11-16-2022

What Ukraine Taught NATO about Hybrid Warfare

Sarah J. Lohmann

Chuck Benson

Vytautas Butrimas

Georgios Giannoulis

Gabriel Raicu

See next page for additional authors

Authors
Sarah J. Lohmann, Chuck Benson, Vytautas Butrimas, Georgios Giannoulis, Gabriel Raicu, Michael Bervell, Milagro Castilleja, Chris Clyde, Christopher J. Eaton, Alex Elmore, Ryan Fisk, Erin Hodges, Frank J. Kuzminski, Vishwa Padigepati, Caitlin Quirk, Brenton M. Riddle, Shuo Zhang, Lucas Cox, and Samira Oakes

U.S. ARMY WAR COLLEGE
SSI
STRATEGIC STUDIES INSTITUTE

UNITED STATES ARMY WAR COLLEGE PRESS
Carlisle Barracks, PA

COLLABORATIVE STUDIES

WHAT UKRAINE TAUGHT NATO ABOUT HYBRID WARFARE

Sarah J. Lohmann

DECISIVE POINT
The USAWC Press Podcast Companion Series

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

What Ukraine Taught NATO about Hybrid Warfare

Sarah J. Lohmann
Editor and Lead Author

Chuck Benson, Vytautas Butrimas,
Georgios Giannoulis, Gabriel T. Raicu
Main Contributing Authors

Michael Bervell, Milagro Castilleja, Christopher Clyde,
Christopher J. Eaton, Thomas A. Elmore, Ryan Fisk, Erin Hodges,
Frank J. Kuzminski, Vishwa Padigepati, Caitlin Quirk,
Brenton M. Riddle, Shuo Zhang
Case Study Authors

Lucas Cox, Samira Oakes
Interns

November 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 are those of the authors and 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 1-58487-843-6

Cover Photo Credits

Front Cover

Basic Leader Course students from the 1st Battalion, 279th Infantry Regiment, 45th Infantry Brigade Combat Team move across a road during the BLC field training exercise at the Yavoriv Combat Training Center on the International Peacekeeping and Security Center in western Ukraine, on October 11.

Photo by: Sergeant Anthony Jones, 45th Infantry Brigade Combat Team

Date Taken: October 11, 2017

Date Posted: October 17, 2017,01:55 a.m.

Photo ID: 3867576

VIRIN: 171011-A-RH707-461

Website: https://www.dvidshub.net/image/3867576/thunderbirds-learn-lead-ukraine

Cyber Attacks (taken from the Norse attack map)

Photo by: Christiaan Colen

Source: Flickr

Website: https://www.flickr.com/photos/christiaancolen/21206509269/in/photolist-xDzBDT-yy9ruu-yzviiN-yzvhGY-yiWUoa-yzvi37-yiWTQX-yiS92w-yy9rwy-yy9rro-244P6UQ-244P6Ys-qqSfPF

Hand Painted Watercolour Ukraine Flag Background

Source: Image by kjpargeter on Freepik. This cover has been designed using assets from Freepik.com

Website: https://www.freepik.com/free-vector/hand-painted-watercolour-ukraine-flag-background_25033790.htm

Back Cover

Thunderbirds Learn to Lead in Ukraine

Specialist Jeremy Pisciotta, a Claremore, Oklahoma resident and member of Headquarters and Headquarters Company, 1st Battalion, 279th Infantry Regiment, provides security for his squadmates during the Basic Leader Course field training exercise at the Yavoriv Combat Training Center on the International Peacekeeping and Security Center in Western Ukraine, on October 11.

Photo by: Sergeant Anthony Jones, 45th Infantry Brigade Combat Team

Date Taken: October 11, 2017

Date Posted: October 17, 2017, 1:55 a.m.

Photo ID: 3867586

VIRIN: 171011-A-RH707-158

Website: https://www.dvidshub.net/image/3867586/thunderbirds-learn-lead-ukraine

Table of Contents

Foreword

Russia's invasion of Ukraine in 2022 forced the United States and its NATO partners to confront the impact of hybrid warfare far beyond the battlefield. Targeting Europe's energy security, Russia's malign influence campaigns and malicious cyber intrusions are affecting global gas prices, driving up food costs, disrupting supply chains and grids, and testing US and Allied military mobility. This study examines how NATO's adversaries are using hybrid warfare, highlights the vulnerabilities in critical energy infrastructure and energy dependencies that exist across the Alliance, and provides mitigation strategies available to the member states.

Cyberattacks targeting the renewable energy landscape during Europe's green transition are increasing, making it urgent that new cybersecurity tools are developed to protect these emerging technologies. No less significant are the cyber and information operations targeting energy security in Eastern Europe as it seeks to become energy independent from Russia and the economic coercion used against Germany, Poland, the Netherlands, Denmark, Finland, and Bulgaria to stop gas from flowing to parts or all of these countries. China's malign investments in Southern and Mediterranean Europe are enabling Beijing to control the critical energy infrastructure of some NATO member states at a critical moment in the global balance of power.

What Ukraine Taught NATO about Hybrid Warfare will be an important reference for NATO officials and EUCOM and US installations operating in the European theater. With US military and NATO troop mobility often dependent on host critical infrastructure for their energy needs, it is more crucial than ever for the United States to increase its supply of technologies to foster energy independence for US military installations in Europe, which have seen a 30 percent increase in troop presence since the beginning of the war.

The technologies highlighted in section two analyze tools for enhancing cybersecurity and energy independence. It is equally important that resilience planning occurs as Europe faces energy shortages that are predicted to lead to grid blackouts, gas shortages, heating challenges, and communications interruptions starting this year and continuing through 2025. The handbook's country-by-country analysis will be helpful for personnel charged with providing cyber support and security, mobility, and communications to the United States and its allies.

The study team of cyber policy analysts—including US military officers, University of Washington students, and researchers from NATO partner nations—led by Dr. Sarah Lohmann offers important mitigation strategies for addressing energy security challenges in today's gray warfare environment. The Strategic Studies Institute is proud to publish this important contribution to the understanding of how to strengthen energy security in an era of hybrid warfare.

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

Acknowledgments

The US Army War College is pleased to acknowledge its partnership with the Henry M. Jackson School of International Studies at the University of Washington on this book project. The case studies included in the book are the work of University of Washington students and US Army War College fellows from Dr. Lohmann's spring 2021 class on NATO, energy and cybersecurity. Our thanks go to University of Washington faculty members Ambassador John Koenig and Dr. Chuck Benson for their valuable insights and contributions as part of this educational partnership.

The authors would also like to thank the NATO Science and Technology Organization and NATO STO (SAS-163) colleagues Dr. Arnie DuPuy and Dr. Dan Nussbaum for their leadership. In early 2019, Dr. DuPuy, Dr. Nussbaum, and Dr. Lohmann initiated a research road map examining the impacts of hybrid warfare on energy security in Europe. One year later, the NATO Science and Technology Office approved the study.

The authors hope the initial research on the cyber aspect of that study can create a foundation for the broader project to be completed and published at the end of 2022. Current advanced critical energy infrastructure warning and cyber threat mitigation systems in place are not adequate to ensure safety and resilience when emerging technologies being integrated into energy systems are not cyber secured. There are large differences between NATO member states in cyber mitigation capabilities and standards.

Thanks also go to the 21st Theater Sustainment Command in Kaiserslautern, Germany, for providing several rounds of feedback and incorporating Dr. Lohmann and her research into its valuable work. Our gratitude also goes to Brigadier General Joseph E. Hilbert of the 7th Army Training Command in Grafenwoehr, Germany, for his interest in the project and for asking the right questions, and Colonel Christopher R. Danbeck for his input and support for research site visits. The authors' appreciation goes to Colonel Michael A. Davis, commandant of the NATO School in Oberammergau, Germany, for bringing the NATO perspective to the study. The contributions from the NATO Energy Security Centre of Excellence and the NATO Hybrid Centre of Excellence were also important to the success of this project.

Our generous appreciation is owed to US Army War College interns Lucas Cox, Ryan Fisk, Erin Hodges, and Samira Oakes for their map prowess and tireless research, editing, and layout assistance. We are also grateful to Casey Dye and the US Army War College's peer reviewers for their work on the book's glossary. Most importantly, deep gratitude is owed to mentors Dr. Carol Evans, Colonel George Shatzer, and Dr. John Deni, who were always ready for a brainstorm—and without whom this book would not have been possible.

Executive Summary

The Russian invasion of Ukraine has highlighted the long-term energy dependencies on Moscow that Europe will neither be able to resolve quickly, nor without great sacrifice. Russia's hybrid warfare—a combination of kinetic strikes against key infrastructure, information manipulation, malign finance, economic coercion, and cyber operations—has used Ukraine to target the heart of Europe's energy security. This war has forced the Continent to consider how to realize its economic, environmental, and geostrategic energy goals on its own.

This study found systemic dependencies and cyber vulnerabilities in critical energy infrastructure throughout the European continent could impact the Alliance's political stability and threaten military effectiveness. Forward mobility and troop readiness is affected directly by energy shortfalls and increasing cyber vulnerabilities across NATO. The following main findings related to cyber and malign influence provide a sobering view of the challenges of hybrid warfare on energy security in NATO nations.

Increased Cyber Threats Threaten Energy Critical Infrastructure

Russia and its agents have successfully penetrated energy networks in Europe and North America and deployed malware to undermine critical systems and infrastructure in the target country. Since the invasion of Ukraine, significant cyberattacks have impacted NATO member states.

Advanced critical energy infrastructure warning and cyber threat mitigation systems currently in place are not adequate to ensure safety and resilience when emerging technologies being integrated into energy systems are not cyber secured. There are large differences between NATO member states in cyber mitigation capabilities and standards.

This book identifies potential solutions to mitigate cyberattacks and increase energy independence for the militaries of NATO member states and to prevent cyber vulnerabilities to energy critical infrastructure. These options include a new generation of cyber early warning systems (CEWS) and microgridding.

Energy Sector Supply-Chain Vulnerabilities Impact Military Operations

Moody's Analytics has reported the greatest risk to the global supply chain is now caused by the Russia-Ukraine military conflict, not the pandemic.

With Russia supplying 43 percent of Europe's natural gas and 40 percent of the world's palladium (used for semiconductors) and Ukraine supplying 70 percent of the world's neon (used to create computer chips), the prolonged uncertainty of the conflict could continue to affect the global supply chain severely.

Going forward, supply-chain components will continue to be subject to major threats from different subchains that interact directly with low-security scrutiny. Cybersecurity vulnerabilities in the gas, power, and nuclear industries are pervasive, increasing the threats due to the interactions within each subchain.

Strategies for higher supply-chain resilience could include: (1) supply-chain mapping and modeling to better predict supply and demand, (2) diversifying suppliers, (3) shortening supply chains, and (4) automation with a careful evaluation of cyber risks.

Malign Influence Is Directly Impacting Critical Energy Infrastructure

Russia views cyberattacks, hacking, and the spread of disinformation as instruments of foreign policy and national security interests. Through compromised websites (such as news sources and official government sites), Russian operatives published fabricated articles, stories, quotes, and other documents criticizing the United States and NATO's presence in Eastern Europe. Information operations and malign influence specifically target the energy sector in countries like Poland, Romania, and Germany, with operational and economic impact.

Early detection of disinformation campaigns is crucial to prevent malicious actors from escalating and exploiting this activity. To solve this problem, a task force could be established within NATO's Joint Intelligence and Security Division to establish a network for detecting and countering disinformation in its nascent stages. The information would then be classified according to its impact (including threat level in terms of timeline) and its possibility of spreading to a local, state, national or international level.

These findings and recommendations are not exhaustive. By using emerging tools to foster energy independence and cybersecurity while countering malign influence, NATO can navigate from a position of strength and resilience in the conflict-laden days ahead.

Introduction

Sarah J. Lohmann

The week before Russia invaded Ukraine in February 2022, the Russian Main Intelligence Directorate (GRU) attacked the websites of Ukraine's defense ministry, army, and two largest banks in a distributed denial-of -service attack called "the largest assault of its kind in the country's history."[1] Of even greater concern was a data-wiping malware found on computers across Ukrainian critical infrastructure organizations (from financial to aviation and IT) on February 23, the same day Putin announced military action against the Donbas.[2] Was this a coincidence?

According to NATO: "Hybrid threats combine military and nonmilitary as well as covert and overt means, including disinformation, cyberattacks, economic pressure, deployment of irregular armed groups and use of regular forces."[3] This book examines how hybrid warfare (including disinformation, cyberattacks, and economic investment and pressure aimed at the energy sector) is shaping the battlefield and rattling energy security across NATO states and beyond. In this era of hybrid warfare, cyberattacks or disinformation campaigns and kinetic attacks happen in coordination in the same limited time frame. Alternatively, cyber and information operations can cause the destruction or disablement of critical energy infrastructure even more potently, and at a lesser cost, than kinetic attacks. Indeed, on the day Ukraine was supposed to start "isolation mode" tests for its new power network to begin the process of decoupling from the Russian grid, Russia started a full-scale invasion of the country.[4]

1. Valerie Hopkins, "A Hack of the Defence Ministry, Army and State Banks Was the Largest of Its Kind in Ukraine's History," *New York Times* (website), https://www.nytimes.com/2022/02/15/world/europe/ukraine-cyberattack.html; and Foreign, Commonwealth, and Development Office of the Government of the United Kingdom, "Government Response: UK Assess Russian Involvement in Cyberattacks on Ukraine," February 18, 2022.

2. Sean Lyngaas, "Key Ukrainian Websites Hit by Series of Cyberattacks," *CNN* (website), February 24, 2022, https://www.cnn.com/2022/02/23/europe/ukraine-government-commercial-organizations-data-wiping-hack/index.html.

3. "NATO's Response to Hybrid Threats," NATO (website), June 7, 2022, https://www.nato.int/cps/en/natohq/topics_156338.htm.

4. Andrew Lee, "War in Ukraine: Russia Attacks Nation Looking to Renewables and EU Grid for Energy Freedom," Recharge (website), February 24, 2022, https://www.rechargenews.com/energy-transition/war-in-ukraine-russia-attacks-nation-looking-to-renewables-and-eu-grid-for-energy-freedom/2-1-1173808.

While this ground war serves as a violation of Ukrainian sovereignty and international norms, Moscow's hybrid warfare has actively targeted Ukraine's energy security since 2014. It has used cyberattacks on the grid and disinformation campaigns, and it has sought to divide NATO Allies around issues such as the certification of the Nord Stream 2 pipeline, which was supposed to deliver gas from Russia to Germany without transiting Ukraine. Using the pipeline as a bargaining chip to escalate conflict with Ukraine, European natural gas prices increased by 62 percent the day of the invasion.[5]

While Russia's methods and targets are not new, Europe can no longer look away. The costs are too high. It is clear the Ukraine conflict is providing NATO members with daily basic lessons in hybrid warfare. Following a major Russian cyberattack on Ukraine's grid repelled by the Ukrainian government on April 8, the cyber agencies of the Five Eyes warned on April 20 that Russia was preparing to target the critical infrastructure of countries that sanctioned Russia.[6]

Perhaps the most clear-cut example of critical infrastructure targeting is Germany, which remained Russia's largest importer of Russian gas, paying $9.5 billion for the product in the first two months of the war alone.[7] At the same time, Germany is a major distributor of Russian gas to other NATO countries and is the economic powerhouse of Europe. Any attacks on Germany's critical infrastructure and economy are felt deeply across the Alliance.

Germany's renewable energy sector has been especially vulnerable to cyberattacks since the invasion of Ukraine. A February 24, 2022, cyberattack on a satellite providing services to Ukraine knocked 5,800 wind turbines in Germany and Central Europe offline, affecting 11 gigawatts of power.[8]

5. Kate Duffy, "Russian Gas Flows to Europe via Ukraine Reportedly Jumped Nearly 40% on Thursday, Underscoring the Continent's Dependence on Putin's Energy," Business Insider (website), February 25, 2022, https://www.businessinsider.in/politics/world/news/russian-gas-flows-to-europe-via-ukraine-reportedly-jumped-nearly-40-on-thursday-underscoring-the-continents-dependence-on-putins-energy/articleshow/89831410.cms.

6. AJ Vicens, "Russian Hackers Thwarted in Attempt to Take Out Electrical Grid, Ukrainians Say," Cyber Scoop (website), April 12, 2022, https://www.cyberscoop.com/ukrainian-electrical-grid-industroyer2-russia-sandworm/; and Cybersecurity and Infrastructure Security Agency (CISA), Alert AA22-110A, "Russian State Sponsored and Criminal Cyber Threats to Critical Infrastructure," CISA (website), April 20, 2022, https://www.cisa.gov/uscert/ncas/alerts/aa22-110a.

7. Dipaneeta Das, "Germany the Top Buyer of Russian Gas at $9.5 Billion since War Began in Ukraine," April 28, 2022, https://www.republicworld.com/world-news/europe/germany-the-top-buyer-of-russian-gas-worth-9-dot-5bn-since-war-began-in-ukraine-report-articleshow.html.

8. Joseph Henry, "Europe Cyberattack Results to 'Massive' Internet Outage; about 5,800 Wind Turbines Went Offline," Tech Times (website), March 5, 2022, https://www-techtimes-com.cdn.ampproject.org/c/s/www.techtimes.com/amp/articles/272624/20220305/europe-cyberattack-results-massive-internet-outage-5-800-wind-turbines.htm.

On April 12, another cyberattack against the German wind-energy company Deutsche Windtechnik caused the company to shut down the remote-control systems of 2,000 wind turbines for a day. Conti, the pro-Russian government ransomware group, launched a cyberattack against another turbine maker, Nordex SE, and forced the company to shut down its IT systems.[9] Interrupting Europe's energy supply through a cyberattack can be much cheaper than kinetic attacks because the current microgrids and wind turbines often do not yet have comprehensive cybersecurity protection.[10]

Step by step, Russia has used hybrid warfare to challenge energy security in Ukraine and across NATO member states as Moscow seeks to beat back NATO influence and expand its power on the world stage. Now an armed conflict, the Ukraine crisis is a case study in how Russia's hybrid warfare has challenged energy security with an impact across NATO, far beyond Ukraine's borders.

For this study, the International Energy Agency (IEA) definition of energy security will be used. The IEA defines energy security as "the uninterrupted availability of energy sources at an affordable price."[11] Energy sources can include electricity, nuclear, oil, gas, coal, and renewables. In this context, NATO has stated that "attacks on complex energy infrastructure by hostile states, terrorists or hacktivists can have repercussions across regions. Since electricity is key to the global energy transition, power infrastructure security is becoming the cornerstone of energy security."[12] This book includes a focus on cyberattacks on the electric grid and on energy critical infrastructure—to include systems operating pipelines, grids, and nuclear energy. It examines how hybrid warfare is being used by NATO's adversaries, what vulnerabilities in critical energy infrastructure and energy dependencies exist across the Alliance, and what mitigation strategies are available to the member states.

---

9. Catherine Stupp, "European Wind Energy Sector Hit in Wave of Attacks," *Wall Street Journal* (website), April 25, 2022, https://www.wsj.com/articles/european-wind-energy-sector-hit-in-wave-of-hacks-11650879000#:~:text=European%20Wind-Energy%20Sector%20Hit%20in%20Wave%20of%20Hacks,governments%20move%20to%20transition%20away%20from%20Russian%20fuel?msclkid=7f9116ddc7cd11ec9178cad5c4c63099.

10. Vytautas Butrimas, "Assessment Study of Cybersecurity of Smart-grid Technologies Employed in Operational Camps," Energy Security Centre of Excellence (website), August 11, 2021, https://enseccoe.org/data/public/uploads/2021/11/vb-cyber-asses-study-v1dot2dot3-oct-1-2021-cyber-sg-for-mil-camps.pdf.

11. "Energy Security: Ensuring the Uninterrupted Availability of Energy Sources at an Affordable Price," International Energy Agency (website), December 2, 2019, https://www.iea.org/areas-of-work/ensuring-energy-security.

12. "NATO's Role in Energy Security," NATO (website), June 23, 2021, https://www.nato.int/cps/en/natohq/topics_49208.htm.

