of-9-mn-customers-compromised.

[20] John Leyden "San Francisco Airport Data Breach: Double Website Hack May Have Lifted Users' Windows Login Credentials," Daily Swig (website), April 14, 2020, https://portswigger.net/daily-swig/san-francisco-airport-data-breach-double-website-hack-may-have-lifted-users-windows-login-credentials; and Reuters Staff, "Prague Airport Says Thwarted Several Cyber Attacks; Hospitals Also Targeted," Reuters (website), April 18, 2020, https://www.reuters.com/article/us-czech-cyber-idUSKBN2200GW.

Agency for Cybersecurity (ENISA), the International Association of Ports and Harbors (IAPH), and the Institution of Engineering and Technology (IET).

NVIC 01-20 requires assessment and documentation of computer systems and network vulnerabilities in a facility security assessment (FSA) and addresses all identified vulnerabilities in applicable sections of the facility security plan (FSP).[21] As shown in figure 10-1, several possible cyber-maritime attacks (GPS jamming, vessel spoofing, flooding, and the creation of a ghost ship) can have systemic logistical effects as shown on Automatic Identification Systems (AIS). Each type of attack can be classified according to the threat to the information, such as jamming versus the availability of information, the system and the attack vector (for example, message injection for AIS spoofing), and the threat category (for example, flooding is also another kind of message injection attack).



Attack	Parkerian Hexad	Systems	Threat Category
GPS jamming	Availability	GPS/Jamming	Jamming
GPS failure/poor transmission	Availability	GPS	(nature, installation)
AIS device off	Availability	(human error)	(human error)
AIS malfunction	Availability	(nature)	(nature)
AIS bad data	Integrity, Availability, Utility	(human error)	(human error)
AIS jamming	Availability	Jamming	Jamming
AIS bit errors	Availability	(nature)	(nature)
Vessel spoofing	Integrity, Authenticity	Msg. injection	Msg. injection
Eavesdropping	Confidentiality, Authenticity	n/a	Eavesdropping
Flooding	Availability	Msg. injection	Msg. injection
Ghost vessel	Integrity, Authenticity, Utility	Msg. injection	Msg. injection
CPA/SART spoofing	Integrity, Authenticity, Utility	Msg. injection	Msg. injection
Disappearance	Integrity, Availability	Msg. deletion	Msg. deletion
AtoN spoofing	Integrity, Authenticity, Utility	Msg. injection	Msg. injection
Data diddling	Integrity, Availability, Authenticity, Utility	Msg. modification	Msg. modification
Weather spoofing	Integrity, Authenticity, Utility	Msg. injection	Msg. injection

Figure 10-1. Types of alleged attacks
(Original by author)

[21] "NVIC 01-20 Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities," US Department of Homeland Security/US Coast Guard Homeport (website), March 3, 2020, https://homeport.uscg.mil/Lists/Content/DispForm.aspx?ID=62174&Source=/Lists/Content/DispForm.aspx?ID=62174.

Cyberattacks on the transport system can block the industry due to a ripple effect in the supply chain. As an entry-level scenario, a cyberattack against maritime facilities could disrupt the customs approval process, facilitate the import of illegal goods, or the proliferation of dangerous operations. Threat actors may also have a bigger target if a cyber threat can proliferate from a port to other interconnected systems like airports or railways.

Figure 2 shows interesting pattern involving a maritime cyber incident, where Marine Traffic, a well-known maritime analytics real-time provider, gives a synoptic picture of an incident that should impact the maritime area. Although the incident is one with an impact only in the maritime field, it can also confuse adjacent areas (such as aviation and other monitoring services) affected by the altered reporting of maritime positioning data. It shows how the information provided automatically by the maritime AIS system is altered, either at the source via GPS spoofing or during the uninterrupted transmission through unsecured AIS protocol or injection. The records date back to October 2021, as shown in figure 10-2, but the systematic errors persisted for months. The attack targeted the positioning of ships and not aviation itself, and the display on the maritime map above an airport is the only illustration of the attack. They could have been positioned above other cities or highways as well.

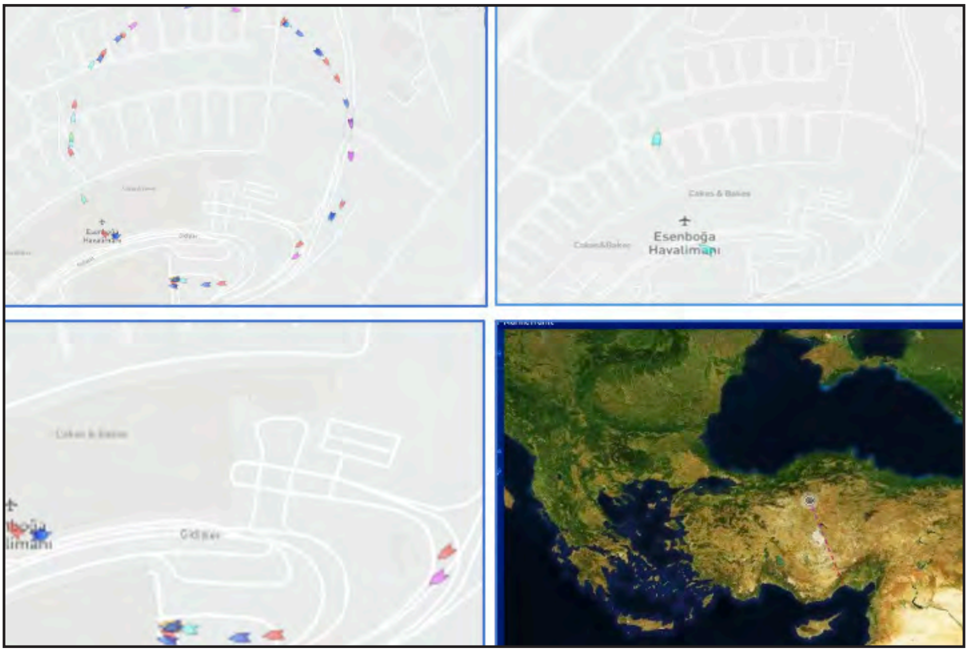


Figure 10-2. Spoofed positions of maritime ships over Ankara Esenboga Airport, October 25, 2021, 20:10 EET

Source: "Global Ship Tracking Intelligence," MarineTraffic (website), n.d., https://www.marinetraffic.com/en/ais/home/centerx:33.062/centery:40.132/zoom:15.

[22]Globally, cargo ships have an average transport capacity of 8,000 containers per voyage, with transportation systems operating at 53 billion passengers annually. Before the global pandemic, more than 8.8 billion passengers traveled through airports worldwide. The examples of transport system management below provide a dimension of operational complexity:

- Maritime: systems for managing the fleet, ships, and maritime traffic
- Airports: systems for managing the fleet, passengers, and air traffic control
- Roads and bridges: traffic signaling systems containing road and lidar sensors which determine ranges through laser
- Highway tunnels: lighting systems, heat, and ventilation sensors
- Railways: traffic-planning systems, power supply, maintenance, and control of stations

To manage these complex systems, the number of IoT devices involved is growing exponentially. Transport and logistics operators must protect their access to operational technology (OT) systems and strengthen cyber resilience to prevent disruptions and ensure safety and security. Any unplanned interruption of operation in one of these environments can lead to supply-chain blockages or severe disruption of the logistical relationships of the systems.

There is an accelerated trend for information technology (IT) to converge rapidly with OT at any point in the transport chain. The decisive effect of combining OT with IT data is exponential growth in process efficiency, but with the inherent risks of cybersecurity. Unfortunately, most OT security teams cannot provide satisfactory system security due to a lack of tools, procedures, and knowledge.