How to Use This Handbook

Written as a handbook of mitigation policies for energy security, the first two sections on vulnerabilities and mitigation strategies and the new technologies being built to address hybrid attacks on energy security can be used in the classroom, whether in a professional military education (PME) context or in a public university context. They are also meant to inform NATO and military officials of the policies and tools available to them in the current gray energy battleground context.

Specifically, the first section assesses key vulnerabilities in critical energy infrastructure in a hybrid warfare context. It starts with an examination of the main gray warfare threats to critical energy infrastructure, including to information technology, operational technology, and industrial control systems. It then looks at vulnerabilities in an Internet of Things environment that are especially prevalent in the critical energy infrastructure sector.Finally, it looks at malign influence and the impact of disinformation on energy security. Each “vulnerabilities” chapter ends with recommendations for successful defense.

The second section provides new research on key hybrid warfare mitigation technologies, including a new generation of early warning systems and independent, non-hackable energy sources such as microgrids.

For commanders and officers ensuring military mobility, communications, and logistics where host critical infrastructure could challenge the mission, section three contains useful briefs and maps on cyber and disinformation targets. This section provides case studies on cyber and disinformation vulnerabilities across NATO member states, mitigation strategies currently in place to deal with those weaknesses, and what members should do to build robust defenses. The NATO countries analyzed were chosen based on their strategic and military relevance for NATO’s energy security.

The Baltics, currently geolocated on the front line to Russia’s hybrid war, are in the process of separating from Russia’s power network. The southeastern member states, with key military hubs for air and sea, have other challenges. Romania, rich in renewables, must ensure it is cyber secured in the Internet of Things environment. Countries like Italy, Türkiye, and Greece have critical infrastructure strongly tied to China and Russia. This dependence is already causing energy insecurity. Plus, Western and Central Europe, with their up-till-now reliance on Russian oil and gas, are now involved in a cyber, information, and economic war that has rattled markets and caused gas and oil prices to soar to historic levels not seen since the 1970s.

The case studies section also provides a cyber and disinformation attack vortex map for each country. The threat information and estimates included in these maps were based on open-source information identifying where major critical energy infrastructure and military assets were located. These data were paired with unclassified information on threat timelines and analysis from country, military, and topic experts and sources. The first rendition of the maps was created in summer and fall 2021. Many of the areas identified in red as highly likely to be attacked in the next six months did indeed see malicious cyberattacks and intrusions or malign information operations. The maps were updated after receiving input from US Army commands and after the invasion of Ukraine in 2022.

It is our hope this study will guide the US Army, NATO officials, energy-sector owners and operators, and engaged citizens to understand the disinformation and cyber operations impacting critical energy infrastructure in NATO states. This handbook presents new research on ways to strengthen energy independence and cyber best practices to mitigate the negative impacts of hybrid war.

Select Bibliography

Butrimas, Vytautas. "Assessment Study of Cybersecurity of Smart-grid Technologies Employed in Operational Camps." Energy Security Centre of Excellence (website). August 11, 2021. https://enseccoe.org/data/public/uploads/2021/11/vb-cyber-asses-study-v1dot2dot3-oct-1-2021-cyber-sg-for-mil-camps.pdf.

Cybersecurity and Infrastructure Security Agency (CISA). Alert AA22-110A. "Russian State Sponsored and Criminal Cyber Threats to Critical Infrastructure." CISA (website). April 20, 2022. https://www.cisa.gov/uscert/ncas/alerts/aa22-110a.

Foreign, Commonwealth, and Development Office of the Government of the United Kingdom. "Government Response: UK Assess Russian Involvement in Cyberattacks on Ukraine." February 18, 2022.

Henry, Joseph. "Europe Cyberattack Results to 'Massive' Internet Outage; About 5,800 Wind Turbines Went Offline." Tech Times (website). March 5, 2022. https://www-techtimes-com.cdn.ampproject.org/c/s/www.techtimes.com/amp/articles/272624/20220305/europe-cyberattack-results-massive-internet-outage-5-800-wind-turbines.htm.

International Energy Agency (IEA). "Energy Security: Ensuring the Uninterrupted Availability of Energy Sources at an Affordable Price." IEA (website). December 2, 2019. https://www.iea.org/areas-of-work/ensuring-energy-security.

Lee, Andrew. "War in Ukraine: Russia Attacks Nation Looking to Renewables and EU Grid for Energy Freedom." Recharge (website). February 24, 2022. https://www.rechargenews.com/energy-transition/war-in-ukraine-russia-attacks-nation-looking-to-renewables-and-eu-grid-for-energy-freedom/2-1-1173808.

NATO. "NATO's Response to Hybrid Threats." NATO (website). June 7, 2022. https://www.nato.int/cps/en/natohq/topics_156338.htm.

NATO. "NATO's Role in Energy Security." NATO (website). June 23, 2021. https://www.nato.int/cps/en/natohq/topics_49208.htm.

Stupp, Catherine. "European Wind Energy Sector Hit in Wave of Attacks." *Wall Street Journal* (website). April 25, 2022. https://www.wsj.com/articles/european-wind-energy-sector-hit-in-wave-of-hacks-11650879000#:~:text=European%20Wind-Energy%20Sector%20Hit%20in%20Wave%20of%20Hacks,governments%20move%20to%20transition%20away%20from%20Russian%20fuel?msclkid=7f9116ddc7cd11ec9178cad5c4c63099.

— Section 1 —

Vulnerabilities

— 1 —

Defending against Cyber Threats to Critical Energy Infrastructure

Vytautas Butrimas

ABSTRACT: In the context of a decade of a record number of cyberattacks in the public and private sectors, this chapter discusses the cyber vulnerabilities of NATO's critical energy infrastructure. Smart technology, information and data storage, and attacker anonymity provide significant vulnerabilities for state and non-state actors seeking to target energy infrastructure in order to intimidate adversaries, economize offensive assets, or disrupt energy flows to vital military and civilian sectors. Cyberattacks on energy infrastructure can target informational technologies, operational technologies, or industrial control systems. Major attacks on energy infrastructure between 2000 and 2021 demonstrate evolving attacker capabilities and the need for more advanced security methods.

Keywords: energy security, smart technologies, cybersecurity, Stuxnet, ISOC, IACS, critical energy infrastructure, cyber threats, critical infrastructure, information technology, operational technology, SolarWinds, Colonial Pipeline, NotPetya, ICS, APT, norms, industrial cybersecurity

The methods of hybrid war described in this study represent a new and more sinister trend in conflict characterized by secrecy, cynicism, and the convenience of denial and a significant challenge to democratic societies based on trust, transparency, and respect for the rights of others. While cybersecurity in the information technology (IT) or office IT realm has witnessed the development and implementation of measures to address threats from cyberspace for decades, industrial cybersecurity practitioners are in catch-up mode. As a milestone, we can compare Bill Gates' famous e-mail sent to Microsoft employees about emphasizing security in its products in 2002.[1] On the other hand, efforts by industrial control system (ICS) practitioners to implement secure coding practices for configuring program logic controllers (PLCs) that are the backbone of industrial automation and control systems (IACS) only began in summer 2020.[2] This change came despite a decade of recorded cyberattacks on PLCs and industrial control systems found in nuclear facilities, petrochemical plants, and steel mills.[3]

In the military sphere where energy is used, the situation is similar. For example, the application of "smart" technologies such as the "smart grid" for military camps of the future creates an additional new task besides protecting the information system.[4] This application will bring together a mass of sensitive and confidential data as it will provide information on the camp's operational activity, its energy supply, and its organization. Thus, adversaries could leverage these data to neutralize the operation of the camp.

On the other hand, in addition to the information or data, the technologies used to operate the smart grid can also be targeted, resulting in service degradation, equipment damage, loss of life, or harm to the environment.[5] Thus, adversaries could disrupt the physical processes involved with the generation, storage, and distribution of power along the smart grid and also degrade or neutralize camp operations.[6] Therefore, it is necessary to apply industry best practices and industrial standards to ensure the cybersecurity, safety, reliability, and performance of the technologies used.

1. Bill Gates, "Trustworthy Computing," Wired (website), January 25, 2002, https://www.wired.com/2002/01/bill-gates-trustworthy-computing/.

2. "Version 1.0 of the PLC 20 Is Due for Release in November 2020," ISA (website), 2020, https://top20.isa.org/top/yearly.

3. Vytautas Butrimas, "Targeting Control and Safety Instrumented Systems (SIS): New Escalation of Cyber Threats to Critical [Energy] Infrastructure," https://www.enseccoe.org/data/public/uploads/2018/10/v.butrimas-new-escalation-of-cyber-threats-to-critical-energy-infrastructure.pdf.

4. Gail Reitenbach, "The U.S. Military Gets Smart Grid," Power (website), January 1, 2012, https://www.powermag.com/the-u-s-military-gets-smart-grid/.

5. Jeff St. John, "The Military Microgrid as Smart Grid Asset," Green Tech Media (website), May 17, 2013, https://www.greentechmedia.com/articles/read/the-military-microgrid-as-smart-grid-asset.

6. Lily Hay Newman, "The Hail Mary Plan to Restart a Hacked US Electric Grid," Wired (website), November 14, 2018, https://www.wired.com/story/black-start-power-grid-darpa-plum-island/.

Why would a motivated advanced persistent threat (APT) actor consider using cyber means to attack the critical energy infrastructure (CEI) of NATO or a member nation? Here are potential reasons:

- To disrupt the fuel (energy) supply just when their military does something they know will draw NATO's response.
- To contribute to service disruptions in dependent civilian infrastructures (transport, telecom, water).
- To intimidate.
- To economize on offensive assets, cyber weapons are reusable while physical weapons (bombs and humans) are not.
- It is effective, cheap (for a state or state-supported actor), and deniable.

There are several challenges in developing, and, most importantly, in implementing cybersecurity policies in the industrial sector. Successful efforts will be judged by the way the following three important questions are answered.

- What are we protecting?
- From which cyber threats?
- How do we protect identified assets from identified threats in the most cost-effective way?

In terms of deciding what to protect, if one is in government, one tends to say government information systems and data need to be protected. Recognition of the dependency on the electric grid that supplies electricity to those chosen assets, however, is missed. If the electricity goes out because of a cyberattack or unintentional incident, then government information systems that need electricity to operate will also fail. This failure impacts the economy and well-being of society through a prolonged failure in the power supply. Resources needed to protect everything are limited, so time and consideration are required in determining what is truly critical and deserves funding.

In answering the second question, it is a mistake to focus only on the threats from hackers, socially motivated hacktivists, and cybercriminals.

States and the “cyber samurai” working for them cannot be safely ignored as sources of APT threats, especially to critical infrastructure. Stuxnet was a targeted cyber weapon developed by a state to attack equipment belonging to the critical infrastructure (CI) of another state. It was a highly sophisticated cyberattack on the systems used to monitor and control a critical industrial process. The apparent success of this attack, which brought no punishment to the attacker and was executed at little cost, has attracted a lot of attention. In recent years, targeted cyberattacks on critical infrastructure have increased. Many of the attacks reveal signs of state involvement, ranging from the UK’s cyber intrusion of Belgian telecommunications company Belgacom to the Russian Chief Intelligence Office’s “Sandworm” team, whose activities have targeted critical infrastructures of the energy sector and other sectors.[7]

In seeking to protect critical energy infrastructure, one must keep in mind that this operating environment is different from the traditional information system or website management systems. This environment is characterized by real-time control and safety systems designed to provide some product or service (such as electricity, fuel, or gas) safely and reliably. These systems were designed with a distinct set of assumptions. One of them was that they would not be connected to the Internet, and the other was that no one would be trying to attack them intentionally.

The answer to the third question focuses on the development of cyber capacity. This area concerns passing laws, developing risk assessments and policies, imposing regulations and standards, and creating units (such as an industrial security operations center) to participate in the implementation of cybersecurity policies for improving resilience of critical systems and effective response to cyberattacks and incidents. Without trained staff who are knowledgeable about plant operations and cyber forensic investigations, no solutions, tools, or early warning instruments will have an effect on reducing the risk to safety, reliability, performance, and improving resilience.

What can be done to lower cyber risks in the energy sector? The first thing that can be done is to be more aware of the importance of answering the three questions discussed above. A process must determine what critical assets and processes need to be protected in the energy and supporting sectors (such as electricity and transportation). To achieve these goals successfully, cybersecurity capacity needs to be

7. Louk Faesen et al., *The Cyber Arms Watch: Uncovering the Stated & Perceived Offensive Cyber Capabilities of States* (Hague: Hague Centre for Strategic Studies, July 2022), 170, https://hcss.nl/wp-content/uploads/2022/05/Cyber-Arms-Watch-HCSS-2022-V.2.pdf; and Andy Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin’s Most Dangerous Hackers* (New York: Doubleday, 2019).

developed. Nations and operators of critical infrastructure need to become more aware of the best practices and standards for securing available industrial control systems. Extra time and effort will be required to convince management and stockholders that spending money on security is justified. The results of answering the first two questions will provide rational, evidence-based answers to questions raised by management.

The next challenge is related to the first one mentioned above, namely, lack of awareness of the complexity of dealing with threats emanating from cyberspace. In terms of ensuring the cybersecurity of critical infrastructure, IT thinking dominates. It is too frequently assumed the IT equipment sitting on a desk is the same as the IT equipment used to monitor and control critical real-time industrial process taking place in gas pipelines, electric grids, transportation (seaports, shipping, trains, aircraft, and highway tunnels), and manufacturing systems. They are not the same and are designed according to different security and engineering criteria. IT-imposed solutions by IT professionals who poorly understand industrial controls systems can have surprising and potentially dangerous results.

In 2008, for example, the Hatch nuclear reactor in the United States experienced an emergency shutdown for two days because of a problem that occurred from executing a software upgrade on a single computer.[8] A bridge of understanding and collaboration is needed between IT cybersecurity professionals and ICS professionals who work with engineering systems. In order to address vulnerabilities, develop strategies, and propose effective solutions for the protection of critical infrastructure from threats emanating from cyberspace, we need to understand the role played by the technologies employed in the energy and other CI sectors—information technology (IT), operational technology (OT), and industrial control systems (ICS).[9]

To determine the best ways to respond to cyberattacks on critical energy infrastructure, it is necessary to define the cyber technologies used to run them and examine the differences between them. All these technologies may be used together, as is often seen in CI-sector industries. They are further described on the next page.

8. Brian Krebs, "Cyber Incident Blamed for Nuclear Power Plant Shutdown," *Washington Post* (website), June 5, 2008, https://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958.html.

9. Global Cybersecurity Alliance, "Industrial Automation and Control System Taxonomy," https://gca.isa.org/hubfs/21-29%20-%20ISAGCA/ISAGCA-IACS%20Taxonomy%20Definitions%20of%20Terms.pdf.

- Information technologies are very data or information centric and are applied in the administrative or office part of a business or commercial enterprise. In a utility providing electricity to customers, for example, IT supports the administration of an enterprise and the interactions outside the company by providing web services, e-mail to employees, and in-processing customer accounts in the billing and accounting department. Its security priority is to protect the data or information processed.[10] The selected cybersecurity measures ensure the confidentiality (granting access to only the authorized user), integrity (protection of the data), and availability (on-demand access to the information).

- Operational technologies are characteristic of the operations center or control room of an electric power, water, or gas utility. These technologies use special hardware and software to monitor and control a physical process such as the generation and distribution of electricity to customers connected to a power grid or the flow of fuel or water down a pipeline. The operators in the control room view information from field devices closest to the physical process through a Human Machine Interface (HMI).[11] In many cases, this equipment would be a Windows PC at a workstation running special monitoring and control software. Operational technologies should remain separate from the IT network, however, this is not always done in practice.

- Industrial control systems are mostly computer based and are used by infrastructures and industries to monitor and control sensitive processes and physical functions. They collect sensor measurements and operational data from the field, process and display this information, and relay control commands to local or remote equipment. They are the hardware and software closest to the actual physical process: remote terminal units (RTUs), PLCs, actuators, drives, sensors, safety instrumented systems (SIS), and field devices.[12] For example, a PLC on a fuel pipeline monitors and reacts to information about the

10. "Debate over IT, OT and Control Systems," Infracritical (website), November, 22, 2019, http://icsmodel.infracritical.com/.

11. "Debate over IT, OT and Control Systems."

12. "Debate over IT, OT and Control Systems."

> flow of fuel provided by a sensor physically placed on the pipe. It acts according to a program entered by the engineer according to changes in preprogrammed set points. The PLC may react by starting a pump or closing a valve depending on a change in the flow in the pipeline or as a response to a command from the control room operator in the OT side.

While having much in common in terms of being computers, IT, OT, and ICS have different security and safety requirements stemming from their functions. Industrial cybersecurity is about enterprise-wide security polices and capabilities employed to ensure safety, reliability, and desired performance of the physical processes being monitored and controlled. The goal of this effort is not just to protect information (IT and OT), but to protect the physical process (ICS).

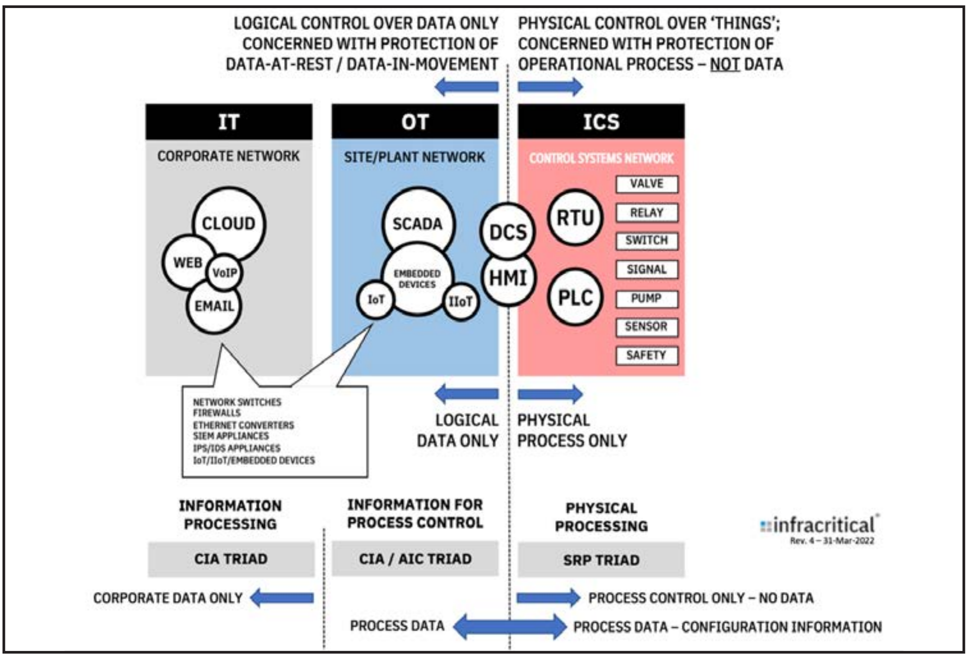

Figure 1-1. IT, OT, and ICS in critical infrastructure
Source: "Debate over IT, OT and Control Systems."

If the IT and OT fail, the operation in the office and control room stops. Even without the IT and OT, however, the physical process will still do something. That is why imposing an office IT cybersecurity measure may not be applicable in an industrial environment. A best cybersecurity practice found in an office IT environment, such as preserving confidentiality with a robust password policy (long alphanumeric and changed often), may not be useful in an industrial environment where failure to enter a correct password in time of emergency may result in damage to property, loss of life, and damage to the environment.

In figure 1-2, cyberattacks on all three parts of a utility/industrial operation are illustrated. If a policymaker thinks protecting "SCADA" will be enough to address cyber threats to critical infrastructure then placing emphasis on employing industry-standard office IT security policies will fail to address the most dangerous attacks (namely, on the ICS monitoring and controlling a physical process, not to mention the physical process itself). Figure 1-2 demonstrates which aspects of CEI were targeted during attacks that occurred between 2010 and 2021.