Multinational Interaction Mechanisms

The current complex geopolitical situation, with variable and omnidirectional risks corroborated with the principles of logistical distribution at the level of the Alliance members, requires the introduction of multinational

[22] "Global Ship Tracking Intelligence," MarineTraffic (website), n.d., https://www.marinetraffic.com/en/ais/home/centerx:33.062/centery:40.132/zoom:15.

logistics. Although multinational logistics was included in the *NATO Logistics Handbook* (2012), there was no agreement at the NATO level. There has been a proposed concept of logistics support to operations through multinational means, such as lead nation, role specialization, and multinational integrated logistic support. Accordingly, there are "four types of multinational logistic support options that may be implemented": preplanned mutual supports between national support elements, one nation formally undertaking support as a logistic lead nation or specialist nation, one or more nations under the operational control of the Joint force commander, or one or more nations forming a multinational logistic/medical unit.[23]

For a complete understanding of the logistical interaction mechanisms within NATO, it is necessary to recall a few aspects, such as collective responsibility for logistics, which imply that neither the member state nor NATO itself can take full responsibility for an entire operation. Cooperation and consideration of all aspects contributing to the operation's success is necessary. From this point of view, the notion of *collective logistics* as "the collective approach undertaken by NATO and nations to plan, generate, synchronize and prioritize national and NATO logistic capabilities, resources and activities to deliver logistic support to NATO missions, operations and exercises, by making use of common processes and organizational structures" is defined.[24]

Beyond the definitions that have widespread acceptance within the NATO logistics community, respectively production (acquisition) logistics, in-service logistics, and consumer (operational) logistics, it is very important to highlight the overlaps of the Conference of National Armaments Directors (CNAD), the NATO Support Organization (NSPO), and the Logistics Committee as the main aspect of three life cycle domains and their lead bodies as shown in figure 10-3.

[23] NATO Standardization Office (NSO), *Allied Joint Doctrine for Modes of Multinational Logistic Support*, NATO Allied Joint Publication (AJP)-4.9, ed. A, ver. 1 (Brussels: NSO, February 2013), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/787266/archive_doctrine_nato_modes_of_multinational_log_spt_ajp_4_9.pdf. This publication was withdrawn without direct replacement, as directed by the NSO in February 2019.

[24] NSO, *Allied Joint Doctrine for Logistics*, AJP-4, ed. B, ver. 1 (Brussels: NSO, December 2018).

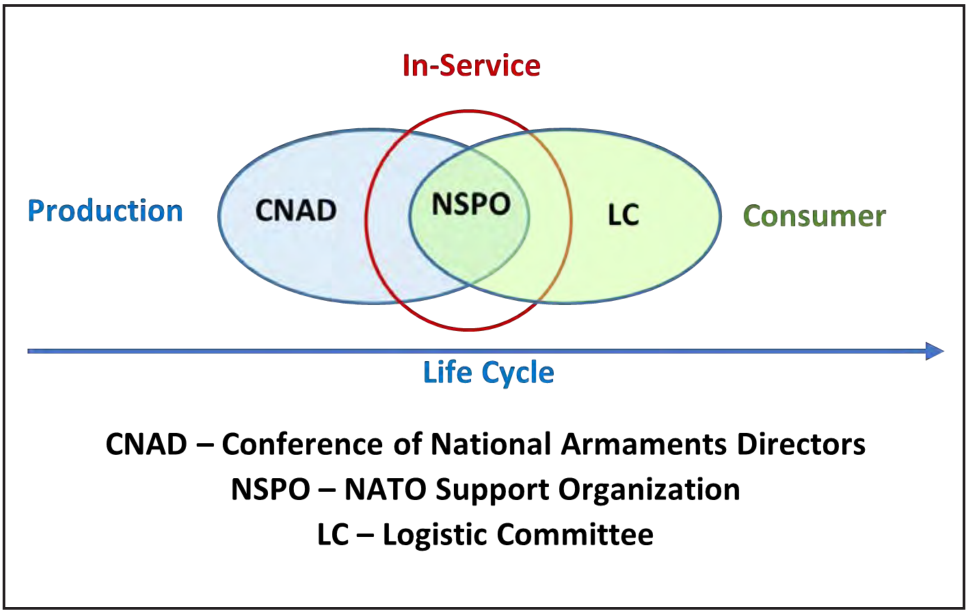

In-Service
Production
CNAD
NSPO
LC
Consumer
Life Cycle
CNAD – Conference of National Armaments Directors
NSPO – NATO Support Organization
LC – Logistic Committee

Figure 10-3. Life cycle domains and their lead bodies
(Original by author)

Complex Risks for Critical Logistic Infrastructure

The functionality and validity of logistics infrastructure play a vital role in many developed countries to enable efficient and resilient logistics chains. Even temporary damage to some elements of the chain can lead to the decommissioning of entire transport branches. An example is the altered functionality of the railway network near the German town of Rastatt due to the construction of a new railway tunnel. As a result, the route between Karlsruhe, Germany, and Basel, Switzerland, was closed for two months for any type of rail transport with the immediate effect of the unavailability of a critical logistics infrastructure. This closure affected 200 freight trains per day passing through this link between Germany, the Netherlands, and Belgium and Switzerland and Italy.[25] This example of the railway logistic closing decision was assumed with some predictability of the short-term adverse effects. It is entirely different when complex risks must be corroborated.

To ensure full coverage of the risks and to provide a systematized working tool, subsequent risks (such as political, economic, social, technological, legal, and environmental risks) will have to be considered under a political,

[25] Nicky Gardner and Susanne Kries, “Major German Rail Route Closed,” Europe by Rail (website), August 19, 2017, https://www.europebyrail.eu/major-german-rail-route-closed/.

economic, social, technological, legal, and environmental risk (PESTLE) acronym umbrella as shown in figure 10-4. Political risks can be separated into macro- and micro-groups, where macro-political can severely affect the logistical infrastructure due to armed conflicts, including but not limited to full-scale wars, guerilla activities, and terrorism. All infrastructure nodes and suppy-chain links (such as roads, bridges, tunnels, train stations, railroads, seaports, or airports) are often strategically targeted or, at best, collateral damage during conflicts like the Donetsk International Airport in Ukraine in 2014.[26]

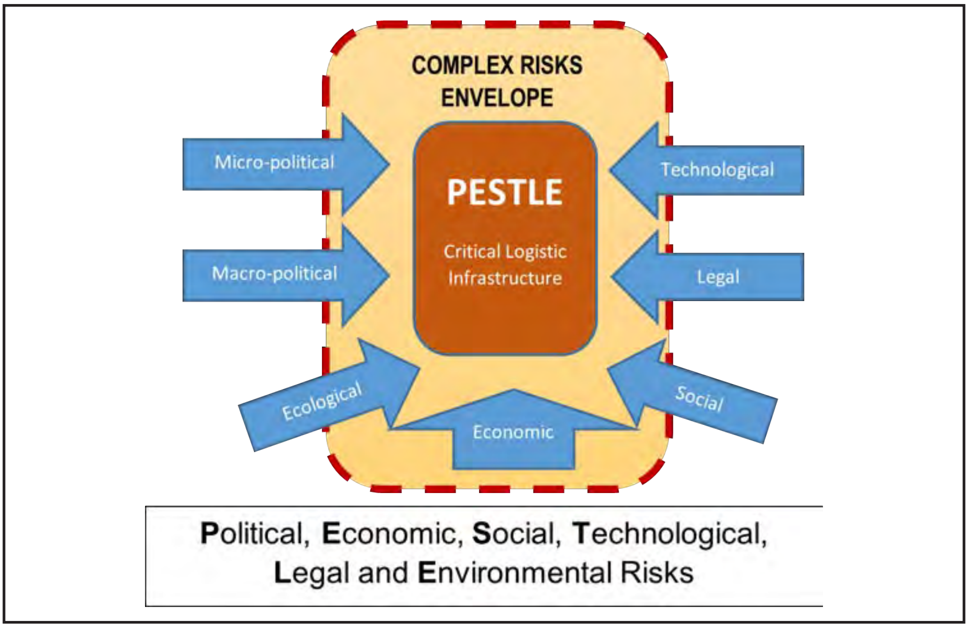

COMPLEX RISKS ENVELOPE
Micro-political
Macro-political
PESTLE
Critical Logistic Infrastructure
Technological
Legal
Ecological
Economic
Social
Political, Economic, Social, Technological, Legal and Environmental Risks

Figure 10-4. PESTLE (critical logistic infrastructure)
(Original by author)

Terrorist attacks also target populated areas and political and economic centers to maximize their psychological impact, as was done in the terrorist attack in Brussels in 2016 with direct damage to the airport and the railway transport system.[27] Also, maritime risks create macropolitical impact, as illustrated by the acts of piracy at Cape Horn or the older incident of

[26] UNIAN, "Cyborgs vs. Kremlin," Ukraine Today (website), 2015, http://cyborgs.uatoday.tv.

[27] Sheena McKenzie, "Brussels Travel: Flights Suspended, Transit Limited," *CNN* (website), March 23, 2016, http://edition.cnn.com/2016/03/22/europe/brussels-explosions-transport-flights-metro-suspended.

the trucker Iyman Faris who planned to blow up the Brooklyn Bridge.[28] Micro-political risks include diplomatic crises and do not necessarily coincide with moments of aggression but can lead to frequent roadblocks and border closures that can disrupt logistics infrastructure.[29] Economic risks have a lower impact on logistics infrastructure, as most infrastructure is usually publicly owned and, therefore, well protected from bankruptcy.

The private elements of a logistics infrastructure can be quite vulnerable to economic risks and can lead to major criticalities, depending on the level of interdependence they have with the rest of the logistics chain. Social risks, by definition, affect individuals or groups of individuals who are then transposed at the level of social status. Individually, it is difficult for an individual to affect the entire infrastructure, but union protests, real or caused by manipulation, can directly affect the logistics infrastructure. Strikes by workers whose status is at risk regularly affect the logistics infrastructure, with airport and railway operations being repeatedly stopped by coordinated strikes.

One example is the coordinated general strike against the supply chain that created a gas shortage in Paris in 2016. During the orchestrated strike, the carriers blocked the road infrastructure serving important ports and oil terminals for the French market.[30] There is an intrinsic vulnerability between social risks and the hybrid aspects of possible foreign interference and manipulation. The technological risks for the logistics infrastructure can be further diversified into operational risks generated by using specific infrastructure and risks related to the control and maintenance of logistics infrastructures. Legal risks for critical logistics infrastructures include diplomatic restrictions and bottlenecks, as outlined in the micro-political risks above. They may be caused by a temporary or permanent blockade of logistic infrastructure or an entire region for reasons of national policy.

There may also be rapid and unforeseen changes in legislation that could seriously affect the logistics infrastructure as a whole. The refugee crisis in Europe can be used as an eloquent example, as its consequences are difficult to manage in the short and medium term, altering the functionality

[28] Kelli Arena and Terry Frieden, "Ohio Trucker Joined al Qaeda Jihad," June 20, 2003, *CNN* (website), http://edition.cnn.com/2003/LAW/06/19/alqaeda.plea/.

[29] Cecilia Emma Sottilotta, "Political Risk: Concepts, Definitions, Challenges," Working Paper Series SOG-WP6/2013 (Rome: LUISS School of Government, 2013).

[30] Alissa J. Rubin, "Gas Runs Low in France as Protesters Block Refineries in Labor Battle," *New York Times* (website), May 25, 2016, https://www.nytimes.com/2016/05/26/world/europe/france-unions-labor-law.html.

of a common Schengen free-trade region.[31] Ecological risks are caused by altering the natural environment and can significantly affect the logistics infrastructure, including ecological catastrophes, low water levels, floods, earthquakes, typhoons, and hurricanes. As direct effects, temporary or even permanent closures of roads, railways, bridges, waterways, and airports may occur. The eruption of Eyjafjallajökull in Iceland in 2013 grounded thousands of airplanes across Europe for several days.[32]

Major Logistical Vulnerabilities and Defense of Choke Points: Suwalki Gap Case Study

One of the most exposed areas is the Suwalki Gap, also known as the Suwalki Corridor, which separates the Russian exclave of Kaliningrad on the Baltic Sea from the Belarusian border, as shown in figure 10-5. The latest military developments in the area have brought permanently stationed Russian troops, advanced aircraft, and nuclear weapons. It is also the only road and rail communication route from Central Europe to the Baltic states—NATO's most exposed members.[33]

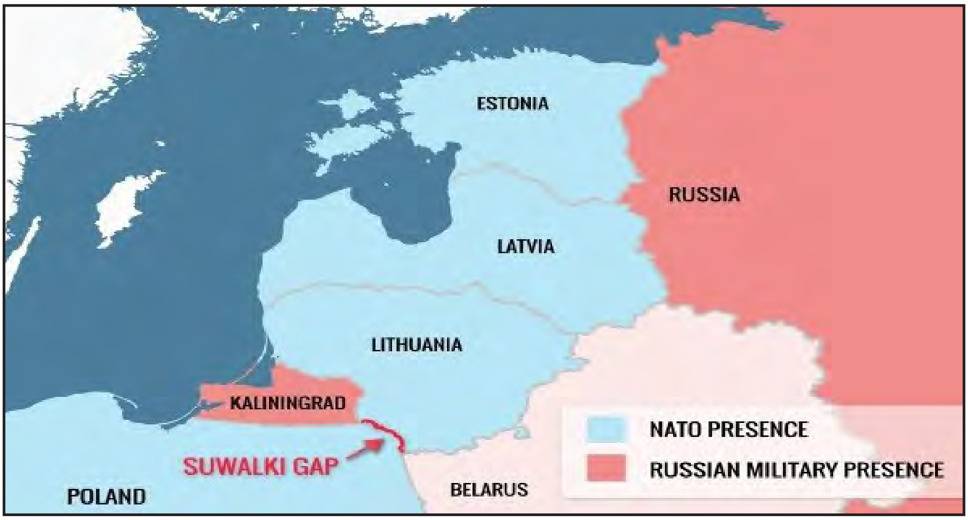


Figure 10-5. Suwalki Gap
Source: Deni, "NATO Must Prepare."

[31] Camilla Turner, "Eurotunnel Warns of Lengthy Delays Due to 'Migrant Activity,'" *Telegraph* (website), 2015, https://www.telegraph.co.uk/news/uknews/11762469/Eurotunnel-suspends-passenger-services-because-of-migrant-activity-in-Calais.html.

[32] Martin Randelhoff, "Eyjafjallajökull – die Auswirkungen in Europa und der ganzen Welt," Zukunft Mobilität (website), May 1, 2010, http://www.zukunft-mobilitaet.net/849/analyse/eyjafjallajoekull-fazit-schaden-flugverkehr-global.

[33] John R. Deni, "NATO Must Prepare to Defend Its Weakest Point—the Suwalki Corridor," *Foreign Policy* (website), March 3, 2022, https://foreignpolicy.com/2022/03/03/nato-must-prepare-to-defend-its-weakest-point-the-suwalki-corridor/.

From a logistical point of view, ground-based transportation infrastructure in the region is not resilient enough because there are only two roads and a rail line connecting Poland with the Baltic states. First, there is one highway with two lanes each way and a second with only a single lane. Western government officials, military leaders, and think-tank experts have been aware of the problem since Russia's first invasion of Ukraine in 2014. Russia can choke the area to disconnect the Baltic countries' land connection with the rest of NATO.