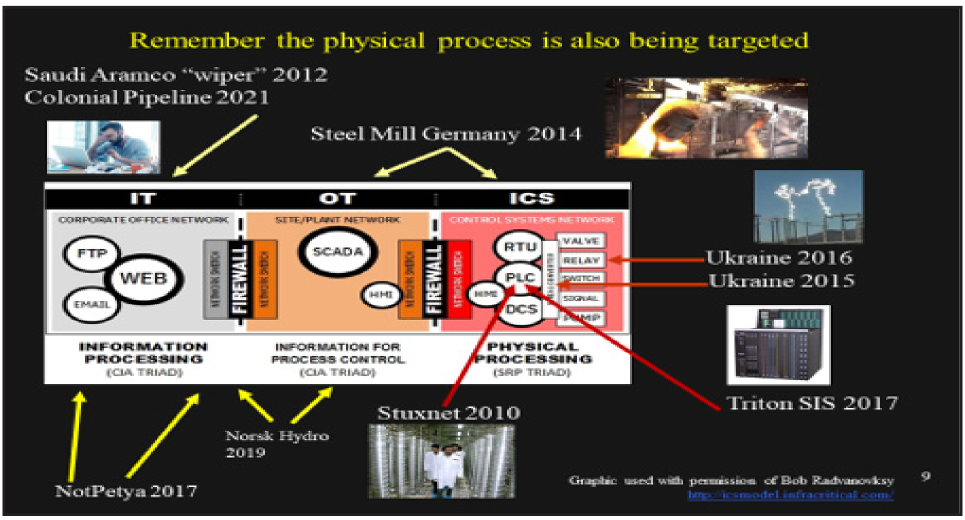

Figure 1-2. Targeted aspects in cybersecurity attacks
Graphic used with permission of Robert Radvanofsky

Case Studies of Incidents Relevant to Industrial Cybersecurity of Critical Infrastructure

The following cases studies present unsettling but continuing trends in industrial cybersecurity.

Maroochy Water Services 2000

This attack is different from the subsequent instances on this list in that it was not the action of a state or criminal organization. There continues to be a trend of substantial weakness existing from intentional, internal destruction by knowledgeable employees.[13]

This event was an intentional, targeted attack by a knowledgeable person on an industrial control system. A disgruntled former subcontractor showed his displeasure at a municipality that refused to hire him permanently by using his insider knowledge of the control systems used in the treatment and distribution of drinking water. His actions caused the control system to experience a series of faults—pumps were not running when they should have been, alarms were not reporting to the central computer, and there was a loss of communication between the central computer and various pumping stations.[14]

The threat of a knowledgeable insider causing havoc in an industrial operation is the most potentially dangerous of threats to the safety, reliability, and performance of industrial operations.

Stuxnet 2010

Stuxnet, the first state-developed cyber weapon, was a computer code capable of producing physical/kinetic effects on the target device or system to attack the critical infrastructure (nuclear enrichment process) of another state. The United States and Israel developed a code that targeted the PLCs of Iran's Natanz nuclear facility, causing centrifuges to fail. It sought a specific network configuration and remained innocuous to other machines.[15]

This attack was a turning point in cyberspace security. Cybersecurity professionals began to understand that the most sophisticated cyberattacks now extended to the engineering behind the technologies used to support the operations of critical infrastructure. The methods employed in this attack appeared repeatedly in cyberattacks on critical infrastructure (such as disabling safety systems, providing false data to operators about the physical process, and manipulating and causing physical destruction of equipment to the surprise of control room personnel). In short, attacks like Stuxnet take away operator view and control of a physical process.[16]

13. Marshall Abrams, "Malicious Control System Cybersecurity Attack Case Study–Maroochy Water Services, Australia," July 3, 2008, https://apps.dtic.mil/sti/pdfs/AD1107275.pdf.

14. Abrams, "Malicious Control System."

15. Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," Wired (website), November 3, 2014, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

16. Ralph Langner, "To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve" (Arlington, VA: Langner Group, 2013), https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf.

Saudi Aramco 2012

One of the world's largest oil companies was the victim of the largest denial-of-computer cyberattack to date as passwords were stolen and computers prevented from rebooting. Approximately 30,000 office IT hard drives were erased in the company offices by a hacker group calling themselves the "Cutting Sword of Justice" while ships waited at port without ordering or invoice information.[17] The cyberattack did not reach into the CI operations, and no equipment or processes were affected. For the Saudis, however, this cyberattack threatened not just its CEI but its economy.[18]

Havex 2014 Malware Attack

According to reports from the Department of Homeland Security Industrial Control Systems Computer Emergency Response Team (DHS ICS-CERT), this reported malware (also known as Dragonfly, Energetic Bear) targeted software/firmware download websites of manufacturers of industrial control systems.[19] Compromised vendor software that customers download from vendor sites allows attackers to access customer networks (including those that operate critical infrastructure).[20] Commentators compared this malware to Stuxnet, since the sophistication and choice of target pointed to nation-state involvement.[21] According to a Symantec analysis, this malware provided a platform for conducting cyber-espionage activities that gave the "attackers the ability to mount sabotage operations against their victims," and, if the attackers had used the sabotage capabilities available, they "could

17. Jose Pagliery, "The Inside Story of the Biggest Hack in History," *CNN Business* (website), August 25, 2015, https://money.cnn.com/2015/08/05/technology/aramco-hack/; US Department of Homeland Security (DHS), "Shamoon," *ICS-CERT Monthly Monitor*, September 2012, https://www.cisa.gov/uscert/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2012.pdf; and Lucian Constantin, "Kill Timer Found in Shamoon Malware Suggests Possible Connection to Saudi Aramco Attack," Computer World (website), August 23, 2012, https://www.computerworld.com/article/2491501/kill-timer-found-in-shamoon-malware-suggests-possible-connection-to-saudi-ar.html.

18. *Al Arabiya News* with AFP, "Saudi Aramco Says Cyber Attack Targeted Kingdom's Economy," Regulatory Cyber Security: The FISMA Focus IPD (website), December 9, 2012, https://www.thecre.com/fisma/?p=4177.

19. "ICS Alert (ICS-ALERT-14-176-02A): ICS Focused Malware (Update A)," US Cybersecurity and Infrastructure Security Agency (CISA) (website), June 27, 2014, https://www.cisa.gov/uscert/ics/alerts/ICS-ALERT-14-176-02A.

20. "ICS Alert (ICS-ALERT-14-176-02A)."

21. Nicole Perlroth, "Russian Hackers Targeting Oil and Gas Companies," *New York Times* (website), June 30, 2014, http://www.nytimes.com/2014/07/01/technology/energy-sector-faces-attacks-from-hackers-in-russia.html?_r=2.

have damaged or disrupted the energy supply in the affected countries."[22] This event should cause anyone who accepts cyber espionage as being part of traditional spying to pause and consider its ramifications.

German Steel Mill 2014

According to an official government report, advanced, persistent threat actors were able to jump across office IT networks to the control networks and eventually access the physical process.[23] Operators were unable to shut down the operation after losing view and control, resulting in physical damage.[24] To quote from the report: "The breakdowns led to the uncontrolled shutdown of a blast furnace, leaving it in an undefined state and resulting in massive damage."

Ukraine December 2015 Cyberattack on Regional Power Grid

Advanced, persistent threat actors succeeded in penetrating the office IT of a utility providing electricity to customers in a region of Ukraine. After conducting reconnaissance, mapping, and acquiring access privileges, they succeeded in acquiring operator view and control at the OT level and proceeded to open breakers at over 30 substations. Over 250,000 customers lost power in the winter just before Christmas. The attackers planted malicious firmware on the serial port servers used to communicate between SCADA control and the remotely located affected substations, causing them to become disabled permanently. The perpetrator ran a previously planted disk-wiper malware (as seen in Saudi Arabia in 2012) attack on the workstations in the control room. With the loss of the hardware and software (SCADA) used for the view and control of the power grid, the operator had to reestablish power and operations manually by sending engineers out to the substations to close the breakers manually and restore power.[25]

22. Symantec, "Dragonfly: Cyber Espionage Attacks against Energy Suppliers" (Mountain View, CA: Symantec Corporation, July 2014), 3, https://docs.broadcom.com/doc/dragonfly_threat_against_western_energy_suppliers.

23. Robert M. Lee, Michael J. Assante, and Tim Conway, "German Steel Mill Cyber Attack, ICS Defense Use Case (DUC)," December 30, 2014, SANS Industrial Control Systems, https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/bltc79a41dbf7d1441e/607f235775873e466bcc539c/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf.

24. Federal Office for Information Security, *The State of IT Security in Germany 2014* (Bonn, DE: Federal Office for Information Security, November 2014), 31, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2014.pdf?__blob=publicationFile&v=3.

25. Robert M. Lee, Michael J. Assante, and Tim Conway, *Analysis of the Cyber Attack on the Ukrainian Power Grid* (Washington, DC: SANS ICS/E-ISAC, March 2016), https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf.

Ukraine December 2016

While this cyberattack on ICS (resulting in a partial blackout of Kyiv) was more limited in duration and scope than the previous year's attack, subsequent analysis showed it to be more sophisticated and potentially far more damaging. It attacked the relays of the electrical grid used to protect bulk power and other critical equipment that distribute electricity on the grid. The attempt implied one of the attacker's goals was to make the operators' option of restoring power through manual control a dangerous one. When restarting power after a blackout any fluctuations in power would have caused damage to very expensive and hard-to-replace bulk power equipment (such as a transformer) if the relays were not there to perform their function.[26]

Since the second attack was more developed than the first and focused on a similar target, it could be argued this advanced, persistent threat actor was using Ukraine as a cyber weapons laboratory for developing attacks on the industrial control equipment used to monitor and manage the power grid in Ukraine. This observation is significant since Ukraine uses equipment of Western manufacture. NATO member states and other industrialized countries using similar equipment should seriously consider that these cyberattacks developed against Ukraine could also be used in their countries.

NotPetya 2017

This incident, as with the two previously covered cyberattacks in Ukraine, took place in the context of a war between Ukraine and Russia-supported separatists in the Ukrainian province of Crimea. Ransomware placed on accounting software used by companies dealing with the Ukrainian tax inspectorate proceeded to spread rapidly throughout the world, stopping Maersk Shipping worldwide operations and affecting other CI sectors.

One of the ransom malware variants, called NotPetya, seems to have been planted in and later spread from Ukraine.[27] Victims experiencing serious disruptions to their operations were found worldwide, ranging from unlikely places, including a candy factory in Australia,

26. Joe Slowik, *CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack* (Hanover, MD: Dragos Inc., 2019), https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf.

27. Matthew J. Schwartz, "Ukraine Power Supplier Hit by WannaCry Lookalike," Inforisk Today (website), June 30, 2017, http://www.inforisktoday.com/ukraine-power-supplier-hit-by-wannacry-lookalike-a-10071.

Russia's biggest oil producer, Rosneft, and Danish shipping company Maersk.[28] Maersk's CEO claimed the NotPetya infection cost Maersk $300 million in damages.[29] This is the first example of the "collateral damage" that can occur in today's targeted cyberattacks on critical infrastructure.

Later analysis of NotPetya indicated the creators of this malware were not cybercriminals motivated by financial gain. It seems the function for encrypting or erasing data on hard drives worked perfectly while the ransomware function did not work.[30] In other words, the attackers did not seem to care if the ransom payment module worked or not. The creators focused on making sure this computer-killing malware would spread quickly and as widely as possible. The motive for this attack seems far more sinister and fits the interests of a state rather than a cybercrime gang. A state in conflict with Ukraine was using cyberattacks as policy achievement tools. As one security analyst explained, "This was a piece of malware designed to send a political message: If you do business in Ukraine, bad things are going to happen to you."[31] Western companies, like Maersk and FedEx/TNT, with offices in Ukraine received "notice" to watch out.

Triton/Trisis/Hatman 2017

In June and again in August 2017, a cyberattack targeted the safety systems of an important petrochemical plant in the Middle East. This is the fifth publicly known ICS-tailored malware, however, it is the first ever to target safety-instrumented systems (SIS).[32]

The intentional attempt to compromise a safety system represents a serious escalation of the cyber threat to critical infrastructure. Control and safety systems are used in an industrial process to protect property, the environment, and, most importantly, people from serious harm resulting

28. "Global Ransomware Attack Causes Turmoil," BBC (website), June 28, 2017, http://www.bbc.com/news/technology-40416611.

29. Ry Crozier, "Maersk Had to Reinstall All IT Systems after NotPetya Infection," *iTNews* (website), January 25, 2018, https://www.itnews.com.au/news/maersk-had-to-reinstall-all-it-systems-after-notpetya-infection-481815?eid=3&edate=20180125&utm_source=20180125_PM&utm_medium=newsletter&utm_campaign=daily_newsletter.

30. Jeremy Kirk, "Latest Ransomware Wave Never Intended to Make Money," Data Breach Today (website), June 29, 2017, https://www.databreachtoday.com/latest-ransomware-wave-never-intended-to-make-money-a-10069.

31. Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," Wired (website), August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

32. Davide Franzetti, "Oil & Gas Cybersecurity and Process Safety Converge Thanks to TRITON," Security Boulevard (website), February 26, 2019, https://securityboulevard.com/2019/02/oil-gas-cybersecurity-and-process-safety-converge-thanks-to-triton/.

from an industrial process that has gone outside the set parameters used to program an automatic response in the SIS to bring a system back to a safe state when changes in temperature, flow rates, pressure, frequency, or other system state indicators exceed safe levels. These systems automatically respond to open or closed valves on a gas pipeline when pressures or flow rates go beyond preset parameters.[33] If something is done intentionally to neutralize the functions of these systems, serious harm can result if a system state exceeds the set parameters. It is like disabling the breaks and seat belts of an automobile traveling down a highway without the knowledge of the driver. In other words, safety systems are the last lines of defense provided by automated technologies.

Of most concern is that this attack almost succeeded in fully compromising safety-instrumented systems made by Schneider Electric. These systems and similar SIS devices are used in many industrial plants around the world. If the perpetrators have developed a technique against the equipment of Schneider Electric, they can apply the same technique in any of the plants that use this or similar equipment. While the cyberattack only worked on a specific version of the device and software, the potential escalation for disruption of Trisis is unsettling.[34]

One important point to mention is that the victim was unaware of the compromised state of the control systems. Even the manufacturer, after the first shutdown in June, found no fault with the equipment and returned it to the victim, where it resumed its place in the plant's operations. The victim had no cyber forensics capability on-site to investigate the incident but had to pay top dollar to bring in specialists from the outside. In short, the industrial site had little or no cybersecurity capability available to monitor and react to the first cyber intrusions, which took place months earlier.

Norsk Hydro 2019

A particularly disruptive variant of the "LockerGoga" ransomware caused an aluminum manufacturing and power company operating in 40 countries and with 3,500 employees to stop its automated operations and switch to manual operations.[35] Investigations later determined the ransomware

33. Krebs, "Cyber Incident Blamed."

34. 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.

35. Jeff Stone, "Norsk Hydro's Cyber Insurance Has Paid Just a Fraction of Its Breach-related Losses So Far," Cyberscoop (website), October 28, 2019, https://www.cyberscoop.com/cyber-insurance-norsk-hydro-lockergoga-attack/.

entered the company's operations through the supply chain. To the credit of the company's robust cybersecurity policy, good documentation on the operation was available to reestablish automated operations. The company still incurred heavy costs in dealing with the disruptions that amounted to more than 30 million euros in the three months of 2019.[36] The fact that this particular ransomware variant was encountered just once leads one to consider this cyberattack also had an experimental purpose behind it.[37]

US-Russian Intrusions in Each Other's Critical Infrastructure from 2018 to Present

The US government issued alerts on state-sponsored espionage activities directed at acquiring access to power grid control systems.[38] There were also reports of US government-sponsored efforts to do the same in the Russian energy sector.[39] While it is probable the adversaries achieved the objective of accessing the targeted control systems, it is not known if any successful attempts were made to leverage that access in order to compromise systems or cause physical damage.

Interception of Chinese Manufactured Transformer by US Government in 2020

In late spring 2020, the *Wall Street Journal* reported on the US government seizure of a Chinese-manufactured bulk-power transformer bound for a power utility in the southwest United States and diverted to Sandia National Laboratories.[40] Other than speculation, no official report has been issued about this event.[41] This incident occurred, however, about the time of a US presidential "Executive Order on Securing the United States

36. A Hotter, "How the Norsk Hydro Cyberattack Unfolded," Fastmarket AMM (website), 2019, https://www.amm.com/Article/3890250/How-the-Norsk-Hydro-cyberattack-unfolded.html.

37. Joe Slowik, *Spyware Stealer Locker Wiper: Lockergoga Revisited* (Hanover, MD: Dragos Inc., 2020), https://pylos.co/wp-content/uploads/2020/04/Spyware_Stealer_Locker_Wiper-_LockerGoga_Revisited.pdf.

38. "Alert (TA18-074A), Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," CISA (website), March 16, 2018, https://us-cert.cisa.gov/ncas/alerts/TA18-074A.

39. David Sanger and Nicole Perlroth, "U.S. Escalates Online Attacks on Russia's Power Grid," *New York Times* (website), June 15, 2019, https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html?auth=login-google.

40. Rebecca Smith, "U.S. Seizure of Chinese-Built Transformer Raises Specter of Closer Scrutiny," *Wall Street Journal* (website), May 27, 2020, https://www.wsj.com/articles/u-s-seizure-of-chinese-built-transformer-raises-specter-of-closer-scrutiny-11590598710.

41. Cynthia Brumfield, "The Mysterious Case of the Missing 250-Ton Chinese Power Transformer," Vice (website), September 22, 2020, https://www.vice.com/en/article/v7gaqb/the-mysterious-case-of-the-missing-250-ton-chinese-power-transformer.

Bulk-Power System." This order placed heavy prohibitions on the purchase of bulk-power equipment from foreign sources.[42]

Bulk-power equipment is costly to replace, as it requires special design and manufacture before being shipped, transported, and installed at its location. Lloyd's of London, a specialist insurance agency, and Cambridge University, estimated the loss of 50 generators can cascade to an extensive long-term regional blackout which, according to the severity of the scenario, could cost the US economy from $243 billion to more than $1 trillion.[43] It should be noted that the Lloyd's study scenario was relatively mild, for it did not include actual damage to bulk-power equipment. It assumed that after the event the grid would slowly energize with compromised protective relays continuing to protect the bulk-power equipment as they return online.

SolarWinds Orion 2020/2021

SolarWinds software is used by many governments, businesses, and industrial enterprises around the world for network monitoring and management. Reminiscent of the Havex cyberattack six years earlier, this incident was a more widespread, successful, and highly sophisticated supply-chain compromise, affecting 18,000 organizations.[44] Many of these organizations work in industrial operations, including the energy sector. What is concerning in this incident is that major original equipment manufacturers (OEM's) that supply online services to infected customers were also infected, raising the potential number of compromised businesses and industrial operations.[45] What made this incident particularly insidious was that the vendor's legitimate software update to the targeted Orion product was tainted with a malware that provided the attacker with a backdoor.[46]

42. White House, "Executive Order on Securing the United States Bulk-Power System," May 1, 2020, https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-securing-united-states-bulk-power-system/.

43. Lloyd's and University of Cambridge Centre for Risk Studies, *Business Blackout: The Insurance Implications of a Cyber Attack on the US Power Grid*, Emerging Risk Report Innovation Series (London: Lloyd's, 2015), https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-lloyds-business-blackout-scenario.pdf.

44. Sergio Caltagirone, Ben Miller, and Kai Thomsen, "The SolarWinds Compromise and ICS/OT Networks" (webinar, Dragos Inc., December 22, 2020), https://f.hubspotusercontent10.net/hubfs/5943619/Webinar-Assets/Dragos%20webinar%20-%20SolarWinds%20Compromise%20-%20v10_KT%20%20-%20%20Read-Only.pdf.

45. Kim Zetter, "SolarWinds Hack Infected Critical Infrastructure, Including Power Industry," *Intercept* (website), December 24, 2020, https://theintercept.com/2020/12/24/solarwinds-hack-power-infrastructure/.

46. Bruce Schneier, "The US Has Suffered a Massive Cyberbreach. It's Hard to Overstate How Bad It Is," *Guardian* (website), December 23, 2020, https://www.theguardian.com/commentisfree/2020/dec/23/cyber-attack-us-security-protocols.

The customers' efforts to apply industry cybersecurity best practice (keep software patched and up-to-date) ironically only made matters worse. Analysis indicates the initial infection of the vendor's Orion software occurred in spring 2020, months before its year-end discovery.

This incident highlighted the lack of cyber capability in industrial operations. If an industrial operator became suspicious of a cybersecurity breach, there were no means immediately available on-site to determine the extent of the compromise. The operator had to embark on a massive replacement of suspected IT equipment or hire a security firm from the outside to come in and do the diagnostic and clean-up work.

Colonial Pipeline Shutdown 2021

Ransomware was planted in the IT part of the company, which resulted in denial of the necessary data and other information required to process and keep track of fuel orders. While the ICS of the pipeline that monitored and controlled the physical processes inside the pipeline was not affected by this ransomware, the loss of billing and accounting information left the operator no choice but to shut down pipeline operations of over 5,000 miles servicing the East Coast of the United States. This failure was due in part to the company not adhering to industry cybersecurity standards. It lacked a comprehensive corporate cybersecurity program that included standards for industrial automation and control system security (IACS). In particular, the International Society of Automation ISA 95 standard addresses enterprise integration including transfer of information between plant instrumentation and corporate information systems.[47]

Conclusion and Recommendations

In summarizing the unsettling and reoccurring trends in cyberspace, the following characteristics and actions are evident. In the attempts to disable industrial safety systems, little or no industrial cyber forensics are available due to a lack of trained investigators familiar with the operations, and IT-centric cybersecurity approaches fall short of protecting CEI and other infrastructure. Further, the increased connectivity and integration of IT, OT, and ICS, while offering advantages, have also introduced new fragilities and exploitable vulnerabilities that did not exist before they were separate. Cyberattacks for the advanced, persistent threat actor are effective, cheap, and

47. "ISA95, Enterprise-Control System Integration," International Society of Automation (website), https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa95.

deniable. Asset owners and even cybersecurity solution providers are surprised when cyberattacks happen, as the threat actor often achieves compromise of the targeted asset long before discovery by the victim. In fact, in most cases, victims are compliant with industry standards and best practices (such as segmentation, updates, and firewalls). Finally, there has been a failure to establish concrete measures at the international security policy level (such as agreements on norms or conventions) that could manage the problem of malicious cyber activities of states in cyberspace.

There are ways to address vulnerabilities and reduce the danger of compromise by improving cyber defense capacities.

- One of them is to establish an industrial cybersecurity operations center (ISOC). Responsibilities tasked to the ISOC include, first, monitoring and checking on anomalous process flows, equipment performance, and data flows with a goal of detecting a cybersecurity breach within 24 hours.

- Second, responsibilities include identifying and recording all component pieces and versions in a control system.

- Third, the ISOC must review available patches and updates of OT devices found closer to the industrial process, such as PLCs and other intelligent industrial electronic devices (IIED).

- Fourth, according to configuration, change management, and safety procedure, it must test and apply selected patches and updates. The ISOC would be responsible for monitoring control and safety system cybersecurity vulnerabilities (such as current patch levels, malware notifications, and newly discovered vulnerabilities) as announced by cybersecurity institutions and vendors.

- Fifth, the ISOC should take part in regular training and education on ICS cybersecurity, including sending at least one staff member per year to organized ICS security conferences and trainings (such as S4, the largest ICS professionals conference, DEFCON hackers conference, and Black Hat) as well as participate in NATO, EU, and other tabletop and "Live Fire" exercises (such as "Locked Shields)," where cyberattacks on control systems are included in the scenarios.

- Sixth, the ISOC should implement the recommendations in this chapter that are beyond the means of current staff capabilities and resources.

- Seventh, it must oversee the operation of network management systems, intrusion detection, or security information and event management (SIEM) systems and internal operating system health tools that can be used in both an investigative and forensic capacity to identify the source of a problem.

- Finally, it must organize and control use of A/V scanning-based solutions according to established policies and procedures. This solution involves conducting or organizing full offline black-box and white-box penetration testing against the switches, routers, firewalls, controllers, and instruments that the operator uses with help of vendors with certified ethical hackers. It is also recommended to use available tools (such as Metasploit), where one can use benign attack scripts to prove the existence of a device vulnerability in an automated fashion. This way, one can demonstrate a conceptual attack on a test bench without damaging anything. Also vital is the operation of a security test lab used to validate patches before deployment, test security exploits on existing equipment and firmware, and find and diagnose other bugs and test code before downloading it to the field and ensuring that user logons to the system and IED configuration changes are documented, updated, and made available on-site for operator personnel.

The next recommendation addresses the spiraling cyber arms race and associated fragile security environment stemming from the uninhibited malicious activities of states in cyberspace through the creation of international norms.

Since 2010, an increasing number of analysts have expressed concern over a spiraling cyber arms race fueled by states directing malicious cyber activities at the critical infrastructure of other states.[48] The attempts by the international security policy community to manage this dangerous behavior have been characterized by one commentator as "[causing] mostly confusion, indecision,

48. Jason Healey and Robert Jervis, "The Escalation Inversion and Other Oddities of Situational Cyber Stability," *Texas National Security Review* 3, no. 4 (Fall 2020): 30–53, https://tnsr.org/2020/09/the-escalation-inversion-and-other-oddities-of-situational-cyber-stability/.

and paralysis. This lack of management has encouraged their use with impunity, despite their potential for causing mass destruction."[49] Because cyberspace allows for offensive and defensive technology to be nearly indistinguishable, there is a chance it could increase the possibility for a major conflict escalating from a cyber incident.

Current defensive measures for protecting the technologies that support operations of CEI may be inadequate in a dynamically changing cyberspace environment where the attacker seems always ahead in discovering new attack vectors and is especially true for states choosing to make malicious use of cyberspace a means to achieve policy objectives unobtainable through peaceful means such as diplomacy. The international security policy-making community needs to create norms for managing malicious behavior of states in cyberspace as well. These norms will lighten the load of defenders and senior engineers already committed to monitoring OT. This latter group is not an equal match against the advanced skills, patience, and resources available to the state-based threat actor. Norms that seek to promote transparency and cooperation among states based on common interests can reduce international tensions from more frequent and increasingly disruptive cyberattacks on critical infrastructure.

There are three basic cyberspace norms NATO can promote to reduce the risk of igniting a spiraling conflict among states. First, states should restrain from directing malicious cyber activity at another state's critical infrastructure.[50] The restraint should come from a common recognition of the important role technology plays for all states in the critical infrastructures that support modern economic activity, national security, and the well-being of society. Today critical infrastructure has an international dimension because of its cross-border character (for example, power grids and pipelines) and interdependency on cyberspace for its safe and reliable operation. The attacker may find that their own critical infrastructure may feel the effects together with the target. In other words, acting with restraint is in everyone's interest.

The second is for states to take responsibility for keeping their cyberspace jurisdictions in order, including responding to malicious cyber activities emanating from or transiting through their cyberspace

49. Jonathan Terra, "NATO Cannot Cede the New Art of Modern Warfare to Russia and China," Reporting Democracy (website), August 4, 2021, https://balkaninsight.com/2021/08/04/nato-cannot-cede-the-new-art-of-modern-warfare-to-russia-and-china/.

50. Adam Segal, "The Development of Cyber Norms at the United Nations Ends in Deadlock. Now What?" Council on Foreign Relations (website), June 29, 2017, https://www.cfr.org/blog/development-cyber-norms-united-nations-ends-deadlock-now-what.

jurisdictions.[51] States cannot stand idly by when these activities are reported. This is of special concern for the targeted state, which could interpret this behavior as preparation of the battlefield activity leading to dangerous escalation. States must act responsibly in order to preserve the stability in cyberspace that all modern nations depend on.

The third norm is to create an organization to monitor and report on the violation of the above norms. This should not be considered a fruitless effort; there are similar examples, such as the Organization for the Prohibition of Chemical Weapons, which was created as part of a signed international convention.[52] Another example is the International Atomic Energy Agency (IAEA), created to address issues of nuclear weapons proliferation.[53] These norms will not cause these APT attacks to cease, but they should reduce the number of incidents by making the potential perpetrator think twice and weigh the consequences of being discovered before acting.

Several initiatives on norms have been proposed by various international organizations and other entities in the past decade. The Organization for Security and Cooperation in Europe (OSCE) in 2012 Permanent Council Decision No. 1039 on the development of confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies created an internal working group to develop and present norms proposals.[54] One of the proposed norms (number 3) in 2013 is similar to the first norm proposed above.[55]

Even the private sector has joined in taking leadership on international norms. In 2017, Microsoft proposed a digital Geneva Convention

51. Chris C. Demchak and Peter Dombrowski, "Rise of a Cybered Westphalian Age," *Strategic Studies Quarterly* 5, no. 1 (Spring 2011): 32–61, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-05_Issue-1/Demchak-Dombrowski.pdf.

52. Vytautas Butrimas, "National Security and International Policy Challenges in a Post Stuxnet World," *Lithuanian Annual Strategic Review* 12, no. 1 (2013–14): 11–32, https://www.researchgate.net/publication/271726264_National_Security_and_International_Policy_Challenges_in_a_Post_Stuxnet_World.

53. "History," International Atomic Energy Organization (website), n.d., https://www.iaea.org/about/overview/history.

54. Organization for Security and Co-operation in Europe (OSCE) Permanent Council, "Decision No. 1039, Development of Confidence-building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies," April 26, 2012, https://www.osce.org/files/f/documents/e/7/90169.pdf.

55. OSCE Permanent Council, "Decision No. 1106, Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies," December 3, 2013, N.3, https://www.osce.org/files/f/documents/d/1/109168.pdf.

for cyberspace.[56] Out of concern for the protection of citizens from the aftereffects of a state-sponsored attack a series of norms were proposed. They resonate with the norm proposals mentioned above: "The world needs an independent organization that can investigate and share publicly the evidence that attributes nation-state attacks to specific countries."[57] To end this short list of examples, the United Nations Group of Government Experts on Advancing Responsible State Behavior in Cyberspace, in the context of international security (GGE), issued a report in May 2021 that highlights the first two norms mentioned above.[58]

While norms cannot fully solve the problem of state-sponsored cyberattacks on critical infrastructure, they do offer the possibility of managing this destabilizing behavior in peacetime. For this reason, it is recommended that NATO support such initiatives.

56. Brad Smith, "The Need for a Digital Geneva Convention," *Microsoft on the Issues* (blog), February 14, 2017, https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/.

57. Smith, "Digital Geneva Convention."

58. *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, May 2021, 13(c), 13 (f), https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf.

Select Bibliography

Butrimas, Vytautas. "National Security and International Policy Challenges in a Post Stuxnet World." *Lithuanian Annual Strategic Review* 12, no. 1 (2013–14). https://www.researchgate.net/publication/271726264_National_Security_and_International_Policy_Challenges_in_a_Post_Stuxnet_World.

Demchak, Chris C., and Peter Dombrowski. "Rise of a Cybered Westphalian Age." *Strategic Studies Quarterly* 5, no. 1 (Spring 2011). https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-05_Issue-1/Demchak-Dombrowski.pdf.

Federal Office for Information Security. *The State of IT Security in Germany 2014*. Bonn, DE: Federal Office for Information Security, November 2014. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2014.pdf?__blob=publicationFile&v=3.

"ICS Alert (ICS-ALERT-14-176-02A): ICS Focused Malware (Update A)." US Cybersecurity and Infrastructure Security Agency (CISA). June 27, 2014. https://www.cisa.gov/uscert/ics/alerts/ICS-ALERT-14-176-02A.

Lloyd's and Cambridge University Centre for Risk Studies. *Business Blackout: The Insurance Implications of a Cyber Attack on the US Power Grid*, Emerging Risk Report Innovation Series. London: Lloyd's, 2015. https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-lloyds-business-blackout-scenario.pdf.

Slowik, Joe. *CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack*. Hanover, MD: Dragos Inc., 2019 https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf.

Symantec. "Dragonfly: Cyber Espionage Attacks against Energy Suppliers." Mountain View, CA: Symantec Corporation, July 2014. https://docs.broadcom.com/doc/dragonfly_threat_against_western_energy_suppliers.

Terra, Jonathan. "NATO Cannot Cede the New Art of Modern Warfare to Russia and China." Reporting Democracy (website). August 4, 2021. https://balkaninsight.com/2021/08/04/nato-cannot-cede-the-new-art-of-modern-warfare-to-russia-and-china/.

White House. "Executive Order on Securing the United States Bulk-Power System." May 1, 2020. https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-securing-united-states-bulk-power-system/.

— 2 —

The Internet of Things Challenge

Chuck Benson

ABSTRACT: The interconnectedness created by the Internet of Things (IoT) poses great value to critical infrastructure (CI), but has also created deep cybersecurity vulnerabilities to CI systems. Attacks on data management systems or supply chains could impact entire systems in ways that were previously unheard of. Threat actor manipulation of CI IoT could undermine NATO actions across Europe. To account for these weaknesses, organizations must increase IT/OT competencies internally and review vendor security protocols prior to implementation.

Keywords: Internet of Things, network, interdependence, data aggregation, data chain, OT skills, risk mitigation, vendor security, retrofit

The Internet of Things, or IoT, is changing the world in substantial ways, and that rate of change is accelerating. The spectrum of IoT device and IoT system applications only continues to grow to include consumer devices and systems such as Amazon's Alexa, smartphone-controlled colorful light bulbs, and home-security devices and systems such as the Ring camera/doorbell.[1] There are medical devices and supporting IT systems such as infusion pumps and pacemakers that monitor heart rate, blood temperature

1. Nicole Wetsman, "Amazon Announces Alexa Program for Hospitals and Senior Care," *Verge* (website), October 25, 2021, https://www.theverge.com/2021/10/25/22740181/amazon-alexa-hospitals-senior-living; and "Video Doorbells," Ring (website), n.d., accessed October 26, 2021, https://ring.com/doorbell-cameras.

and respiration, and alter the patient's heart rate as needed.[2] Internet of Things systems are found in, and will increasingly be found in, public-safety systems, city-planning and management systems, amateur and professional athletics and sports, research systems, and transportation systems.[3] While all these areas are important for various reasons, one of the most critical is the association with IoT devices and systems in local, national, and international physical critical infrastructure. One of the most important of these is energy infrastructure.

While there are a number of definitions and descriptions of IoT, a useful and succinct pair of definitions are: an IoT device is a networked computing device that interacts with its environment in some way, and an IoT system is comprised of many IoT devices (tens, hundreds, thousands, or more), as well as a supporting infrastructure for connectivity, data aggregation, sometimes command and control, data management, data analytics, and data publishing.[4]

Internet of Things systems in support of critical infrastructure have the potential to bring profound value, increased performance, and sustainability for many types of critical infrastructure. This arrangement, however, also brings new dependencies of that infrastructure on these new IoT systems while adding additional value. Exacerbating this problem is that many, and likely most, IoT systems are poorly implemented, partially implemented, under- or unmanaged, or all of the above in addition to other potential issues. At this point in time, few institutions, corporations, governments, or nation-states are very good at broad and deep implementation and ongoing operation of IoT systems. This lack of ability creates significant issues for cybersecurity and risk mitigation. In the realm of hybrid warfare, it provides a lucrative target with potential for large damage and disruptions for possibly relatively little investment and exposure for an adversary.

2. Inga Shugalo, "Security Crisis of Cardiac Pacemakers Paves the Way for IoT Security Evolution in Cardiology," *Health Care Blog*, July 29, 2019, https://thehealthcareblog.com/blog/2019/07/29/security-crisis-of-cardiac-pacemakers-paves-the-way-for-iot-security-evolution-in-cardiology/; and Gavin O'Brien et al., *Securing Wireless Infusion Pumps in Healthcare Delivery Organizations*, NIST Special Publication 1800-8 (Gaithersburg, MD: National Institute of Standards and Technology/National Cybersecurity Center of Excellence, August 2018), https://doi.org/10.6028/NIST.SP.1800-8.

3. "Perspectives: Internet of Things in Sports," Deloitte (website), n.d., accessed October 26, 2021, https://www2.deloitte.com/us/en/pages/consumer-business/articles/internet-of-things-sports-bringing-iot-to-sports-analytics.html; and Sarah Way, "Public Transport Emerges as the Top Use of IoT in Cities," *Cities Today* (blog), September 9, 2020, https://cities-today.com/public-transport-emerges-as-the-top-use-of-iot-in-cities/.

4. Chuck Benson, *Managing IoT Systems for Institutions and Cities* (New York: Auerbach Publications, 2019), https://www.taylorfrancis.com/books/9780429490996.

Differences between "Traditional" IT versus IoT

Although they share some attributes, IoT differs from traditional IT in several ways. The lack of awareness or understanding of their differences contributes to or facilitates unexpected exposure stemming from the deployment of IoT systems in support of critical infrastructure.

Scale. The number of IoT devices is estimated to be in the low tens of billions and appears to be growing exponentially.[5]

Variety and variation. There are a rapidly growing number of new and differing types of IoT systems, and each IoT device has multiple components, each potentially from a different source provider. Currently, the provenance of any software component can be difficult, if not impossible, to determine.

Lack of language. This term refers to a lack of common, familiar language to discuss, plan for, and manage risk for the deployment and operation of these systems within institutional, corporate, governmental organizations, and partner organizations.

Organizational interdependency. Within an institution, corporation, government, international alliance, or other entity, IoT systems span many departments and supporting organizations—traditional central IT, traditional distributed and local IT, facilities operations, capital development, security office, risk office, multiple vendors, contractors, and subcontractors—many of which need some level of communication and coordination, ranging from occasional to fully immersed. This creates substantial organizational interdependency and a network of potential gaps in coordination and communication.

Out of sight, out of mind. These networked computing devices of IoT systems are usually embedded in the working environment, such as building, campus, production facility, resource delivery facility (for example, pipeline), or other. As such, they can be out of sight, out of mind. Often, planners, operators, and users do not see sensors and actuators (sometimes in the thousands or more) as actual networked computers exposed to the same cyber risks and cyber adversaries as traditional computing devices (such as workstations, laptops, tablets, and phones).

Lack of precedent. Across multiple industries and sectors—not least of which energy and energy resource delivery—institutions, governments,

5. Bojan Jovanovic, "Internet of Things Statistics for 2022 – Taking Things Apart," DataProt (website), May 13, 2022, https://dataprot.net/statistics/iot-statistics/.

and corporations are not good at these implementations from a cyber-risk and cybersecurity perspective. This is particularly true in an increasingly complex networked environment and network of competitors, adversaries, near-adversaries, and others. Repeated, well-configured, risk managed, cyber secure, IoT system delivery and operation is an immature space.

This is not at all to say that so-called traditional IT is not important. It is critical for business operations and data management and analysis. Caring for and supporting traditional IT, however, are different from doing these things for IoT, and it is essential to recognize that having IT planning and support capacity does not mean there is also IoT systems planning and support capacity.

Infrastructure and IoT

Increasingly, where there is infrastructure, there is IoT. Energy infrastructure is no exception. Internet of Things systems are virtually guaranteed to be included with, and a critical part of, any new infrastructure. Similarly, there is strong motivation to retrofit existing infrastructure with IoT systems because—if the systems are well-chosen, well-deployed, and well-operated/managed—the network of IoT sensors can provide valuable frequent environmental and operational information in support of system performance, operational prediction, and safety. For example, there are IoT-enabled roads and traffic-monitoring systems for monitoring and reporting road conditions, weather, traffic, and wildlife movement around roads. There is also monitoring of the structural health of concrete across many industries to include remote continuous monitoring of temperature, humidity, corrosion rate, pH, strains/stress, and cracks.[6] The fatal condominium collapse in June 2021 is an unfortunate recent reminder of the importance of infrastructure health. Similarly, IoT systems are important to monitor, regulate, and improve performance of offshore wind turbines for electricity generation and for "supporting pipeline operations with environmental monitoring, infrastructure management, enhancing operations controllers, and energy management."[7]

6. Kathy Pretz, "Internet of Things Technology Will Connect Highways, Street Lights, and Vehicles," IEEE Spectrum (website), June 20, 2019, https://spectrum.ieee.org/internet-of-things-technology-will-connect-highways-street-lights-and-vehicles; and Alex Jablokow, "How IoT Uses Sensors to Add Intelligence to Concrete Infrastructure," *IoT for All* (blog), November 11, 2020, https://www.iotforall.com/how-iot-adds-intelligence-to-concrete-infrastructure.

7. Jeremy Kivi, "How the Internet of Things Has Influenced Midstream Pipeline Operations," *Schneider Electric Blog*, October 3, 2017, https://blog.se.com/oil-and-gas/2017/10/03/iiot-midstream-pipeline-operations/.