The Kaliningrad exclave hosts numerous Russian combat forces, including the Russian Baltic Fleet, advanced air defenses, and mobile nuclear-capable Iskander-M missiles. From a political-military point of view, due to Russia's particularly sensitive threat perception to its control of this noncontiguous territory, there are risks of escalation due to misinterpreted NATO's actions.

Although it is not logically possible for Russia to move because it would activate Article 5 of the Alliance, involving an attack on NATO territory and triggering a NATO military response, experience with the invasion of Ukraine in two stages (2014 and 2022) must be taken into account to avoid surprises. NATO must be prepared for worst-case scenarios, not being able to trust the Kremlin's announced intent based on estimated strategic logic, and focus on actual Russian military capabilities in the region.

During the last Zapad military exercises, Russian and Belarusian planners practiced closing the Suwalki corridor by attacking from Belarus in the direction of Kaliningrad.[34] This plan has particularly relevant consequences after the outbreak of the 2022 Russo-Ukrainian War due to Moscow's inflammatory reaction to the European cutoff of goods flowing to Kaliningrad Oblast as part of the new sanctions regime. NATO will have to strengthen the logistics elements in the Suwalki Corridor area, taking into account the unilateral abrogation by Russia of the 1997 NATO-Russia Founding Act. The result is not unexpected, as Russia's behavior often sends specific signals of undermining stability and security in Europe.[35]

Through this political agreement, NATO has fulfilled its collective defense missions to the states that were once part of the Warsaw Pact by "ensuring the necessary interoperability, integration, and capability for reinforcement

[34] Chris Bott, "ZAPAD 2021 Brief," *Proceedings* 147, no. 9 (September 2021): 1,423, https://www.usni.org/magazines/proceedings/2021/september/zapad-2021-brief.

[35] John R. Deni, "The NATO-Russia Founding Act: A Dead Letter," Carnegie Europe (website), June 19, 2017, https://carnegieeurope.eu/strategiceurope/71385.

rather than by additional permanent stationing of substantial combat forces."[36] This agreement forces Russia to "exercise similar restraint in its conventional force deployments in Europe."[37] The premises of a "current and foreseeable security environment" were initially created, but the Russian side did not fully respect the conditions.[38] The political and military events of the last decade have experienced a gradual degradation of the assumptions of 25 years ago.

The British and Canadian ground forces should return to the mainland on a brigade level with 4,000 troops in their relatively small contingents in Estonia and Latvia. At the same time, the German ground forces should expand to the size of a brigade in Lithuania. In order to prevent any threats, in addition to the recent temporary increases in the US rotating presence, the permanent presence of armored units, combat aviation, electronic warfare, drones, engineers, and air defense units must be established. European countries with an important military dimension in the Alliance, like France, Italy, and Spain, must employ interoperable battalion-size units of approximately 800 troops each on permanent bases in Poland or Lithuania.

Logistical Challenges of Relocating NATO Capabilities on the Eastern Flank: Russia - Ukraine War Case Study

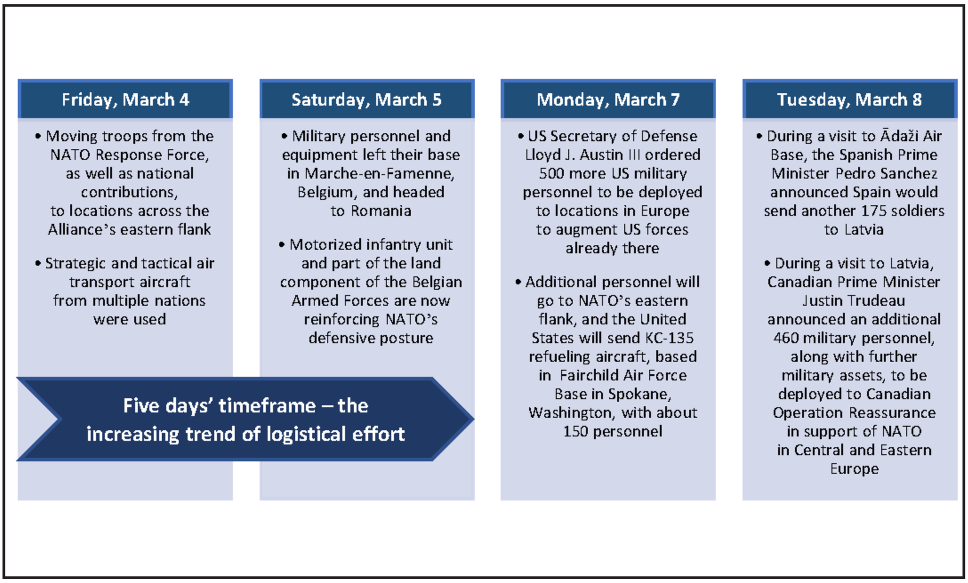
The growing security needs of Alliance members due to the risks posed by the Russian invasion of Ukraine have increased NATO's readiness and vigilance across Europe. The Alliance mechanisms effectively mobilized the logistical effort during a week at the beginning of March 2022. The mobilization of resources was efficient, as shown in figure 10-6, with thousands of troops deployed to the central and southeastern parts of the Alliance and more placed on standby.

The NATO Response Force (NRF) is a multinational force comprised of up to 40,000 land, air, maritime, and special operations personnel that NATO can deploy at short notice as needed. Since the end of February 2022, the Alliance has deployed forces to Romania, with France leading this year's highest-readiness element of the NRF. The Alliance transferred more than 350 soldiers, supplies, and armored vehicles from France for five days using 21 transport planes. The mission included a naval air group supporting a surveillance and air defense system.

[36] "Press Releases: Statement by the North Atlantic Council," NATO (website), March 14, 1997, https://www.nato.int/docu/pr/1997/p97-027e.htm.

[37] Antony J. Blinken, "Speech: The Stakes of Russian Aggression for Ukraine and Beyond," US Mission to International Organizations in Geneva (website), January 20, 2022, https://geneva.usmission.gov/2022/01/20/the-stakes-of-russian-aggression-for-ukraine-and-beyond/.

[38] Deni "NATO-Russia Founding Act."



Friday, March 4

- Moving troops from the NATO Response Force, as well as national contributions, to locations across the Alliance's eastern flank
- Strategic and tactical air transport aircraft from multiple nations were used

Saturday, March 5

- Military personnel and equipment left their base in Marche-en-Famenne, Belgium, and headed to Romania
- Motorized infantry unit and part of the land component of the Belgian Armed Forces are now reinforcing NATO's defensive posture

Monday, March 7

- US Secretary of Defense Lloyd J. Austin III ordered 500 more US military personnel to be deployed to locations in Europe to augment US forces already there
- Additional personnel will go to NATO's eastern flank, and the United States will send KC-135 refueling aircraft, based in Fairchild Air Force Base in Spokane, Washington, with about 150 personnel

Tuesday, March 8

- During a visit to Ādaži Air Base, the Spanish Prime Minister Pedro Sanchez announced Spain would send another 175 soldiers to Latvia
- During a visit to Latvia, Canadian Prime Minister Justin Trudeau announced an additional 460 military personnel, along with further military assets, to be deployed to Canadian Operation Reassurance in support of NATO in Central and Eastern Europe

Five days' timeframe – the increasing trend of logistical effort

Figure 10-6. Example of short-term actions using a variety of logistics
(Original by author)

US Navy F/A-18E Super Hornet fighters from the Nimitz-class aircraft carrier USS *Harry S. Truman* strengthened NATO's presence along the eastern flank. The missions increased vigilance and training for the joint air patrols of the Alliance and NATO enhanced Air Policing (eAP) efficiency.

The French Air and Space Force's Rafale fighters integrated with NATO's Allied Air Command can be refueled by A-330 multi-role tanker transport (MRTT) aircraft and can safeguard the skies above the eastern flank. They took off from their home base at Mont-de-Marsan, France, to fly combat air patrol missions. The A-330 MRTTs conduct refueling for three hours two times daily.[39]

From their home bases in the Netherlands, with air-to-air refueling, the Dutch air forces extended their air policing mission along the eastern flank utilizing F-16s and F-35s to fly enhanced vigilance activities. Four Royal Netherlands Air Force F-35 fighter jets landed at Graf Ignatievo Air Base near Plovdiv, Bulgaria, to safeguard the skies with the Bulgarian Air Force. Germany and the Netherlands plan to send Patriot

[39] Diana Stancy Correll, "USS *Truman* Aircraft Join Buildup of NATO Air Policing Patrols over Eastern Europe," *Navy Times* (website), March 4, 2022, https://www.navytimes.com/news/your-navy/2022/03/04/uss-truman-aircraft-join-buildup-of-nato-air-policing-patrols-over-eastern-europe; and Stefano D'Urso, "We Updated Our ORBAT Map with All the Assets Deployed across Eastern Europe for the Ukrainian Crisis," Aviationist (website), March, 10, 2022, https://theaviationist.com/2022/03/10/orbat-map-ukraine-update/.

missile systems to Slovakia to protect and safeguard Allied airspace in the region. According to NATO, we can cite multiple events and relocations of troops using various worldwide logistical resources in March 2022 over a few days.[40] Summarizing the case study, NATO has about 130 jets on high alert, and there are more than 120 Allied ships at sea, from the High North to the Mediterranean Sea.

Supply Chain Resilience

Interoperability Context and Operating Principles

It is very important to summarize the role of the Logistics Committee (LC), which "meets as the senior advisory body on logistics in NATO under the chairmanship of the Secretary General twice a year, in joint civil and military sessions. It has two permanent co-chairmen, namely the Assistant Secretary General for Defense Policy and Planning (ASG DPP), and the Deputy Chairman of the Military Committee (DCMC). The Committee reports jointly to both the Council and the MC, reflecting the dependence of logistics on both civil and military factors."[41]

It operates as a joint civil and military body with representatives from the Security Committee, NATO's Support Agency, Standardization Agency, and other sectors participating. Member countries are represented by senior civil and military representatives. The Logistics Committee carries out its work through six subordinate bodies, of which the first two play the principal role:

- the Logistics Committee Executive Group
- the Movement and Transportation Group
- the Standing Group of Partner Logistic Experts
- the Logistic Information Management Group
- the Petroleum Committee

[40] SHAPE Public Affairs Office, "News Archive: NATO Allies Send Reinforcements to the Eastern Flank," NATO (website), March 13, 2022, https://shape.nato.int/news-archive/2022/nato-allies-send-reinforcements-to-the-eastern-flank.

[41] "Logistics," June 21, 2017.

- the Ammunition Transport Safety Group[42]

There is a close cooperation between the Logistics Committee and the Civil Emergency Planning Committee (CEPC) for coordinating support of the Alliance's overall defense effort using civil resources. There are interrelated responsibilities between these two committees and their related subcommittees to cooperate closely. The Logistics Committee also works with the NSPA, NATO Standardization Office, and the Committee of the Chiefs of Military Medical Services in NATO.[43]

The Joint Support and Enabling Command (JSEC) has an important role in crises and conflicts as "a static operational headquarters with multinational personnel directly subordinate to the Supreme Allied Commander Europe (SACEUR)."[44] The JSEC's mission is a 360-degree approach to contribute to enablement and help the Alliance to reinforce and sustain military forces in the Euro-Atlantic area. The JSEC was established in 2018 and reached its full operational capability in 2021. About 300 Allied soldiers and civilians are assigned to JSEC activity.

Changes Triggered by Threats and Incidents

The overlapping areas between terrorist groups and criminal networks have further reduced the differentiation between national responsibility and international reaction. Illicit trafficking and proliferation activities overlap with illegal immigration routes and international criminal hubs. Inevitably, sovereign prerogatives and national border controls grow at odds with the global nature of the terrorist threat.[45] Undergoverned or poorly governed spaces on the margins of NATO's territory expose areas of Europe to the risk of terrorist infiltration, and many adapt their logistics to fit the different legislative frameworks.[46] NATO's Allied Maritime Strategy recognized in 2011 its importance and roles in maritime security due to an increase in transnational criminal and terrorist activities. It included support for law

[42] "Logistics," June 21, 2017.

[43] "Logistics Committee," NATO (website), August 3, 2015, https://www.nato.int/cps/en/natohq/topics_61715.htm.

[44] Joint Support and Enabling Command (JSEC), NATO JSEC (website), n.d., https://jsec.nato.int.

[45] Stefano Santamato and Marie-Theres Beumier, *The New NATO Policy Guidelines on Counterterrorism: Analysis, Assessments, and Actions*, Institute for National Strategic Studies (INSS) Strategic Perspectives, no. 13 (Washington, DC: Center for Strategic Research/INSS/National Defense University Press, February 2013), https://www.files.ethz.ch/isn/161531/Strategic-Perspectives-13.pdf.

[46] Jean-Louis Bruguière, *What I Couldn't Say: Interviews with Jean-Marie Pontaut,* ed. Robert Laffont (Paris: RAND Europe, 2009); and Erik J. G. van de Linde et al., *Quick Scan of Post 9/11 National Counter Terrorism Policymaking and Implementation in Selected European Countries* (Leiden: RAND Europe, 2002), https://www.rand.org/pubs/monograph_reports/MR1590.html.

enforcement and the prevention of the transport and deployment of weapons of mass destruction.[47] A major challenge is the interconnection of supply chains that attract additional mutually reinforcing threats. Successful approaches have included classic situations where NATO assets and contributions in patrolling the maritime environment are well known. Due to today's global financial challenges, smarter approaches are needed to boost capacity and manage resources.

NATO's contribution to the fight against terrorism has been considered outside of its mainstream activity for a long time. Following the September 11 attacks, NATO's response included the decision, taken at the 2002 Prague Summit, to "adapt" the Alliance to the challenge of terrorism and make its assets and capabilities available to the fight against terrorism. Civil emergency planning (CEP) was the discipline that supported the Alliance's counterterrorism efforts more than any other, with the exclusion of NATO's operational engagements.

CEP's contribution to the CBRN response and consequence management directly results from its civil defense role in mitigating the effects of possible nuclear, biological or chemical warfare. Similarly, most of the planning capacity and progress in critical infrastructure protection is due to CEP's role in supporting the logistics of the war effort and ensuring the normal activity of civil society. NATO's role in airspace management and maritime security is linked to the Alliance's main military defense mandate and can be considered.

Resilience Commitment and Logistics

Resilience, a society's ability to withstand only partially predictable shocks, necessarily combines civil society preparedness and military capacity available at any given time. The principles of resilience included in Article 3 of the Alliance's founding treaty "In order more effectively to achieve the objectives of this Treaty, the Parties, separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack" reflects the individual commitment of every ally to maintaining and strengthening NATO's resilience. This commitment also reduces the vulnerability of NATO as a whole.[48]

[47] "Alliance Maritime Strategy – II. The Maritime Security Environment, Paragraph 6," NATO (website), March 18, 2011, https://www.nato.int/cps/en/natohq/official_texts_75615.htm.

[48] "The North Atlantic Treaty, Washington D.C. – April 4, 1949," NATO (website), last updated April 10, 2019, https://www.nato.int/cps/en/natolive/official_texts_17120.htm.