This additional capability, however, depends on complex subsystems, partner systems requiring technical and human management, complex technical and human organizational networks, and concomitant interdependencies between them that create real points of exposure and risk in an increasingly adversarial environment. An important critical subset of that infrastructure is that of energy production, delivery, and consumption.

To the degree that NATO forces depend on energy for operational requirements and force protection, keeping energy resources intact, operational, deliverable, and resilient is critical.[8] Transitively, then, the IoT systems that support these capabilities must also be kept intact, operational, deliverable, and resilient.

This chapter will focus primarily on risk analysis and mitigation steps in the interest of defending and protecting IoT systems in support of energy infrastructure. That said, considerations for defense of this infrastructure can be flipped and used in consideration of offensive operations for energy infrastructure that the adversary is motivated to protect or defend. For example, it is possible NATO forces might desire to interrupt temporarily the energy supply to an adversary. This chapter will primarily focus on protecting the IoT aspect of the energy supply and resources in which NATO is interested.

A Framework for Analysis

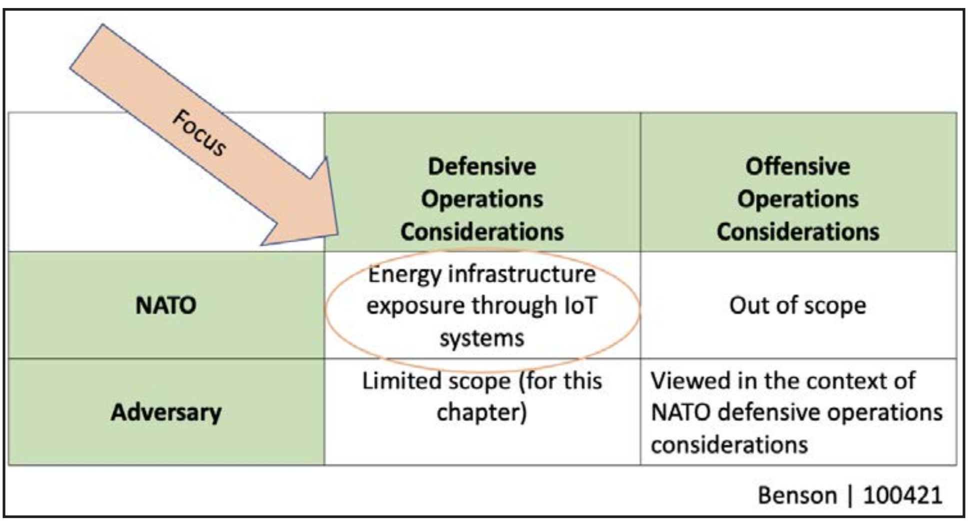

Figure 2-1. Chapter scope

8. NATO, *Allied Joint Doctrine for Force Projection*, Allied Joint Publication 3.14 (Brussels: NATO Standardization Office, November 2007).

To accomplish this, one framework for reflecting upon IoT systems and deployments will be chosen, though this is not the only approach. For this example, the IoT data pipeline will be used. In turn, this will be analyzed within a 2 x 2 matrix with NATO and the adversary on one axis and offensive and defensive operations on the other.

Regardless of physical manifestation, IoT systems will have an array of sensors, actuators, or a combination at one end of the data pipeline. These sensors or actuators can number in the 10s, 100s, 1,000s, or more. An example of a sensor might be a temperature sensor, pressure sensor, or air particulate sensor. An example of an actuator might be a remotely controlled valve in an oil or energy source pipeline. These sensors will feed data into an often-specialized or proprietary data aggregator where a server that speaks the language of the sensors collects data from each sensor and converts them into a more standard data format or protocol for subsequent processing in aggregate. Alternatively, the server may also be a command-and-control server that sends command-and-control data/signals to an actuator to change, for example, the rate of flow of a liquid in a pipeline.

The path from the sensors to the aggregator could be over a tightly controlled and managed network, public network, or something in between. The path could be fairly simple, such as through one or two router hops on the way to the aggregator, or through very complex multiple hops and complex network switching.

From the data aggregator, data will be processed in more traditional, though still nontrivial, ways. These data will still require extensive data management. An inexhaustive list of data management tasks and processes includes extensible data storage, data cleaning and curating, data backup and recovery, data encryption, and data compression.

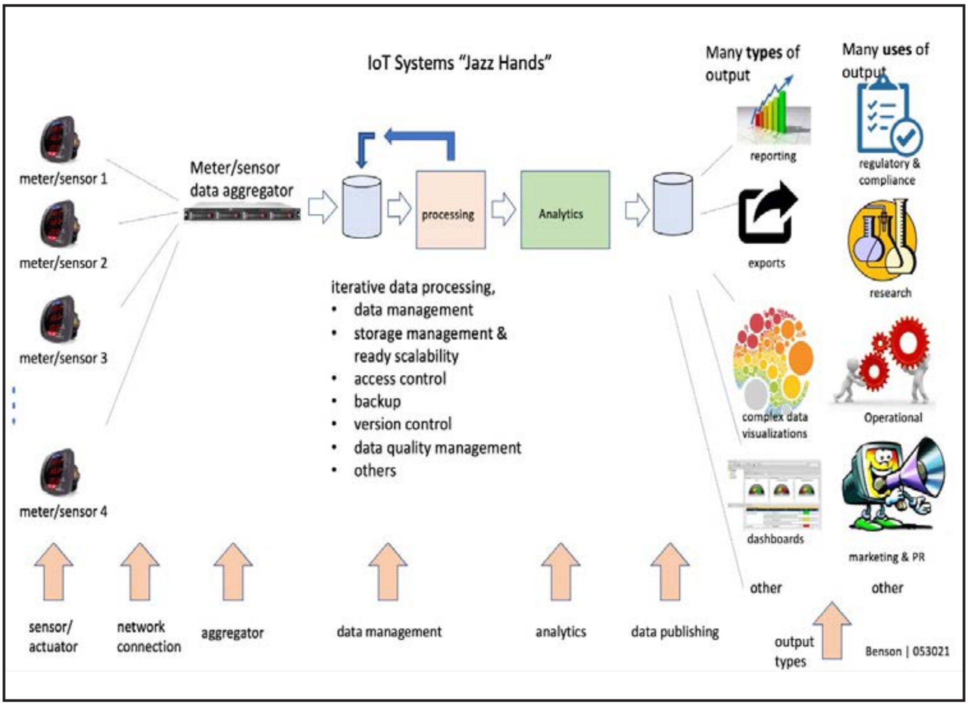

Figure 2-2. Multiple links in the IoT data pipeline (also known as "jazz hands")
Source: Chuck Benson

Subsequently, that data will go through one or many analytical processes either through specially configured off-the-shelf analytical tools (such as SPSS, Matlab, and others) or proprietary tools. Further, data-visualization tools and programming languages, such as Tableau and R, can be considered part of the analysis process (as well as the publication process).[9] Ever-evolving artificial intelligence approaches can also be applied to the analysis. Proprietary visualization tools are also possibilities.

Finally, the processed and analyzed data are made available for human use in the form of reports, spreadsheets, exports, dashboards, visualizations, and combinations of these. Further, this information could be for operational use, monitoring, troubleshooting, regulatory/compliance, public information, or even marketing.

Breaking any point in this chain can render the entire data pipeline ineffective at least temporarily and possibly permanently. This means

9. "IBM SPSS Software," IBM (website), n.d., accessed October 26, 2021, https://www.ibm.com/analytics/spss-statistics-software; "MATLAB," MathWorks (website), n.d., accessed October 26, 2021, https://www.mathworks.com/products/matlab.html; and "Business Intelligence and Analytics Software," Tableau (website), n.d., accessed January 23, 2019, https://www.tableau.com/.

the physical infrastructure of energy flow and transport can be impacted with sufficient disruption to be a useful strategic, operational, and/or tactical target by an adversary. It is also important to remember, as the Colonial Pipeline example has shown, that it can be enough to attack business information systems only to motivate an operator to shut down the physical portion of the infrastructure because of lost revenue (for example, due to the inability to measure or invoice in a timely fashion).[10]

Examples of IoT in energy infrastructure include the following:

- A pipeline might have acoustic sensors for crack-initiation detection, magnetic sensors for corrosion detection, and remote operation of valves and other actuators.[11]
- A fuel depot will have storage tanks with inventory (level) sensors, stored oil/fuel composition detectors, flow-rate monitoring, seismic detection, and more.
- Fuel transport vehicles, land or maritime, will likely have IoT-based fleet asset-management systems, vehicle safety systems, cargo (oil/fuel) operational and safety systems, and other systems.[12]
- A wind turbine farm will have sensors and actuators to enhance reliability, add additional control capabilities, and increase security.[13]
- Other examples include battery farms, pumping stations, remotely controlled circuit breakers, photovoltaic array management (solar cells), hydrogen fuel farms, and others.[14]

10. Stephanie Kelly and Jessica Resnick-ault, "One Password Allowed Hackers to Disrupt Colonial Pipeline, CEO Tells Senators," Reuters (website), June 8, 2021, https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/.

11. "4 Ways IoT Reimagines Pipeline Monitoring in Oil & Gas," *BehrTech* (blog), July 3, 2019, https://behrtech.com/blog/4-ways-iot-reimagines-pipeline-monitoring-in-oil-gas/.

12. "Internet of Things in Oil & Gas," Deloitte (website), n.d., accessed December 15, 2021, https://www2.deloitte.com/us/en/pages/consulting/articles/iot-digital-oil-and-gas.html.

13. Lina Alhmoud and Hussein Al-Zoubi, "IoT Applications in Wind Energy Conversion Systems," *Open Engineering* 9, no. 1 (January 2019): 490–99, https://doi.org/10.1515/eng-2019-0061.

14. "After Many False Starts, Hydrogen Power Might Now Bear Fruit," *Economist* (website), July 4, 2020, https://econ.st/3DW1XEB.

Supply-chain Considerations

Supply-chain exposure and challenges are prevalent across the entire IoT data pipeline. At the device level, on the far left of the data pipeline diagram, the devices—sensors and actuators—have many software components from many different providers.[15] There may be a real-time operating system (RTOS) in the device, which could be sourced from several different providers. There can be diverse sources for web services software, encryption software, business logic software, TCP/IP networking software, wireless protocol software, and others.[16] These sources can have other sources, suppliers, or subcontractors. Many vulnerabilities, some existing, deployed, and "in the wild" for several years, have been found in software libraries supporting the networking "TCP/IP stack." Every packet of network communication goes through this portion of the software on the device, so if it is compromised, a malicious actor could exploit this vulnerability and eavesdrop on the communication, disrupt device operation, or control the device operation.[17] Similarly, networking hardware and software can be sourced from a variety of places, to include potentially adversarial countries such as China (Huawei).[18] The device data aggregator and/or command-and-control hardware and software (server, cloud-based service/application) will also likely have complex software assembled with software from many suppliers.

Applications in the IoT data pipeline used for data management, processing, and analysis, as well as software applications used in publishing data (such as reports, dashboards, and download portals) can also have software components from multiple different providers—who can also source from many different providers, and so on.

15. *Hearing on China, the United States, and Next Generation Connectivity before the US-China Economic and Security Review Commission,* 115th Cong. (2018), 132.

16. Craig Hunt, "Chapter 1. Overview of TCP/IP," in *TCP/IP Network Administration*," 3rd ed., O'Reilly (website), n.d., accessed May 7, 2021, https://www.oreilly.com/library/view/tcpip-network-administration/0596002971/ch01.html.

17. "Project Memoria," Forescout (website), n.d., accessed December 15, 2021, https://www.forescout.com/research-labs/project-memoria/.

18. Kevin Baron, "NATO Has 'Growing Realization' about Risks of Using Huawei Gear, Top General Says," Defense One (website), February 25, 2020, https://www.defenseone.com/threats/2020/02/nato-has-growing-realization-about-risks-using-huawei-gear-top-general-says/163318/.

IoT Considerations in Risk Analysis and Defensive Operations for Energy Security

Because breaking the IoT data pipeline, which directly supports energy infrastructure anywhere, can cause disruption of energy flow and delivery, each point in the chain should be studied as well as the corresponding interfaces between each point. Time and resources, particularly staffing resources, will provide a limit to the level of detail and granularity of analysis for any fixed time period, but that does not prevent a structured, consistent, and repeatable approach.

For each point in the chain, the data pipeline, it is important to ask what the likelihood and impact of a successful attack would be. For example, the respective likelihoods and impacts of sensor or actuator damage, degradation, destruction (in part or in whole), network problems between sensors and aggregator/command-and-control servers, hardware and software supplied by potential adversaries with backdoors, and other control and disruption mechanisms and network equipment and software of unknown or questionable provenance should be considered. Furthermore, flawed or compromised data management software and/or analysis software and the likelihood of an insider threat anywhere, or in multiple places, in the IoT data pipeline should be examined.

Other considerations and potential for analyses include IoT life-cycle stages and supply-chain issues at the device level all the way up the data pipeline. Further, these different frameworks can be integrated and cross-matrixed. That integration with three different frameworks with multiple components, however, begins to become unwieldy in application, particularly for constrained resources.

Using IoT Systems to Disrupt Neighbor IoT Systems

Notably, it is possible an IoT system can be hacked to get into another IoT system on the network. For example, in the 2008 Baku-Tbilisi-Ceyhan Turkish pipeline explosion, the attackers hacked the networked video-surveillance system and then used that as a stepping off point for a subsequent attack on the industrial controls of the pipeline itself.[19]

19. Ariel Bogle, "A Cyber Attack May Have Caused a Turkish Oil Pipeline to Catch Fire in 2008," *Slate Future Tense* (blog), December 14, 2014, http://www.slate.com/blogs/future_tense/2014/12/11/bloomberg_reports_a_cyber_attack_may_have_made_a_turkish_oil_pipeline_catch.html.

Figure 2-3. 2008 Turkish pipeline hack and explosion
Source: Reuters (used with permission)

The idea and approach of this type of vulnerability and attack is that different networks within an organization, enterprise, and nation-state have many different subnetworks that are connected and often interdependent. The issue is that, often, these different subnetworks can have distinct levels of security, risk, and operational oversight. This heterogeneity of risk and exposure level can occur because of the different external providers/vendors of network services and devices used to implement and operate different network services and equipment. Similarly, several aspects of the overall network may be treated and supported quite differently because of substantial organizational and cultural differences within separate divisions of the same organizational entity, nation-state, or alliance, the central IT division, and the operational technology/facilities operations divisions.[20]

Exacerbating the varying security/risk posture challenge is that the operator of the comprehensive network comprised of the smaller networks, not uncommonly, implicitly assumes the whole network has the same level of risk exposure and allows "trust" between interconnected subnetworks that have distinct levels of risk and security. This assumption creates vulnerability. An attacker can attack and garner access to a more exposed, less secure, subnetwork. Then, because implicit trust may exist between subnetworks,

20. "IoT and Cybersecurity Risk: Core Issues for the Building Industry," Cyber-BE Lab (website), February 24, 2021, https://cyber.be.uw.edu/2021/02/24/part-i-iot-and-cybersecurity-risk/; and "IoT Policy Landscape: Implications for Managing Security in the Built Environment," Cyber-BE Lab (website), February 24, 2021, https://cyber.be.uw.edu/2021/02/24/part-ii-iot-policy-landscape/.

the attacker can use that foothold in the more exposed subnetwork to traverse into other, often more sensitive, and critical, subnetworks.

While this weak-link-network approach has since been disputed in the 2008 pipeline case, it is a known attack vector. Another example is the Target cyberattack in 2013 where the attacker gained access because of Target's relationship and network connection with a heating, ventilation, and cooling (HVAC) vendor.[21] HVAC systems, some of the earliest IoT systems, remain a prolific sector. Another example is alleged access to Boston-area hospitals through an HVAC vendor.[22]

Operational Technology Skill Set Shortages

A short supply of staffing and skill sets in operational technology (OT) is needed to implement, operate, and manage IoT systems. There is also a short supply of skill sets that can work well across organizational, historical, and work-culture boundaries. "Resolving an issue often takes both data analysis and a wrench . . . ."[23]

This shortage of needed skill sets also contributes to improper and/or incomplete and risk-laden IoT systems deployments and operation. While this OT skill set capacity shortage will likely shrink in the future, it will take time. In the meantime, there is a good probability that marginally installed, operated, and exposed IoT systems, not the least of which are energy infrastructure systems, will continue in the near term.

Mitigating Risk

With the rapid growth in the number, size, and complexity of IoT systems and their respective interdependencies, there is growth in the number of motivated, nation-state, and criminal malicious actors. Due to their deepening and broadening capabilities, the shortage of IoT system deployment and operational capacity for organizations, corporations, institutions, and

21. Robert M. Lee, "Closing the Case on the Reported 2008 Russian Cyber Attack on the BTC Pipeline," *SANS Institute* (blog), June 15, 2015, https://www.sans.org/blog/closing-the-case-on-the-reported-2008-russian-cyber-attack-on-the-btc-pipeline/; and Brian Krebs, "Inside Target Corp., Days after 2013 Breach," *Krebs on Security* (blog), September 21, 2015, https://krebsonsecurity.com/2015/09/inside-target-corp-days-after-2013-breach/.

22. Steve Alder, "HVAC Vendor Allegedly Hacked: Access Gained to Hospital Systems," *HIPAA Journal* (website), August 23, 2021, https://www.hipaajournal.com/hvac-vendor-allegedly-hacked-access-gained-to-hospital-systems/.

23. Benson, *Managing IoT Systems*.

alliances mitigating risk in this environment is challenging. There are, however, things that can be done. A short list of potential mitigation steps includes:

- Do not assume similar levels of risk exposure and security across a large, multicomponent network.
- Ascertain, as much as possible, the source of the provided software in devices and other aspects of the IoT data pipeline.
- Demand, review, and ask for evidence of vendor/provider security and risk mitigation and practices.
- Begin immediately to build communication channels and shared language and interests across divisions/departments in an organization, particularly traditional IT and OT divisions, departments, and units.
- Begin internal development of IT and IT/operational technology competencies. Outsourcing is also possible, but these skill sets are in short supply and high demand.
- Begin to develop budgets around these needs and capabilities. These needs are not going away and will continue to grow.

The University of Washington has implemented and continues to develop a "Four Pillar" program to provide a framework for addressing these IoT systems issues as an organization/institution:

- Policy review, modification, and development
- Outreach, education, awareness, and assistance across the enterprise
- Self-awareness and threat awareness
- Interorganizational coordination

While each of these components, relationships, and the dependencies between them requires substantial work, this framework does provide a mechanism with which to orient to a very complex problem set.[24]

24. Benson, *Managing IoT Systems*.

Conclusion

Internet of Things systems directly enable and facilitate energy infrastructure strategy and operations. A core and critical component of these systems is the IoT data pipeline. There is a high likelihood that damaging, destroying, or disrupting this IoT system data pipeline will have immediate and potentially catastrophic effects on the physical infrastructure for making energy available to NATO forces and partners. Because of its importance and its natural logical flow, this data pipeline provides a traceable path to serve as a basis for risk analysis, intelligence, and the operational and strategic needs for NATO forces in Europe.

Select Bibliography

Alhmoud, Lina, and Hussein Al-Zoubi. "IoT Applications in Wind Energy Conversion Systems." *Open Engineering* 9, no. 1 (January 2019). https://doi.org/10.1515/eng-2019-0061.

Benson, Chuck. *Managing IoT Systems for Institutions and Cities*. New York: Auerbach Publications, 2019. https://www.taylorfrancis.com/books/9780429490996.

Hearing on China, the United States, and Next Generation Connectivity before the US-China Economic and Security Review Commission. 115th Cong. (2018).

"HVAC Vendor Allegedly Hacked: Access Gained to Hospital Systems." *HIPAA Journal* (blog). August 23, 2021. https://www.hipaajournal.com/hvac-vendor-allegedly-hacked-access-gained-to-hospital-systems/.

"Internet of Things in Oil & Gas." Deloitte (website). n.d. accessed December 15, 2021. https://www2.deloitte.com/us/en/pages/consulting/articles/iot-digital-oil-and-gas.html.

"IoT Policy Landscape: Implications for Managing Security in the Built Environment." Cyber-BE Lab (website). February 24, 2021. https://cyber.be.uw.edu/2021/02/24/part-ii-iot-policy-landscape/.

Jablokow, Alex. "How IoT Uses Sensors to Add Intelligence to Concrete Infrastructure." *IoT for All* (blog). November 11, 2020. https://www.iotforall.com/how-iot-adds-intelligence-to-concrete-infrastructure.

Lee, Robert M. "Closing the Case on the Reported 2008 Russian Cyber Attack on the BTC Pipeline." *SANS Institute* (blog). June 15, 2015. https://www.sans.org/blog/closing-the-case-on-the-reported-2008-russian-cyber-attack-on-the-btc-pipeline/.

Pretz, Kathy. "Internet of Things Technology Will Connect Highways, Street Lights, and Vehicles." IEEE Spectrum (website). June 20, 2019. https://spectrum.ieee.org/internet-of-things-technology-will-connect-highways-street-lights-and-vehicles.

— 3 —

Malign Influence and Disinformation

Georgios Giannoulis and Erin Hodges

ABSTRACT: This chapter outlines hybrid activity and the tools available to actors to conduct hybrid warfare, vulnerabilities brought about by cyber-integration and the concept of information warfare as a "gray zone" in conflict. Current efforts by the Russian Federation and its proxies to destabilize the information landscape surrounding its invasion of Ukraine are detailed, and recommendations are made to counter disinformation, including media regulation reform, the establishment of disinformation task forces, cultivating populations that are resilient to information warfare, and diversifying supply chains and the information landscape.

Keywords: hybrid threats, information diffusion, disinformation, energy security, Russia-Ukraine War, supply chains

Introduction

The energy sector is one of the main pillars of a state's operation and sustainability. Protecting and ensuring the smooth operation of critical energy infrastructure is a primary goal of democratic societies. Increasingly, advanced systems for parametric surveillance and control of facilities are being introduced into the operation of critical infrastructure and the broader energy sector. This integration offers better oversight and remote accessibility but introduces potential vulnerabilities to malicious activities such as hybrid threats.

Defining Hybrid Activity

According to *The Landscape of Hybrid Threats: A Conceptual Model*, "Hybrid threat can be characterized as coordinated and synchronized action that deliberately targets democratic states' and institutions' systemic vulnerabilities through a wide range of means. Activities exploit the thresholds of detection and attribution as well as the border between war and peace."[1]

Hybrid actors seek strategic objectives by challenging the security environment of democratic states and institutions. Their objectives are to undermine decision-making processes, raise unhealthy polarization in the society, and challenge democratic values by introducing new attack vectors in an unprecedented manner.

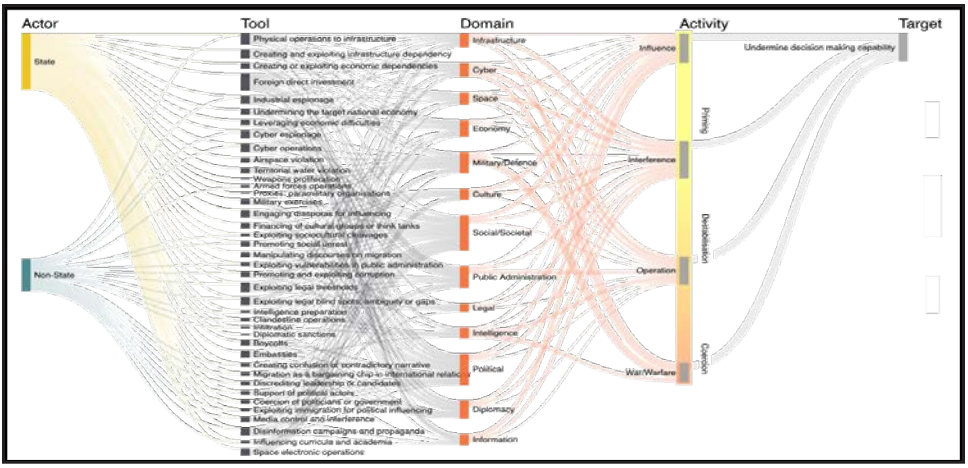

Figure 3-1. Diagram of the conceptual model
Source: *The Landscape of Hybrid Threats: A Conceptual Model* (used with permission)

From the above diagram, it becomes evident that a hybrid actor, who may be a state or non-state actor, has a variety of weapons (tools) applicable to different domains that can be used to address the systemic vulnerabilities of a democratic state. Hybrid actions can be employed in many ways, from low intensity (such as influence) to the escalated version of hybrid warfare. In a hybrid actor's operational plan, objectives are not clearly defined in terms of time, hence, there are no deadlines or due dates for actions. Unlike traditional operational plans, the attacker is relieved of the stress and

1. Georgios Giannopoulos, Hanna Smith, and Marianthi Theocharidou, *The Landscape of Hybrid Threats: A Conceptual Model* (Luxembourg: European Centre of Excellence for Countering Hybrid Threats, February 5, 2021), 13, https://www.hybridcoe.fi/wp-content/uploads/2021/02/conceptual_framework-reference-version-shortened-good_cover_-_publication_office.pdf.

cost of gathering and consuming resources at a specific time and place, as the targeted center of gravity, "the source of power that provides moral or physical strength, freedom of action, or will to act," can be shifted in time.[2]

This modular and agile attack scheme available to hybrid actors gives them the flexibility to move forward or backward, escalate or de-escalate, and synchronize in parallel or in a series of independent actions at their will and according to the circumstances. In that way, hybrid actors ensure the viability and continuity of their plans, have the chance to test possible reactions or response plans, and confuse the situational awareness of the target state. At the same time, they are able to stay undetected and unattributed at the gray zone between legal and illegal, acceptable and unacceptable, and peace and war.

The Cyber Domain and Information Diffusion

One of the most critical domains in hybrid conflicts is the cyber domain because it constitutes the main channel of information diffusion (information circulated in isolated, mostly interdependent networks around the globe). The Internet, Internet of Things (IoT) systems, telecommunication networks, and many other systems and networks can carry large amounts of data from encrypted and critical information to less significant, publicly accessed networks. Cyberspace offers fertile ground for state actors, non-state actors, or proxies of states to act effectively, rapidly, and anonymously under the threshold of detection. Hybrid actors are trying to gain access to any available information that can be processed individually or studied in correlation with similar samples taken in different time periods as a way of revealing and learning multilevel behavioral patterns of the target state and gaining intelligence while reducing the chance of detection.

2. Joint Chiefs of Staff (JCS), *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02 (Washington, DC: JCS, August 2021).

Cascading Effect of Hybridity

In multidimensional spaces of action, hybrid actors set up their operational plans driven by systemic vulnerabilities and exposures of the targets. This vulnerable domain may not be the prime target of the hostile actor, but domain interdependence can allow for further action toward the desired domain. Such an activity may trigger cascading effects, offering opportunities for hybrid actors to exploit more domains by engaging diverse tools in synchronized and coordinated actions that can be used as force multipliers in the field.

Influence and Disinformation

According to figure 3-1, influence is a low-intensity activity in which a hybrid actor has the chance to act in a gray zone and remain under the threshold of detection and attribution. Influence is usually a prolonged and effective process as it gains access through political, societal, and ideological gaps in liberal democratic societies. Activities in the cyber domain are effective in infrastructure like the energy sector, while information congestion and disinformation are part of the toolkit hybrid actors use to build influence.

According to the definition established by the European Union:

> "Disinformation is verifiably false or misleading information created, presented and disseminated for economic gain or to intentionally deceive the public and can have a range of consequences, such as threatening our democracies, polarizing debates, and putting the health, security and environment at risk."[3]

In the energy era, we have experienced how coordinated disinformation campaigns target energy diversification and security development projects—mostly across Eastern European countries. Especially for the development of nuclear power plants, the manipulation of public opinion to oppose against such an investment is evident. In Poland, for example, disinformation related to a possible radiation exposure like the Chernobyl

3. "Tackling Online Disinformation," European Commission (website), n.d., https://digital-strategy.ec.europa.eu/en/policies/online-disinformation.

nuclear accident has impacted conversations about energy diversification.[4] In addition, instrumentalizing ideological active organizations who fight for environmental protection against hazardous materials and the proliferation of nuclear power installations could be considered coordinated information activity toward the same goal.[5]

Principle aspects of democratic societies (such as freedom of speech, freedom of expression, and freedom of media) can be weaponized by malicious actors to manipulate or polarize the society. These core values of democracy can be converted into systemic vulnerabilities and constitute potential targets in the hybrid context. While democracies follow transparent and fair procedures in every means of information dissemination, they also leave room for internal and external hostile interference. On the other hand, news media are obliged to provide reliable information and support the democratic processes by adhering to journalistic principals and ethical codes.

Due to global digitalization and the proliferation of computers and smart devices, the media news sector has been transformed. Social media platforms today have taken over the majority of the information load, leaving less room for traditional journalistic news. The modern method of dissemination of information is performed without sufficient transparency, usually anonymously, with no adequate fact-checking or relevant accountability, providing fertile ground for disinformation.[6]

Through the broader market strategy of social media that use segmentation of people in groups according to their interests, disinformation campaigns have become more sophisticated and effective by tailoring informative content to each group. In that way, the detection of malicious information becomes more difficult.[7]

4. Karolina Baca-Pogorzelska, "How Chernobyl Fake News Poisons Nuclear Energy Debate in Poland," Notes from Poland (website), April 25, 2020, https://notesfrompoland.com/2020/04/25/how-chernobyl-fake-news-poisons-nuclear-energy-debate-in-poland/.

5. Aleksander Król, "Warsaw Institute Review: Information Warfare against Strategic Investments in the Baltic States and Poland," Warsaw Institute (website), July 19, 2017, https://warsawinstitute.org/information-warfare-strategic-investments-baltic-states-poland/.

6. European Centre of Excellence (CoE) for Countering Hybrid Threats, *Countering Disinformation: News Media and Legal Resilience*, Hybrid CoE Paper 1 (Luxembourg: European CoE for Countering Hybrid Threats, November 2019), https://www.hybridcoe.fi/wp-content/uploads/2020/07/News-Media-and-Legal-Resilience_2019_HCPaper-ISSN.pdf.

7. Carme Colomina, Héctor Sánchez Margalef, and Richard Young, *The Impact of Disinformation on Democratic Processes and Human Rights in the World* (Strasbourg, FR: European Parliament, April 2021), https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653635/EXPO_STU(2021)653635_EN.pdf.

The amount of information circulated through the Internet is enormous. Every minute, Facebook users share 150,000 messages, WhatsApp users share 40,000,000 messages, and Instagram users post 350,000 stories and upload 500 hours of video.[8] In addition to traditional paper and broadcasting media, phone calls and messages can illuminate how congested the information environment is and how challenging it is to track disinformation.

Counter Disinformation

It is important to highlight the behavioral attitude cultivated through social media. Unfortunately, users have become passive receivers of messages rather than critical thinkers of what they read and listen to due to insufficient time to process the flow of information. This shortcoming constitutes a serious vulnerability where disinformation can become more digestible. The conditions for the flourishing of disinformation are enhanced when social unrest, caused by an economic crisis or pandemic, prevails at the same time in society. Through such a situation, humans seek to reinforce the feeling that something is wrong and someone is responsible, either for causing or not preventing the problem. In this way, the trust in states and institutions is shaken, and a gap is created that can be exploited by hybrid actors to undermine decision-making capabilities.

Several attempts have been made and several measures have been taken at the national and multinational level, such as the European Union (EU), but there is no consensus on counter-disinformation best practices. In addition, though several legal tools exist, they cannot be applied to the same extent by all member states, due to cases of insufficient resources to support the measures or the absence of law enforcement authorities to implement such laws. Nevertheless, disinformation can still be an international problem, extending beyond national borders, that can only be countered by a collective approach (such as EU-level action) or an even broader approach.

Russian Malign Influence during the 2022 Ukrainian Invasion

The Russian invasion of Ukraine has highlighted the breadth of impact possible when malign influence and disinformation combine with military action. Russia has capitalized on its vast economic and informational

8. Domo Inc., "Data Never Sleeps 8.0," 2020, https://web-assets.domo.com/blog/wp-content/uploads/2020/08/20-data-never-sleeps-8-final-01-Resize.jpg.

networks to further its invasion while attempting to divide Western powers. While the invasion has had a unifying effect on most of NATO and the EU, it has also identified areas of fundamental weakness. The allied response, which has focused mainly on cutting economic and energy ties with the Russian Federation, has deprived Moscow of important economic and political capital, warranting a higher risk of Russian hybrid attacks in the NATO bloc.

Disinformation

The role of Russian disinformation in conjunction with the war has played out differently than it has in the past and can be linked to the fact that Russian state television networks are banned across the European Union, and social media platforms like Facebook and Twitter have reduced the reach of Russian propaganda dramatically. Instead, the Kremlin's disinformation has been focused toward Russian nationals and the Russian-speaking diaspora in neighboring countries and farther abroad.

The use of the term *special operation* in the early days of the war was innately deceptive, and the press releases from Russian embassies and the Ministry of Foreign Affairs have been sharing blatant falsehoods. The main objective of this disinformation campaign was to lead Russians to believe their military was conducting defensive operations, as opposed to an offensive invasion of its neighbor. Some of these lies include claims that the United States is operating a biochemical laboratory in Ukraine and that Ukraine was attempting to build a nuclear bomb at the Chernobyl nuclear power plant. Both claims have been dismissed by Western governments and independent fact-checkers.[9] More recently, Russian propaganda has focused on efforts to misrepresent Ukrainian refugees as "victims of [the Kyiv regime's] Nazism" to misconstrue Russian looting in Ukraine as internationally sanctioned trade and mislabel NATO as an aggressor toward Russia and Ukraine.[10]

Cohesive efforts by governments and corporations in the United States and Europe have highlighted a key strategy in future information wars. By controlling the reach of Russian propagandists and openly discussing the falsehoods in a unified fashion, these efforts have made it much more difficult for the Russian regime to narrate international events falsely.

9. Mark Scott, "As War in Ukraine Evolves, So Do Disinformation Tactics," *Politico* (website), March 10, 2022, https://www.politico.eu/article/ukraine-russia-disinformation-propaganda/.

10. "Time Stopped for Russia in 1945: A Digest of Russia Propaganda for May 31," Ukrinform (website), June 1, 2022, https://www.ukrinform.net/rubric-ato/3504015-time-stopped-for-russia-in-1945-a-digest-of-russian-propaganda-for-may-31.html.

Furthermore, this information warfare has not done what the Russians usually do best—capitalizing on preexisting divisions within nations and organizations. This failure has proven to be a Western advantage. This victory should not be considered a conclusive success over all Russian disinformation though. For example, because of difficulties in algorithmic recognition of languages beyond English, TikTok and YouTube have had Russian-language users and accounts parrot otherwise banned Kremlin propaganda. Telegram has also provided a substantial platform for the spread of misattributed war videos, often reaching multiple countries and tens of thousands of readers nearly simultaneously.[11]

Russia's disinformation at home has been robust. First, the Kremlin has severely limited unsanctioned reporting. Independent reporters have been chased out of positions, and protesters have been arrested. In early March, draft legislation proposed that anti-war protesters could be conscripted into military service.[12] Moreover, Russia's considerable disinformation networks have turned almost 90 percent of their efforts inward.[13] There is no viable way to measure the efficacy of these efforts accurately while so little information is coming into and out of Russia, but when the war ends, the West must find ways to infiltrate the Russian-language information spaces successfully to provide the necessary context to Russian nationals. Without this effort, there is a significant risk of a generation of Russians unaware of the truth and hostile toward Western states because of hardships their government caused. Moreover, a population of misled citizens could provide Russia with more vectors for disinformation in the same way it incentivizes hackers—without necessarily employing them.

The success of the Western world, in light of the changing disinformation landscape, demands a collaborative effort to continue to discover, describe, and destroy disinformation before it can be widely disseminated. It is also vital to remember that influence does not only occur in information spaces. The invasion of Ukraine has highlighted that hostile actors can leverage economic and infrastructural investment to further their needs. Diverse supply chains will diminish this effect.

11. Scott, "Disinformation Tactics."

12. Reuters in Moscow and Gareth Jones, "Fearing Martial Law or Conscription, Some Russians Try to Flee Abroad," Reuters (website), March 3, 2022, https://www.reuters.com/world/europe/fearing-martial-law-or-conscription-some-russians-try-flee-abroad-2022-03-03/.

13. Scott, "Disinformation Tactics."

Recommendations

Some of the following measures could safeguard the credibility of the information against malicious influential activities.

Shaping the Legal and Regulatory Framework of Media Platforms

Although many countries have established rules and norms to govern information flow through journalistic media, especially during campaigns and elections, they still need to fill the associated gap with global social media companies. Institutions like the EU need to define the legal status, relevant regulation, and accountability of social media platforms to bolster transparency and fair competition with the corresponding journalistic media. At the same time, democratic principles (such as freedom of expression, freedom of speech, and equity) should be safeguarded.[14]

Creation of a Disinformation Rapid Response Force

A task force should be established within NATO's Joint Intelligence and Security Division to establish a network for detecting and countering disinformation in the nascent stages. This task force should be staffed by local, credible actors with a strong presence at the community level. Their focus would be on building a network to ensure every state is able to evaluate disinformation from multinational and multicultural perspectives to determine the identity and motives of perpetrators more accurately through data analysis. This information would then be classified according to its impact, including a threat-level timeline, and its possibility of spreading to local, state, national, or international levels.

Diversification of Supply Chains

Because malign influence is not exclusively disinformation, NATO's logistics committee should identify necessary goods produced outside the Alliance. Wherever possible, it should work to stockpile or diversify supply chains to create minimal disturbances, should non-Allied nations use their economic influence to interrupt supply. This action would give NATO nations a full scope of responses to aggression.

14. European CoE for Countering Hybrid Threats, *Countering Disinformation*.

Education on Disinformation Efforts

Many resources, including funding efforts to enhance news literacy, should be a high priority for governments. The development of critical thinking and the cultivation of the ability to draw real facts through an information storm cannot be obtained easily, especially today when the majority of information is provided through social media. This ability must be acquired from the early stages of education so it can be assimilated more easily in the future. Hence, due to the digitalization of learning methods, it would be advisable to teach children the methodology and value of analyzing and exploiting the content of information through the Web.

Since 2019, the Council of Europe, through its European Media Literacy Week, has advocated for the promotion of media literacy, and it has had an expert research group since 2011. These efforts should be leveraged to help member states create and implement national media-literacy programs for children and adults. The most convenient and easiest way to protect from disinformation is to follow a diversity of people or groups and perspectives on websites and in traditional media. Relying upon limited, biased news and resources increases the odds of falling victim to false rumors.[15]

In conclusion, many practices for countering malign information exist. It is questionable, however, whether and to what extent they can be applied. Surveillance and censorship (of journalists, in particular) oppose the fundamental principles of democracy (such as freedom of speech, expression, and the press). Additionally, constraints may lead to a conflict with private-interest and free-market competition, where social media companies design and constantly improve their algorithms to dominate the global market. Instead, NATO nations must candidly analyze areas of influence dominated by hostile actors and build contingency plans to address areas of weakness.

15 Darrell M. West, "How to Combat Fake News and Disinformation," Brookings (website), December 18, 2017, https://www.brookings.edu/research/how-to-combat-fake-news-and-disinformation/.

Select Bibliography

Baca-Pogorzelska, Karolina. "How Chernobyl Fake News Poisons Nuclear Energy Debate in Poland." Notes from Poland (website). April 25, 2020. https://notesfrompoland.com/2020/04/25/how-chernobyl-fake-news-poisons-nuclear-energy-debate-in-poland/.

Colomina, Carme, Héctor Sánchez Margalef, and Richard Young. *The Impact of Disinformation on Democratic Processes and Human Rights in the World*. Strasbourg, FR: European Parliament, April 2021. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653635/EXPO_STU(2021)653635_EN.pdf.

European Centre of Excellence (CoE) for Countering Hybrid Threats. *Countering Disinformation: News Media and Legal Resilience*, Hybrid CoE Paper 1. Luxembourg: European CoE for Countering Hybrid Threats, November 2019. https://www.hybridcoe.fi/wp-content/uploads/2020/07/News-Media-and-Legal-Resilience_2019_HCPaper-ISSN.pdf.