Beyond programmatic statements, several aspects of resilience are inextricably linked to the interdependencies of the supply-chain elements. Starting at the Warsaw summit in 2016 and reaffirmed in 2021, there are "seven baseline requirements for national resilience against which member states can measure their level of preparedness. These requirements reflect the core functions of continuity of government, essential services to the population and civil support to the military, which must be maintained under the most demanding circumstances. They are all connected, which means "if one area is impacted, another may suffer as a result."[49] They consist of: assured continuity of government and critical government services, resilient energy supplies internally and across borders, the ability to deal effectively with uncontrolled movement of people, and resilient food and water resources; the ability to deal with mass casualties; resilient civil communications systems; and resilient transport systems. These requirements ensure "NATO forces can move across Alliance territory rapidly and that civilian services can rely on transportation networks, even in a crisis."[50]

Most of the seven requirements are either major dependencies on the supply of goods or services in the supply chain, or, more dangerously, influence, govern, or even block the supply chain. An important component of the resilience of the supply chain and its logistics components is represented by exercise-type activities such as Locked Shields, the largest and most complex international live-fire exercise, organized by the NATO Cooperative Cyber Defense Center of Excellence (CCDCOE) in Tallinn, Estonia. These exercises, run annually for over a decade, are conducted in real time with participants from the civilian, military, and critical infrastructure areas working under pressure simulating complex cyberattacks.[51]

Pillars of Supply Chain Resilience

In order to be truly effective, "any action NATO will take in the field of counter-terrorism will have to take into account the principle of Nonduplication and Complementarity further elaborated by the policy's commitment to coordinate and leverage NATO resources with those of other nations and international organizations."[52] NATO is shifting its focus to specific programs and areas in which it has unique assets that can

[49] "Resilience, Civil Preparedness, and Article 3," NATO (website), June 11, 2021, https://www.nato.int/cps/en/natohq/topics_132722.htm.

[50] "Resilience, Civil Preparedness, and Article 3."

[51] SHAPE Public Affairs Office, "Exercise Locked Shields 2022 Concludes," NATO (website), April 23, 2022, https://shape.nato.int/news-archive/2022/exercise-locked-shields-2022-concludes.

[52] Santamato and Beumier, *New NATO Policy Guidelines*.

support Allied counterterrorism efforts. It provides a logical structure that goes from defining NATO's purpose and role in combating terrorism to priority areas of engagement. In order to develop advanced resilience capabilities, approaches derived from standard logistics global expertise that involve actions and features are described below.

- Increasing the ability to absorb shocks by minimizing the risk of disrupting the supply chain and other severe impacts, for example, by flexibly switching from primary to secondary supply routes, rebalancing the worldwide supply, or switching suppliers.

- Redesigning the global network and increasing flexibility by using dual-source redundancy or approaches that include nearshoring to reduce dependence on complex global logistics and vertical integration to bring production to critical components including semiconductors or other in-house IT elements. How to balance flexibility, efficiency and effectiveness when redesigning a global network can only be done on the basis of comprehensive risk assessments.

- New parameters for supply-chain buffers when the organization needs to develop an effective multitier inventory strategy, which tends to generate new stock targets in the high-volatility nodes of the supply chain. The Alliance should assess the capacity resetting or changing of utilization targets and identify triggers that signal when to add capacity or activate ready-to-use capacity based on usage trends.

- Managing suppliers proactively by assessing the criticality of suppliers and adjusting relationships with all of them to ensure the availability of resources. This action gains transparency in several areas of suppliers to assess upstream risks properly. To manage vendor reliability correctly, traditional KPIs (such as "on time, in full") and other risky KPIs (such as geographic distribution) can be monitored. Suppliers may be asked to change the way information is shared.

Reaction speed when disruption occurs is needed to manage normal volatility, avoid interruptions, and increase resilience. NATO must apply agile ways of working in different functions and regions where the logistics system operates. Any deviation must be managed transparently and a forward-looking view of risks and opportunities must be developed through simulation. The rapid response should support multi-enterprise supply-chain management, end-to-end risk management, and planning scenarios based on anticipation and simulation.

Conclusion and Further Developments

Ensuring the advanced logistics and resilience of the supply chain within the Alliance is a complex one and cannot be addressed by a simplifying algorithm. The functional interdependence between the logistics nodes and the involved economic actors requires an increased capacity to adapt to the economic, social, and political conditions in challenging times.

In the medium term, hybrid threats, advanced security, and the integrity of the supply chain will have to be addressed in collaboration with legacy risk and accelerated digital transformation. This process is especially pertinent as the Alliance must expand its logistical capabilities as former neutral countries join NATO. To address the complex and integrated approach of convergent threats to NATO logistical infrastructures and their ripple effects, NATO must develop the Integrated Maritime Logistics Concept.[53]

An important direction of development is represented by the need to accelerate the development of supply-chain virtualization in the context of emerging threats and autonomous operations in conjunction with the concrete needs of cybersecurity and cyber-resilience in logistics. To improve the resilience of the supply chain at the Alliance's level, NATO must consider a series of interrelated elements to increase the ability to absorb shocks and dysfunctions, develop alternative supply-chain buffers, reduce dependencies, and redesign the global supply chain to build a more agile, resilient, and responsive system.

Following analysis of exercises addressing these challenges, multiple decision-making levels of the Alliance found that the lack of sufficient workers persists, affecting efficiency in the short and medium term. NATO must find solutions for increasing the number of human operators or a correct balance between systems with human assistance and automatic ones.

[53] "Combined Joint Operations from the Sea Centre of Excellence (CJOS COE)," in *NATO-Accredited Centres of Excellence: 2021 Catalogue* (Norfolk, VA: Supreme Allied Commander Transformation, 2021), https://www.cmdrcoe.org/fls/pubs/2021_COE_CATALOGUE.pdf, 21.

The new threats have raised major concerns at the Alliance level and prompted NATO leaders to ask the Secretary-General to lead a forward-looking reflection on the future of NATO, called NATO 2030. As part of this effort, the Alliance seeks to strengthen its commitment with civil society, the young generation, and the private sector. During 2021, six NATO 2030 dialogues explored how the private sector can contribute address major technology-based security risks and increase overall resilience.[54]

Critical infrastructure and supply-chain security dialogues will help NATO to understand the private-sector perspective on critical security and defense infrastructure challenges. Technology is playing an increasingly important role in military capabilities and operations, so supply chains need to remain secure and resilient across the Alliance, especially as the importance of private actors grows.[55]

[54] "NATO-Private Sector Dialogues Focus on NATO 2030 Initiative," NATO (website), June 2, 2021, https://www.nato.int/cps/en/natohq/news_184601.htm.

[55] "Critical Infrastructure and Security of Supply Chains," GLOBSEC (website), April 21, 2021, https://www.globsec.org/events/critical-infrastructure-and-security-of-supply-chains.

Select Bibliography

"Civilian Expert Helps NATO Establish Communication Lines." NATO (website). January 27, 2012. https://www.nato.int/cps/fr/natohq/news_83812.htm?selectedLocale=en.

"CLC/TS 50701: Railway Applications – Cybersecurity." European Standards (website). 2021. https://www.en-standard.eu/clc/ts-50701-2021-railway-applications-cybersecurity.

"Critical Infrastructure and Security of Supply Chains." GLOBSEC (website). April 24, 2021. https://www.globsec.org/events/critical-infrastructure-and-security-of-supply-chains.

Deni, John R. "NATO Must Prepare to Defend Its Weakest Point—the Suwalki Corridor." *Foreign Policy*. March 3, 2022. https://foreignpolicy.com/2022/03/03/nato-must-prepare-to-defend-its-weakest-point-the-suwalki-corridor.

Randelhoff, Martin. "Eyjafjallajökull – die Auswirkungen in Europa und der ganzen Welt." Zukunft Mobilität (website). May 1, 2010. http://www.zukunft-mobilitaet.net/849/analyse/eyjafjallajoekull-fazit-schaden-flugverkehr-global.

Santamato, Stefano, and Marie-Theres Beumier. *The New NATO Policy Guidelines on Counterterrorism: Analysis, Assessments, and Actions*. Institute for National Strategic Studies (INSS) Strategic Perspectives, no. 13. Washington, DC: Center for Strategic Research/INSS/National Defense University Press. February 2013. https://www.files.ethz.ch/isn/161531/Strategic-Perspectives-13.pdf.

Transportation Security Administration. *Enhancing Public Transportation and Passenger Railroad Cybersecurity*, Security Directive 1582-21-01. Washington, DC: Department of Homeland Security, December 31, 2021. https://www.tsa.gov/sites/default/files/sd-1582-21-01_signed.pdf.

About the Contributors

Lucas M. Cox, at the time of writing this publication, was an intern with the Strategic Studies Institute at the US Army War College and a graduate of the University of Washington Henry M. Jackson School of International Studies with a degree in international security, foreign policy, peace, and diplomacy and a double minor in political science and Russian, Eastern European, and Central Asian studies with a focus on the former Soviet economic and security spheres. He is also the 2023 University of Washington Triana Deines Rome Center Intern and will begin an internship at NATO's Science and Technology Organization in April 2023.

Denise Feldner is a lawyer and technology expert based in Berlin. She founded Bridgehead Advisors, a strategy consulting firm. She works in private equity and is a member of the board of a bank. She was CEO of a group of elite universities and represented them on the Global Council of Research-Intensive University Networks. Feldner was chief of staff to the president of Heidelberg University and legal adviser to the CEO of InnovationLab GmbH. She was a member of the "Weiter.Denken. Ordnen.Gestalten" project of Herrhausen Society, Deutsche Bank.

Trevor P. Helmy graduated from the University of Washington Henry M. Jackson School of International Studies in June 2022. In addition to his work with the University of Washington NATO Emerging Technology Task Force, he has contributed to the University of Washington Center for Human Rights' research on US deportation flights. He plans to attend law school and pursue a career in international public interest law.

Frank J. Kuzminski is a US Army officer and strategist. A native of Poland, he emigrated to the United States in 1990. He graduated from the United States Military Academy in 2004 with a bachelor of science degree in electrical engineering and was commissioned as an Infantry officer. After serving in multiple operational assignments worldwide, Kuzminski was assigned to the Army Staff at the Pentagon, and he later served as a strategic plans officer with I Corps at Joint Base Lewis-McChord, Washington. He is currently a doctoral candidate in international studies at the University of Washington. He holds a master of public administration degree from Harvard University. He is married with two children and speaks Polish and French.

Sarah J. Lohmann is a visiting research professor of security studies at the US Army War College, an assistant professor of international studies at the University of Washington, and a nonresident fellow with the American Institute for Contemporary German Studies at Johns Hopkins University. She is a co-lead of the NATO Science and Technology project "Energy Security in an Era of Hybrid Warfare." She holds a bachelor's degree in communications and German from Wheaton College (Illinois), a master of international service degree from American University (Washington, DC), and a doctorate in political science from the Universität der Bundeswehr (Neubiberg, Germany).

Marcus Mohlin is an active-duty officer serving at the Swedish Armed Forces Headquarters as lead for long-term analysis at the Plans and Policy Division. With a background initially as a submarine officer and then as a commanding officer of the Navy Counter SOF unit, he also has operational experience from Angola as a military observer with the UN and as staff officer in the NATO-led operation in Bosnia and Herzegovina. Mohlin holds a doctorate from the Finnish Defence University and has lectured and published on strategic theory and defense planning at the Swedish Defence University in Stockholm where he is a senior lecturer.

Aleksander Olech is a visiting lecturer at the Baltic Defence College and analyst at the Defence24. Previously, he served as the director of the Security Programme at the Institute of New Europe. A graduate of the European Academy of Diplomacy and War Studies University, he has undertaken research at several international institutions, among others, the Université Jean Moulin III in Lyon, the Institute of International Relations in Prague, the Institute for Peace Support and Conflict Management in Vienna, the NATO Energy Security Centre of Excellence in Vilnius, and the NATO StratCom in Riga. Olech is the scholarship holder of the OSCE & UNODA Peace and Security Programme and the NATO 2030 Global Fellowship. His main research interests include security in Central and Eastern Europe, terrorism, energy security, challenges in Africa, and the role of NATO and the EU with regard to hybrid threats.

Wuraola Oyewusi is a Nigerian pharmacist and data scientist with expertise in clinical health care and application of data-science methods. Her research spans a range of use cases from natural language processing (NLP) to health care and data curation. She lives in the United Kingdom and is the recipient of the Global Talent Visa in AI, Machine Learning, and Data Science.

Gabriel T. Raicu is the vice-rector for research and innovation at the Maritime University of Constanta (CMU) and the director of the Center for Excellence in Maritime Cyber Security (MarCySCoE) at CMU. He developed the first maritime cybersecurity simulator at CMU since 2017, the year when the International Maritime Organisation (IMO) began to address maritime cybersecurity threats. He is the initiator and coordinator of the annual BSCySeC#X conferences (BlackSea Cybersecurity Maritime Conferences), this year in its sixth edition. He has numerous contributions in the area of early warning systems for cyber/energy security, in the areas of protection of critical maritime systems and the development of cybersecurity infrastructures. He is also the president of CYSCOE – Cyber Security Cluster of Excellence.

Silke Ruhl, VMD, holds a master of science degree in public health She joined the army in 2008 after completing her doctoral thesis to work in the field of food and water health inspection. She became a specialist for microbiology during this time and was deployed in KFOR and ISAF as leading laboratorian at the veterinary laboratory and served as a public health expert for the mission. She joined the NATO Centre of Excellence for Military Medicine (NATO MILMED COE) in 2016 and became the branch chief of the FHPB in 2018. The focus of the branch is deployment health surveillance and FHP information for NATO.

Sabrina Schulz is the co-CEO of Econnext, a company holding in the area of renewable energy and sustainability. She was the executive director of the Sustainable Development Solutions Network Germany. Between 2018 and 2020, she served as head of the Berlin office at KfW, Germany's national public bank. From 2012 to 2018, she was the director of the Berlin office at E3G-Third Generation Environmentalism, a climate and energy think tank. From 2009 to 2011, she was a policy adviser on climate and energy to the British High Commission in Canada. Schulz holds a master of arts degree in public policy and management from the University of Potsdam, for which she also studied at the University of Konstanz and the Université Catholique de Louvain. She also holds a master of arts degree in international politics and a PhD from the University of Wales at Aberystwyth in the United Kingdom.

Máté Tóth has spent 12 years working for the NATO Centre of Excellence for Military Medicine (NATO MILMED COE), mostly in communication and information management roles. From 2016 to 2018, he also worked for the United Nations High Commissioner for Refugees as the information management coordinator for Central

Europe's nine countries. In his current role as senior communications officer, he is the technical lead of multiple innovation projects of the NATO MILMED COE, dealing with medical information management (such as the Medical Machine-Translation Project, the Global Health Dashboard, and the Near-Real-Time Surveillance Project).

Megan A. Ward is an interdisciplinary researcher who studies disinformation, ideological extremism, and law enforcement communities. She received her PhD from the University of Washington Henry M. Jackson School of International Studies and her master of science degree in homeland security from San Diego State University. She is the recipient of the Women in Defense National Scholarship and the Joseph and Yetta Blau Award for Excellence in Research. Ward currently acts as an International Policy Institute cybersecurity fellow and has published articles for the Wilson Center Science and Technology Innovation Program (STIP) Series.

The United States Army War College educates and develops leaders for service at the strategic level while advancing knowledge in the global application of Landpower.

The purpose of the United States Army War College is to produce graduates who are skilled critical thinkers and complex problem solvers in the global application of Landpower. Concurrently, it is our duty to the Army to also act as a "think factory" for commanders and civilian leaders at the strategic level worldwide and routinely engage in discourse and debate on the role of ground forces in achieving national security objectives.