Giannopoulos, Georgios, Hanna Smith, and Marianthi Theocharidou. *The Landscape of Hybrid Threats: A Conceptual Model.* Luxembourg: European Centre of Excellence for Countering Hybrid Threats, February 5, 2021. https://www.hybridcoe.fi/wp-content/uploads/2021/02/conceptual_framework-reference-version-shortened-good_cover_-_publication_office.pdf.

Król, Aleksander. "Warsaw Institute Review: Information Warfare against Strategic Investments in the Baltic States and Poland." Warsaw Institute (website) July 19, 2017. https://warsawinstitute.org/information-warfare-strategic-investments-baltic-states-poland/.

"Tackling Online Disinformation." European Commission (website). n.d. https://digital-strategy.ec.europa.eu/en/policies/online-disinformation.

"Time Stopped for Russia in 1945: A Digest of Russia Propaganda for May 31." Ukrinform (website). June 1, 2022. https://www.ukrinform.net/rubric-ato/3504015-time-stopped-for-russia-in-1945-a-digest-of-russian-propaganda-for-may-31.html.

West, Darrell M. "How to Combat Fake News and Disinformation." Brookings (website). December 18, 2017. https://www.brookings.edu/research/how-to-combat-fake-news-and-disinformation/.

— Section 2 —

Mitigations

— 4 —

Early Warning Systems for Cyber Defense in Energy Security

Gabriel T. Raicu and Sarah J. Lohmann

ABSTRACT: Cybersecurity is pivotal to ensuring the collective security of NATO, especially due to the Alliance's dependence on the availability and safety of energy resources. Cyber early warning systems in the field of energy security can make a major contribution to preventing cyberattacks and providing countermeasures capable of securing energy resources and enabling unrestricted military mobility at the Alliance level. This chapter presents the principles of the development of early warning systems and analyzes the advantages and limitations of the current systems. It then proposes a new generation of early warning systems that uses virtualization and artificial intelligence to identify and neutralize attacks before they destroy energy critical infrastructure.

Keywords: early warning, energy security, cybersecurity, resilience

Introduction

Early warning systems (EWS) for cyber defense in energy security are vital to ensuring NATO's medium- and long-term goals. Accurate discovery of threats in their early stages has the advantage of correctly identifying and ensuring the effectiveness of the countermeasures needed to prevent the disruption of the energy, logistical, and operational capabilities of Alliance forces. A defining element of NATO's effectiveness is safeguarding military mobility using modern technologies that provide capabilities for protection and preemptive action against kinetic or cyberattacks. Most current EWS are not adequate to repel cyberattacks on critical energy infrastructure in the emerging technology environment.

This chapter first identifies the challenges with predicting today's cyberattacks. It then analyzes the limitations of current cyber early warning systems (CEWS). Finally, it proposes a new generation of EWS that is having success at defeating malicious cyber intrusions due to its virtualization of critical energy infrastructure and effective use of artificial intelligence.

The design and implementation of CEWS include many research challenges, starting with the correct identification of the generic set of indicators, intelligence gathering, forecasting, and fusing multiple data sources together. With NATO pushing for greater interoperability and mobility than ever before, the need for strategic coherence, operational cooperation and information exchange has never been greater. Energy dependencies will continue to create asymmetries. Hostile actors conduct aggressive energy operations that blur the lines of traditional conflict. Energy infrastructure and the intrinsic access to energy resources can be turned into weapons of trust—breaking against the Allied states in the region through cyberattacks. Potential attacks to the energy supply-chain components could fundamentally disrupt the joint military capabilities and cohesion of the Alliance at a time when NATO's eastern flank and the Black Sea region are under threat.[1]

The adaptability of cyberattackers is enhanced by the process of continuously discovering new vulnerabilities and by unlimited access to information and research resources from malicious actors. Therefore, cybersecurity, viewed from a defender's perspective, must demonstrate a constant ability to adapt and be proactive.

To prevent unforeseeable future effects in energy networks, EWS are required to minimize the security impact by detecting potentially harmful, usually unclassified, system behavior based on an existing knowledge base. Early warning systems must often process fuzzy and low quality (often uncertain) data.[2] The need to process ambiguous data increases due to the volume of threats, increased complexity, and the dynamic of communication and privacy concerns.[3] The problem of learning where the

1. A. Dupuy, "Energy Security Is Critical to NATO's Black Sea Future," Atlantic Council (website), May 12, 2022, https://www.atlanticcouncil.org/blogs/turkeysource/energy-security-is-critical-to-natos-black-sea-future.

2. Joachim Biskup et al., "08102 Working Group Early Warning Systems," in *Perspectives Workshop: Network Attack Detection and Defense*, ser. Dagstuhl Seminar Proceedings, ed. G. Carle et al. (Dagstuhl, DE: Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, Germany, 2008), http://drops.dagstuhl.de/opus/volltexte/2008/1493.

3. David K. Arrowsmith, R. J. Mondrag, and M. Woolf, "Data Traffic, Topology and Congestion," in *Complex Dynamics in Communication Networks*, ed. Ljupco Kocarev and Gábor Vattay (Berlin/Heidelberg: Springer, 2005), 127–57.

next attack will come from using uncertain or ambiguous data is a relatively new challenge. Classical intrusion detection approaches based on traditional algorithms cannot cope with such threats. In order to best understand how an EWS using AI and virtualization improves on the current outdated systems, an assessment of the drawbacks to older generation early warning systems will first be analyzed.

Problem with Older Generation EWS

The growing importance of EWS has manifested itself in the growth of research initiatives in the beginning of the last decade around the world.[4] The major difficulties are to process the petabytes of information provided by trillions of devices interconnected to networks with huge transfer capabilities and to interpret the useful content of encrypted packets, as well as the hypervisor-based services and platforms, proactive for cybersecurity and oriented to future Internet needs. In addition, much of this big data is stored in the complex Cloud environment, where security, confidentiality, and data validity must be secured under conditions that foster maximum trust.[5]

Existing EWS Concepts, Systems, and Sustainable Approaches Overview

Over the past decade, two key techniques have been used to detect network-based intrusions: detecting resources misuse and detecting anomalies. The first comprises the group of signature-based systems where detection is performed by defining malicious behavior, using a set of pre-saved models stored in a database. Traffic is checked in practice for a previously known attack pattern either by testing the entire batch of data, including payload, or by checking the header. Conventional and widely used intrusion detection (IDS) systems cannot work satisfactorily in very high bandwidth

4. Mario Golling and Björn Stelte, "Requirements for a Future EWS – Cyber Defence in the Internet of the Future," in *3rd International Conference on Cyber Conflict Proceedings,* ed. Christian Czosseck and Enn Tyugu (Tallinn, EE: NATO Cooperative Cyber Defense Centre of Excellence, 2011), https://www.digar.ee/arhiiv/en/download/107746.

5. Kai Hwang, Sameer Kulkareni, and Yue Hu, "Cloud Security with Virtualized Defense and Reputation-based Trust Management," in *Eighth IEEE* (*Institute of Electrical and Electronics Engineers*) *International Conference on Dependable, Autonomic and Secure Computing Proceedings* (Chengdu, CN: IEEE Computer Society Technical Committee on Scalable Computing/National Natural Science Foundation of China, 2009), 717–22, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5380613.

environments.[6] It is not feasible to inspect the entire payload due to the great amount of processing power required. There are, however, different ways to overcome these restrictions by using machine-learning techniques to perform a full payload inspection with a bandwidth of more than 1 gigabyte per second.[7]

In the case of systems based on anomaly detection, a behavioral model is built that contains data such as types, quantities, and daily traffic allocation of the monitored network. Detection is done by measuring the current state of the system and comparing it with the values obtained from the model. The approach is effective when machine-learning techniques are used, such as data extraction and evolutionary algorithms, expert systems, and neural networks. One method that can be used to increase efficiency is to combine methods, such as applying evolutionary algorithms to data-mining systems. Due to its characteristics, this type of IDS is often known as Network Behavioral Analysis (NBA).[8] There is an evolutionary step beyond NBA under the framework of Network Situation Awareness (NSA), where the network monitoring process includes high-level visualization and data management.[9] Technical approaches use distributed denial-of-service detection with honeypots, which are set to detect, deflect, or counteract attempts by unauthorized users. Other helpful approaches include diversion of traffic to capture systems, use of the control advantages offered by dedicated protocols, and use of human experience to detect anomalies. The complexity of the analysis and the increasing bandwidth and the large number of services limit the efficient applicability of the listed methods in the long run.

Early warning systems depend heavily on the efficiency of the technologies used that have had several generational developments. Combinations of methods have been proposed to overcome some of the limitations inherent in IDS, such as those based on combined AI methods, event monitoring, data exchange and automated analysis of captured payloads, malicious behavior, and rehearsals. In the last decade, the following examples of technical approaches have been used.

6. Alex Shenfield, David Day, and Aladdin Ayesh, "Intelligent Intrusion Detection Systems Using Artificial Neural Networks," *ICT Express* 4, no. 2 (June 2018): 95–99, https://www.sciencedirect.com/science/article/pii/S2405959518300493/pdfft?md5=e59991f5920a04dc95674cddb9c67e42&pid=1-s2.0-S2405959518300493-main.pdf.

7. "ReMIND – Real-time Machine Learning Intrusion Detection," http://www.first.fraunhofer.de/owx 1 4079 2 2 0 4be4ae1a1c59c1.html.

8. "Network Behavior Analysis (NBA)," Sun Valley Networks (website), n.d., https://www.sunnyvalley.io/docs/network-security-tutorials/what-is-nba.

9. Golling and Stelte, "Requirements for a Future EWS."

EWS and IDS Based on Combined AI Methods

Early warning and intrusion detection systems based on combined AI methods (FIDeS) aim to develop an advanced, intelligent system for detecting Internet attacks on both local area networks and wide area networks as early as possible.[10] The system took into account the classic File Transfer Protocol, Simple Mail Transfer Protocol, and Hyper Text Transfer Protocol, but not the newer protocols, such as Simple Object Access Protocol, which enables distributed elements of an application to communicate as well.[11] The system seeks to reduce the number of false positives resulting from the classical approach to using an anomaly-based IDS in an early warning system based on the use of various AI methods such as declarative knowledge representation, explanation generation, and cognitive assistance, with FIDeS providing assistance and practical instructions, not just simple intrusion detection.

Systems Enabling Responses to Anomalous Live Disturbances

The event monitoring enabling responses to anomalous live disturbances (EMERALD) environment is dedicated to tracking malicious behavior on large networks and consists of a suite of scalable distributed tools for network surveillance, attack isolation, and automated response.[12] The system uses models developed from over a decade of research experience based on the correlation of large volumes of data in distributed systems, offering the advantage of flexibility and abstraction layers given the use of highly distributed, configurable surveillance and response monitors.

Worldwide Observatory of Malicious Behaviors and Attack Threats

Worldwide observatory of malicious behaviors and attack threats (WOMBAT) was developed as a European project (STREP).[13] The project was structured on three levels to achieve its objectives: "(i) real time gathering of a diverse set of security related raw data, (ii) enrichment of this input by means of various analysis techniques, and (iii) root cause identification

10. "FIDeS," Universität Bremen (website), n.d., https://www.informatik.uni-bremen.de/~sohr/FIDeS/index_e.htm.

11. Ensar Şeker, "Use of Artificial intelligence Techniques/Applications in Cyber Defense" (Tallinn, EE: NATO CCD-COE, 2019), https://arxiv.org/pdf/1905.12556.

12. "Event Monitoring Enabling Responses to Anomalous Live Disturbances (EMERALD)," SRI International (website), n.d., http://www.csl.sri.com/projects/emerald/.

13. "Worldwide Observatory of Malicious Behaviors and Attack Threats," European Commission CORDIS (website), n.d., https://cordis.europa.eu/project/id/216026.

and understanding of the phenomena under scrutiny."[14] It has benefited from information resources such as Symantec-managed Deepsight, which is a Cloud-hosted web portal providing technical intelligence. It has also used the worldwide distributed honeypot system operated by Eurocom—a decoy computer system intended to attract cyberattacks to gain information about cybercriminals' identities and methods. Other data have been gleaned from the nationwide EWS used by CERT Polska or Hispasec's largest collection of malwares.[15]

Classical EWS Architectures Limitations, Challenges, and Solutions

Systems that try to monitor network status and detect new network threats and anomalies have the following drawbacks:

- Global monitoring systems like network telescopes, an Internet system that allows the observation of large-scale network attacks, are based on dark address space with high detection rate of worms and network intrusions. Focused attacks, however, are difficult to recognize and attribute.[16]
- Deep Packet Inspection (DPI) can detect many threats and anomalies; however, it cannot be scaled at the level of a large-scale network or Internet backbone.[17]
- Data flows, or reactive programming, are some of the most important sources for information based on the evaluation of sampled flow technology, unable to provide 100 percent accurate results.[18]
- Most IDS systems are limited to evaluating only logs, flows, or packet counts.

---

14. Hervé Debar, "Sticky: March 2008 Archives," WOMBAT Project (website), March 19, 2008, https://wombat-project.eu/sticky/2008/03/.

15. "Worldwide Observatory of Malicious Behaviors and Threats," European Commission CORDIS (website), July 15, 2019, https://cordis.europa.eu/project/id/216026.

16. Konstantinos Demertzis et al., "Darknet Traffic Big-Data Analysis and Network Management to Real-Time Automating the Malicious Intent Detection Process by a Weight Agnostic Neural Networks Framework," *Electronics* 10, no. 7 (2021), https://www.mdpi.com/2079-9292/10/7/781/pdf.

17. Wenguang Song et al., "A Software Deep Packet Inspection System for Network Traffic Analysis and Anomaly Detection," *Sensors* 20, no. 6 (2020), https://www.researchgate.net/publication/340013171_A_Software_Deep_Packet_Inspection_System_for_Network_Traffic_Analysis_and_Anomaly_Detection.

18. Vijay Mann, Anilkumar Vishnoi, and Sarvesh Bidkar, "Living on the Edge: Monitoring Network Flows at the Edge in Cloud Data Centers," in *2013 Fifth International Conference on Communication Systems and Networks Proceedings* (Bangalore, IN: IEEE, 2013), https://www.inf.ufpr.br/aldri/disc/artigos/2014/patrick_art2.pdf.

- There is a weakness in the inherent division between network- and host-based indicators. It is almost impossible to correlate these disparate data streams efficiently.
- Anomaly detection is only performed on a segmented piece of a larger network, is hard to profile as a "normal" operation, and does not provide any level of attribution.[19]
- The operation of heterogeneous infrastructures that cannot be interconnected, regardless of their technological level, is also an obstacle to the efficiency of EWS.

To resolve these issues, the use of a system of artificial neural networks, a computational model with processing elements with inputs and outputs based on predefined functions, provides the average false positive rate percentage of 0.03.[20] The system is particularly useful in detecting and classification of botnet attacks, as well as analysis of standard cyber traffic, cyber-physical systems traffic, and real-time traffic analysis.

A modern IDS is also good at detecting regular intrusions but has low efficiency against AI-powered adversaries in which attackers inject malicious inputs—false positives and negatives. The opponent's malicious AI can use a special alternation of false positive and negative elements to trick IDS into infiltrating the network.

A development to counter adverse AI is currently underway, consisting of several honeypots collecting information needed to train EWS's AI to strengthen machine learning against deception technology. This technology relies on strategically placed decoy systems and cyber-traps around the network. The system is designed to have a confusing and nonlinear response capable of disorienting attackers by preventing them from identifying real targets and allowing observers to track attackers' tactics in real time.[21] Although the deception system is essentially effective, the defense is generally static, making it easier for the opponent to distinguish

19. Eric Gyamfi and Anca Jurcut, "Intrusion Detection in Internet of Things Systems: A Review on Design Approaches Leveraging Multi-access Edge Computing, Machine Learning, and Datasets," *Sensors* 22, no. 10 (2022), https://www.mdpi.com/1424-8220/22/10/3744/pdf?version=1652517852.

20. Maciej A. Mazurowski et al., "Training Neural Network Classifiers for Medical Decision Making: The Effects of Imbalanced Datasets on Classification Performance," *Neural Networks* 21, nos. 2-3 (2008): 427–36, https://doi.org/10.1016/j.neunet.2007.12.031.

21. Daniel William, "How AI Can Help Improve Intrusion Detection Systems," GCN (website), April 15, 2020, https://gcn.com/cybersecurity/2020/04/how-ai-can-help-improve-intrusion-detection-systems/291266/.

over time, using his own AI, a honeypot from a real asset, and defeating the decoy defense.

A few applications provide solutions to the problem of the static defense, such as DeepDig, or DEcEPtion DIGging, developed at the University of Texas at Dallas that "plant traps and decoys onto real systems before applying machine learning techniques in order to gain a deeper understanding of attackers' behavior."[22] DeepDig uses the behavior of real systems it mimics by transforming each cyberattack into a training session for IDS system AI capabilities.[23]

EWS Using Emergent Technologies Addresses Hybrid Threats

Classical cybersecurity models and practices are not conducive to application in emerging or heterogeneous environments such as OT or IoT. Over the last decade, virtualization technologies have drastically changed cybersecurity methods. To meet new security demands in the changing hostile environment, advanced machine-learning techniques promoting new architectures and innovative models for network behavior analysis and learning algorithms need to be developed to build the new generation of EWS systems.

To address this challenge, the principles of virtualization could drastically change the way cybersecurity is applied, forcing mechanisms and rules of application to be reconstrued. The virtual environment is ubiquitous with an accelerated evolution of Cloud computing concepts that will lead to the adaptation of large-scale machine-learning techniques to meet new security challenges.[24] New architectures, sophisticated network behavioral analysis models—which conduct network monitoring to ensure security—and learning algorithms can be used to build next-generation EWS. The goal of this system is also to develop approaches and models for detecting anomalies and behaviors considered within normal limits for systems,

22. Gbadebo Ayoade et al., "Improving Intrusion Detectors by Crook-sourcing," December 9, 2019, in *Proceedings of the 35th Annual Computer Security Applications Conference* (San Juan, PR: Association for Computing Machinery, December 2019), https://www.semanticscholar.org/paper/Improving-intrusion-detectors-by-crook-sourcing-Ayoade-Al-Naami/fef9e447174994c10b359bb1934d19c7c6e4fe9b?p2df; and "Computer Scientists' New Tool Fools Hackers into Sharing Keys for Better Cybersecurity," Department of Computer Science/University of Texas Dallas (website), February 27, 2020, https://cs.utdallas.edu/cs-new-tool-fools-hackers-cybersecurity/.

23. Gbadebo Ayoade et al., "Automating Cyberdeception Evaluation with Deep Learning," in *53rd Hawaii International Conference on System Sciences Proceedings* (Maui: Hawaii International Conference on System Sciences, January 2020), https://www.researchgate.net/publication/337287036_Automating_Cyberdeception_Evaluation_with_Deep_Learning.

24. Kaushik Pal, "10 Ways Virtualization Can Improve Security," Techopedia (website), October 22, 2021, https://www.techopedia.com/2/31007/trends/virtualization/10-ways-virtualization-can-improve-security.

sharing information between multiple EWS depending on threat levels. The approach must be holistic and consider the latest general security management initiatives.

This is done by developing new methods for malware detection and behavioral analysis. Temporal and spatial flow characteristics must then be integrated into the model. Low structured patterns are created by searching for enhanced malware detection at various levels in the network. Sensor data are then interpreted by enhancing distributed analyzing capabilities.[25]

Early warning cybersecurity systems are dependent on the efficiency of the technology and the accuracy of the logic of recognizing a cyber threat.