The Strategic Studies Institute publishes national security and strategic research and analysis to influence policy debate and bridge the gap between military and academia.

The SSI Live Podcast Series provides access to SSI analyses and scholars on issues related to national security and military strategy with an emphasis on geostrategic analysis. https://ssi.armywarcollege.edu/ssi-live-archive

The Center for Strategic Leadership provides strategic education, ideas, doctrine, and capabilities to the Army, the Joint Force, and the nation. The Army, Joint Force, and national partners recognize the Center for Strategic Leadership as a strategic laboratory that generates and cultivates strategic thought, tests strategic theories, sustains strategic doctrine, educates strategic leaders, and supports strategic decision making.

The School of Strategic Landpower provides support to the US Army War College purpose, mission, vision, and the academic teaching departments through the initiation, coordination, and management of academic-related policy, plans, programs, and procedures, with emphasis on curriculum development, execution, and evaluation; planning and execution of independent and/or interdepartmental academic programs; student and faculty development; and performance of academic-related functions as may be directed by the Commandant.

The US Army Heritage and Education Center makes available contemporary and historical materials related to strategic leadership, the global application of Landpower, and US Army Heritage to inform research, educate an international audience, and honor soldiers, past and present.

The Army Strategic Education Program executes General Officer professional military education for the entire population of Army General Officers across the total force and provides assessments to keep senior leaders informed and to support programmatic change through evidence-based decision making.

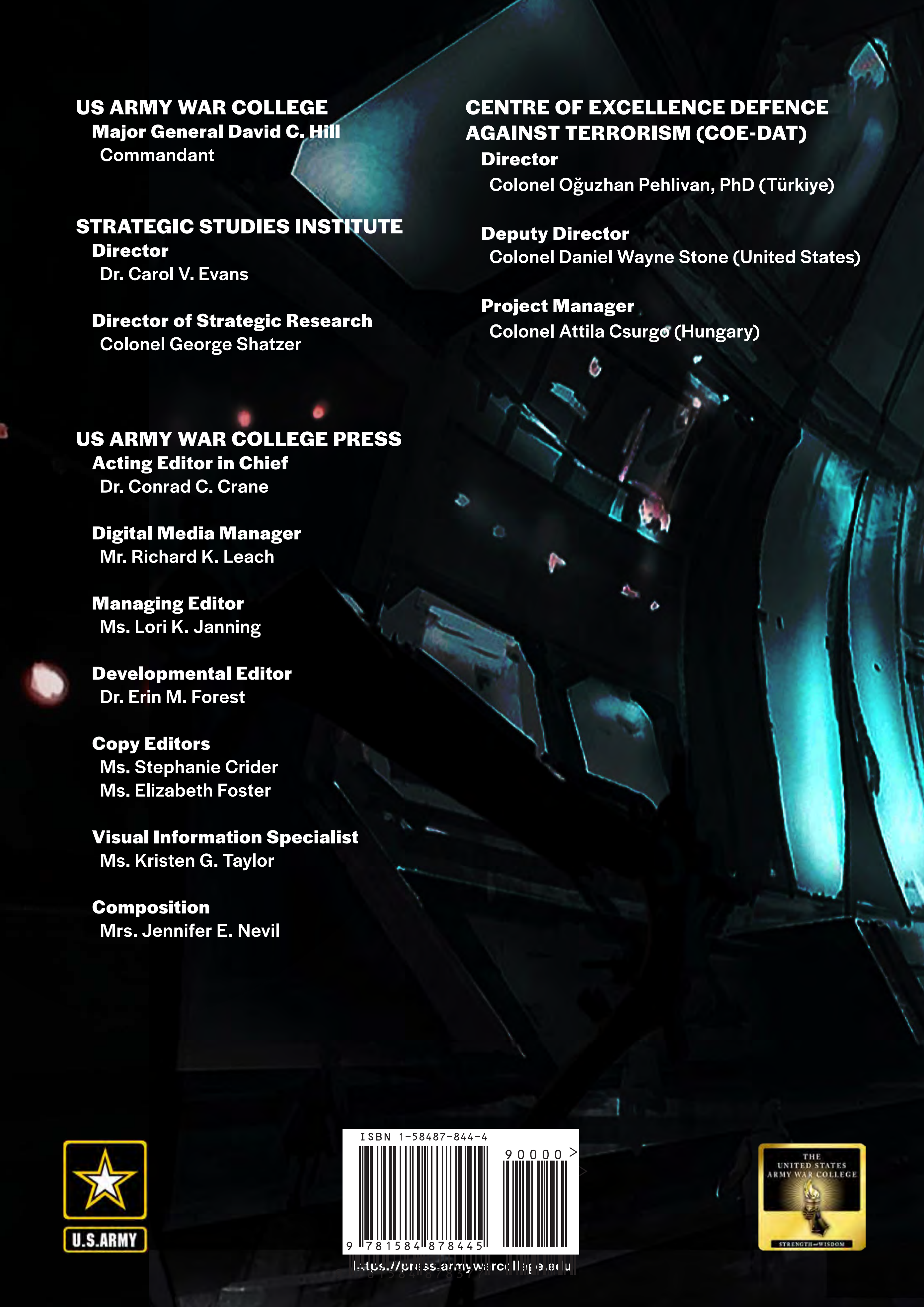
US ARMY WAR COLLEGE PRESS

The US Army War College Press supports the US Army War College by publishing monographs and a quarterly academic journal, *Parameters*, focused on geostrategic issues, national security, and Landpower. Press materials are distributed to key strategic leaders in the Army and Department of Defense, the military educational system, Congress, the media, other think tanks and defense institutes, and major colleges and universities. The US Army War College Press serves as a bridge to the wider strategic community.

All US Army Strategic Studies Institute and US Army War College Press publications and podcasts may be downloaded free of charge from the US Army War College website. Hard copies of certain publications may also be obtained through the US Government Bookstore website at https://bookstore.gpo.gov. US Army Strategic Studies Institute and US Army War College publications may be quoted or reprinted in part or in full with permission and appropriate credit given to the US Army Strategic Studies Institute and the US Army War College Press, US Army War College, Carlisle, PA. Contact the US Army Strategic Studies Institute or the US Army War College Press by visiting the websites at: https://ssi.armywarcollege.edu and https://press.armywarcollege.edu.

The US Army War College Press produces two podcast series. Decisive Point, the podcast companion series to the US Army War College Press, features authors discussing the research presented in their articles and publications. Visit the website at: https://ssi.armywarcollege.edu/decisive.

Conversations on Strategy, a Decisive Point podcast subseries. features distinguished authors and contributors who explore timely issues in national security affairs. Visit the website at: https://ssi.armywarcollege.edu/cos.


US ARMY WAR COLLEGE

Major General David C. Hill
Commandant

STRATEGIC STUDIES INSTITUTE

Director
Dr. Carol V. Evans

Director of Strategic Research
Colonel George Shatzer

US ARMY WAR COLLEGE PRESS

Acting Editor in Chief
Dr. Conrad C. Crane

Digital Media Manager
Mr. Richard K. Leach

Managing Editor
Ms. Lori K. Janning

Developmental Editor
Dr. Erin M. Forest

Copy Editors
Ms. Stephanie Crider
Ms. Elizabeth Foster

Visual Information Specialist
Ms. Kristen G. Taylor

Composition
Mrs. Jennifer E. Nevil

CENTRE OF EXCELLENCE DEFENCE AGAINST TERRORISM (COE-DAT)

Director
Colonel Oğuzhan Pehlivan, PhD (Türkiye)

Deputy Director
Colonel Daniel Wayne Stone (United States)

Project Manager
Colonel Attila Csurgo (Hungary)

ISBN 1-58487-844-4
90000
9 781584 878445

https://press.armywarcollege.edu