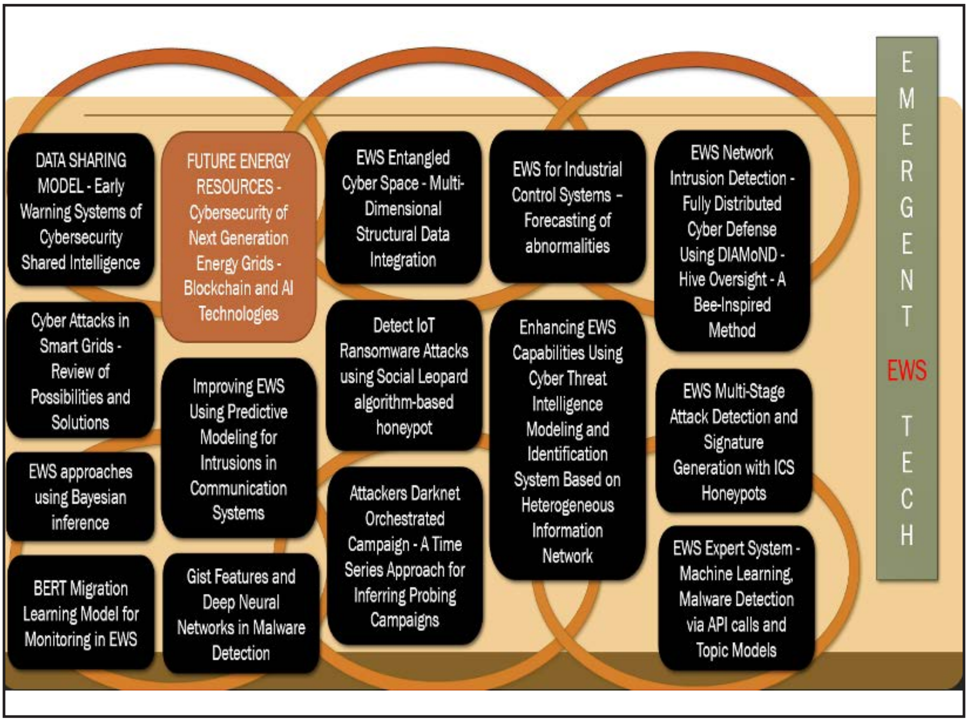

Figure 4-1. EWS extended research directions and development areas explored by the SAS-163 scientific team

Source: Gabriel Raicu and Sarah Lohmann, "Energy Security in the Era of Hybrid Warfare," SAS-163 Research Project Annual Workshop, Project EWS Concepts (Oberammergau, DE: December 2021).

25. M. Golling and B. Stelte, "Requirements for a Future EWS – Cyber Defence in the Internet of the Future," in *3rd International Conference on Cyber Conflict Proceedings*, ed. Christian Czosseck and Enn Tyugu (Tallinn, EE: NATO Cooperative Cyber Defense Centre of Excellence, 2011), https://www.digar.ee/arhiiv/en/download/107746.

To overcome the barrier of efficiency of conventional systems, a series of paradigm shifts can be used. In the following descriptions, a series of principles and methods will be reviewed to open up new areas of constructive approach to EWS.

As an important and general step in increasing the efficiency of the systems, the data-sharing capability will have to be extended to obtain a model of early warning systems with active cybersecurity shared intelligence. An EWS with included cybersecurity intelligence sharing will provide the framework to exchange information in real time and provide updated information to all subsequent modules involved in the system. The main development will be focused on a comprehensive review of knowledge exchange and cyber trust models as well as alternative models from other industrial domains. It will consist of research development by iterative reviews of requirements and features established to support a cyber model that promotes information sharing among partners in coordination with regulatory requirements.

When it comes to EWS to address smart-grid risks, one must consider that smart-grid networks tend to replace traditional networks due to the inherent advantages of efficient management and adaptability to transient regimes, reduced backup requirements, increased resilience and efficiency and self-healing capacity, elasticity in the integration of renewable energy resources, and innovative distribution systems to final consumers.[26] There are, however, a number of elements that need to be considered from a technical point of view. They combine the classical energy network with the ICT network, resulting in a system with multiple advantages because it includes smart devices, monitoring devices, renewable resources, meters, and automatic decision systems.

In addition to the advantages and possibilities of development, smart grids also have a number of disadvantages due to their nature. These disadvantages include the large number of access points, lower physical security, frequent updating of network devices, the difficulty of ensuring trust and the risk of spoofing, communication inefficiency and different level of training between the teams serving the network, the use of protocols and commercial hardware, and software with a high-attack envelope on IP networks and adjacent infrastructure. Attacks can be briefly listed as using dedicated or conventional malware such as ransomware,

26. Suman Advesh Yadav et al., "A Review of Possibilities and Solutions of Cyber Attacks in Smart Grids," in *1st International Conference on Innovation and Challenges in Cyber Security Proceedings* (Greater Noida, IN: IEEE, February 2016), https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7542359.

unauthorized access by stealing or leaking credentials, false alerts, distorted messages, denial of service, and traffic analysis and network mapping for future exploitation.[27]

Detection measures must be approached holistically due to their complexity since attackers can range from non-malicious users, who may harm the system out of sheer curiosity, to dissatisfied consumers, untrained or unhappy internal employees, rivals, terrorists, or hostile state actors. It is also difficult to have accurate attack attribution, due to the risk of plausible deniability or the use of pressure groups made up of disinformed users.

When the issue of long-term sustainability involves the use of renewable energy, blockchain and AI technologies must be considered as a base for cybersecurity of next generation energy grids. Renewable energy sources and the increasing interest in green energy has been the driving force behind many innovations in the energy sector, such as how utility companies interact with their customers and vice versa.

Even though this new combination brings a plethora of advantages, it also increases the cyberattack surface of the energy grid. These vulnerabilities can be aggravated by cybersecurity challenges but alleviated by the advancements in AI and blockchain technologies. In the following section, a series of technologies that approach the problem of threat detection and ensuring resilience are reviewed.

27. Rossella Mattioli and Konstantinos Moulinos, *Communication Network Interdependencies in Smart Grids* (Athens: European Union Agency for Network and Information Security, 2015), https://www.enisa.europa.eu/publications/communication-network-interdependencies-in-smart-grids/@@download/fullReport.

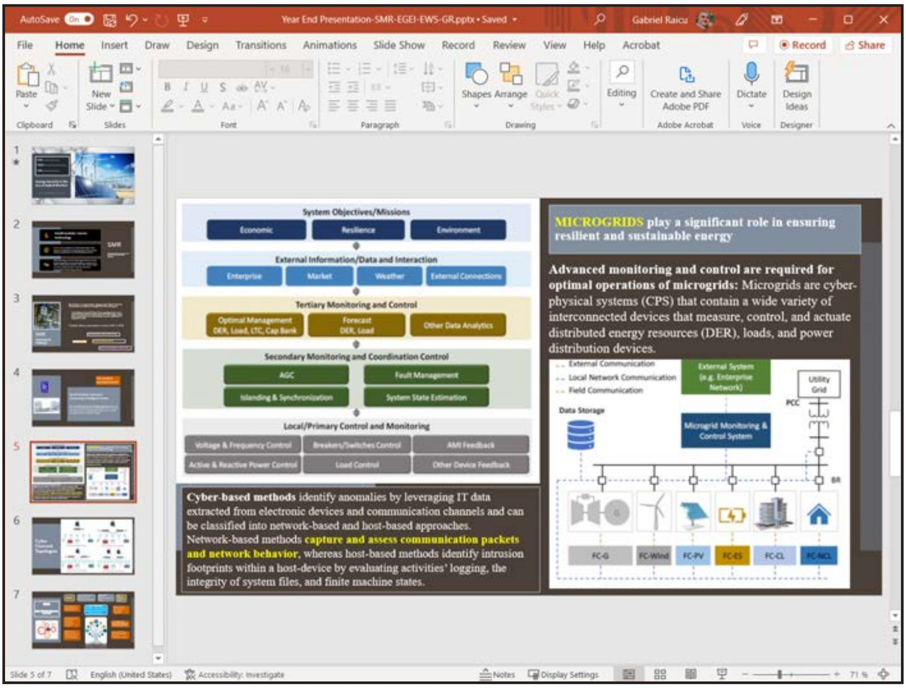

Figure 4-2. Advanced monitoring in microgrids

Source: Tuyen V. Vu et al., "Cyber-Physical Microgrids: Toward Future Resilient Communities," *IEEE Industrial Electronics Magazine*, September 24, 2020, https://ieeexplore.ieee.org/document/9205672.

Forecasting Abnormalities: EWS for Industrial Control Systems

A new feature-based framework of abnormalities forecasting is proposed for early warning for cyber-physical control systems where detection of ICS anomalies must recognize intelligent cyberattacks and differentiate them from naturally occurring errors and failures.[28] The system can have a dual role preventing cyberattacks and providing early signaling of defects. The signals captured from the monitoring nodes are translated into behaviors using feature discovery techniques. Each characteristic has its own behavior and well-defined decision limits between normal and abnormal behavior. A virtual model of the monitored installation such as a power plant is used.[29]

28. Masoud Abbaszadeh and Lalit Keshav Mestha, "Situation Awareness and Dynamic Ensemble Forecasting of Abnormal Behavior in Cyber-Physical System/US Patent Application 20200067969," FreePatentsOnline (website), https://www.freepatentsonline.com/y2020/0067969.html.

29. Masoud Abbaszadeh, Lalit K. Mestha, and Weizhong Yan, "Forecasting and Early Warning for Adversarial Targeting in Industrial Control Systems," in *2018 IEEE Conference on Decision and Control (CDC) Proceedings* (Miami: IEEE, December 2018), https://doi.org/10.1109/CDC.2018.8619332.

The problem of characteristic variation over time is addressed using state models selected by a cluster Gaussian mixture model (GMM). This means that not all subpopulation data points are assigned, but the subpopulations can be learned by the model automatically through a probability distribution. As such, it is the fastest algorithm for learning mixture models.[30] The predicted results over time represent the anticipated evolution of the characteristics, calculated by applying a Kalman predictor adaptive to each overall model. The general forecast of the characteristics is then obtained through the process dynamic mediation based on the future characteristic vector evolution designing process in a retractable horizon mode. The forecast is compared to the decision limit to estimate whether and when the characteristic vectors will cross the border.[31]

One example of the successful use of EWS for industrial control systems is General Electric's (GE) Digital Ghost, which can protect from malicious cyberattacks. It was developed at GE's Research Lab. Digital Ghost provides an additional layer of protection by combining artificial intelligence and machine-learning technologies with sensing and controls to locate and neutralize cyberattacks. The GE engineers used the physics of a natural-gas pipeline, created a Digital Twin, and combined it with machine learning to protect critical infrastructure. In the testing phase, Digital Ghost found and neutralized a cyberattack in the virtualized operating gas turbine at GE Power's manufacturing facility in Greenville, South Carolina. In validation studies, it has located over 98 percent of cyberattacks. It has, however, only been able to neutralize them when over 50 percent of the assets' sensors have already been compromised.[32]

EWS with Fully Distributed Cyber Defense using DIAMoND

Another approach allows the use of local information available on nodes and distributed decision-making algorithms to detect and exploit critical system resources. The main feature of this method is the unusual ability to detect anomalies quickly, using little memory and only local information. The efficiency of the system allows an increase of about 20 percent in the detection capacity over parallel isolated anomaly detectors. The algorithms

30. "Gaussian Mixture Models," Scikit-learn (website), https://scikit-learn.org/stable/modules/mixture.html.

31. Lindsay Kleeman, "Understanding and Applying Kalman Filtering" (PowerPoint presentation, Monash University Clayton Campus, Melbourne), https://www.cs.cmu.edu/~motionplanning/papers/sbp_papers/kalman/kleeman_understanding_kalman.pdf.

32. General Electric (GE) Research, "Digital Ghost: Real-time, Active Cyber Defense," GE (website), https://www.ge.com/research/offering/digital-ghost-real-time-active-cyber-defense.

used have a nonparametric, fully distributed coordination framework that translates the biological success of these methods into similar operations useful in cyber defense.[33]

EWS Approaches Using Bayesian Inference

The Internet is the area most exposed to cyber risks due to reduced data structuring and a strong increase in various threats. It requires a combination of classical and innovative approaches using Bayesian inference to analyze network scenarios to detect early threats. Theoretical bases and experimental verifications on real attack scenarios improve the predictive capacity.[34]

EWS Based on Entangled Cyber Space

The major challenge of cyber defense is the inefficiency of counteracting the sophisticated attacks of opponents given the interconnection of modern societies at the level of physical and cyber events. To counteract the effects of this situation, it is necessary to build proactive cyber-defense models that consider the interconnection and relations between events and activities in the physical, social, media and economic realities of cyberspace.[35] The concept of proactive cyber-defense models can use entanglement principles to overcome loosely connected events. Entangled cyberspace is an integrated approach for predicting cyberattacks. It can provide a solid foundation for building proactive cyber-defense models in a seemingly tangled space where there are always major correlations between the physical and the cyber environment.[36]

To generate an efficient early warning system component, continuously adaptable to multidimensional realities and with advanced prediction capabilities, an analytical framework of cyber analysis must be introduced.

33. Maciej Korczyński et al., "DIAMoND: Distributed Intrusion/Anomaly Monitoring for Nonparametric Detection," in *2015 24th International Conference on Computer Communications and Networks* (*ICCCN*) *Proceedings*, (Las Vegas: ICCCN, August 2015), https://www.researchgate.net/publication/278018275_DIAMoND_Distributed_IntrusionAnomaly_Monitoring_for_Nonparametric_Detection.

34. Harsha Kumara Kalutarage, Sira Ahmed Shaikh, and Francis Lee Bu Sung, "Towards an Early Warning System for Network Attacks Using Bayesian Inference," in *2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing Proceedings* (New York: IEEE, November 2015), https://ieeexplore.ieee.org/document/7371513.

35. Ruth Ikwu, "Multi-dimensional Structural Data Integration for Proactive Cyber-Defense," in *2017 IEEE International Conference on Cyber Situational Awareness, Data Analytics and Assessment Proceedings* (London: IEEE, June 2017).

36. Ruth Eneyi Ikwu, "The Entangled Cyberspace: An Integrated Approach for Predicting Cyber-attacks," (PhD thesis, Brunel University London, 2018).

This framework achieves the intersection and correlation of events from multiple physical, social, economic, and virtual layers.[37]

EWS Capabilities Using Heterogeneous Information Networks

The approach addresses the general issue of open exchange of cyber-threat information (ITC) to get a complete real-time picture of the cyber-threat situation. One mandatory step is to design a metaschema of threat information to describe the semantic relationship of the infrastructure nodes, and, in a second step, to model information about cyber threats on a heterogeneous information network (HIN).[38] To do the modeling, different types of infrastructure nodes and rich relationships between them are integrated. Next, it is necessary to define a meta-path and meta-graph infrastructure threat similarity measure (MIIS) and present a heterogeneous graph convolution network (GCN) approach based on MIIS measurements to identify the types of infrastructure node threats involved.

37. Alex Barnett, Simon Smith, and Dick Whittington, "Paper 081: Using Causal Models to Manage the Cyber Threat to C2 Agility: Working with the Benefit of Hindsight" (conference presentation, 18th International Command & Control Research & Technology Symposium, Alexandria, VA, June 2014), https://apps.dtic.mil/sti/pdfs/ADA607000.pdf.

38. Yali Gao et al., "HinCTI: A Cyber Threat Intelligence Modeling and Identification System Based on Heterogeneous Information Network," *IEEE Transactions on Knowledge and Data Engineering* 34, no. 2 (February 2022), https://ieeexplore.ieee.org/document/9072563.

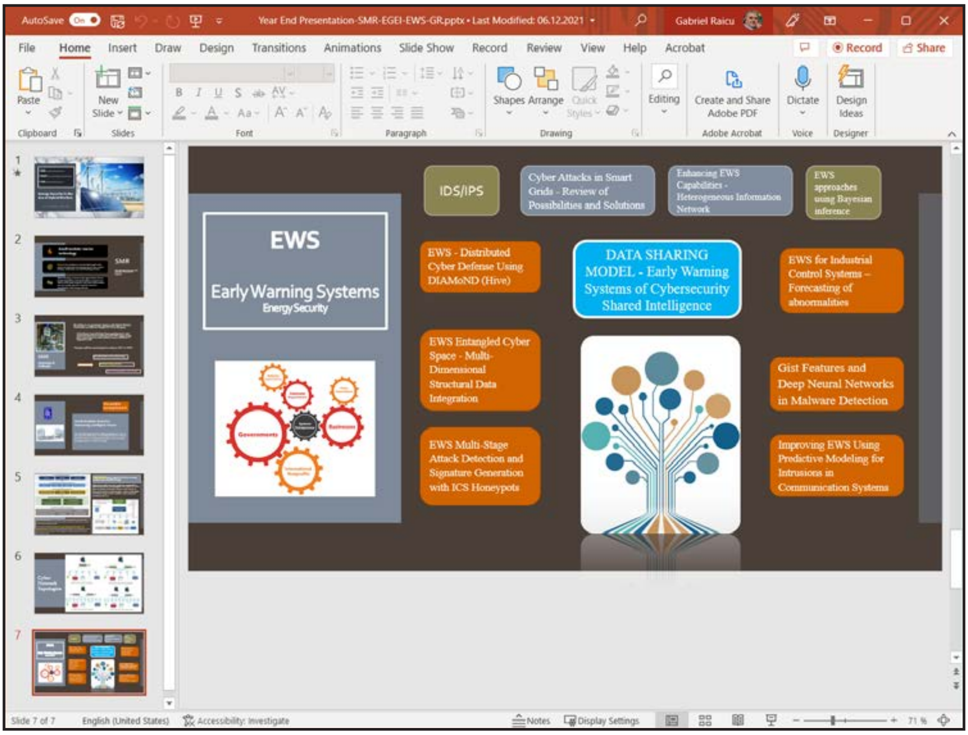

Figure 4-3. EWS emergent technology research directions in the medium term by the SAS-163 scientific team

Source: Gabriel Raicu and Sarah Lohmann, "Energy Security in the Era of Hybrid Warfare," SAS-163 Research Project, April 2022, Project EWS Concepts in the medium term.

Conclusion

The effectiveness of EWS and their degree of relevance vary greatly depending on the approach used. Early warning systems can usually be considered 100 percent effective on a large scale only if the attackers and their attack techniques do not evolve, and the attack patterns are only those already stored in the event history. The major challenge is the lack of adaptability of EWS due to the lack or inconsistency of predictive capabilities, even in classical AI approaches. The authors propose a combination of technologies and methods that, if understood holistically, can provide solutions with significant long-term predictive capabilities to NATO commanders in protecting the new energy environment, which includes renewables, pipeline sensors, smart grids, and IoT integration at every level.

This protection of the energy sector is critical to the Alliance's security, as any disruption affects the continuity of the supply chain and the effectiveness of the defense. It is extremely important that cyber threats in the field of energy security are properly and fully addressed. The Russo-Ukrainian War reiterated the importance of security in the energy sector and logistical capabilities at the Alliance level for the full preservation of NATO's military mobility potential. Increasing military presence in the Black Sea region requires a strong NATO deterrence and defense posture, especially at the cyber and energy nexus. It ranges from strategic coherence and strengthening partnerships across the region to national and common capabilities deployment in the area.

The contribution of new generation EWS automatic response can make the difference between preemptive efficiency and merely reactive measures if old generation EWS continue to be used. These new generation EWS should be used in Allied exercises to improve logistical support and integrated infrastructures. Dual-use critical infrastructures for energy; transport on land, in the air, and on water; and cyber can be modeled and simulated using virtualization and artificial intelligence that employs machine learning for increasingly accurate results. These measures ought to increase significantly the accessibility of energy supplies and the timely and effective military mobility to all contributing NATO nations in a broad spectrum of operational contexts.

Select Bibliography

Abbaszadeh, Masoud, Lalit K. Mestha, and Weizhong Yan. "Forecasting and Early Warning for Adversarial Targeting in Industrial Control Systems." In *2018 IEEE Conference on Decision and Control (CDC) Proceedings*. Miami: IEEE, December 2018. https://doi.org/10.1109/CDC.2018.8619332.

Dupuy, A. "Energy Security Is Critical to NATO's Black Sea Future." Atlantic Council (website). May 12, 2022. https://www.atlanticcouncil.org/blogs/turkeysource/energy-security-is-critical-to-natos-black-sea-future.

"FIDeS." Universität Bremen (website). https://www.informatik.uni-bremen.de/~sohr/FIDeS/index_e.htm.

Gao, Yali et al. "HinCTI: A Cyber Threat Intelligence Modeling and Identification System Based on Heterogeneous Information Network." *IEEE Transactions on Knowledge and Data Engineering* 34, no. 2 (February 2022). https://ieeexplore.ieee.org/document/9072563.

"Gaussian Mixture Models." Scikit-learn (website). https://scikit-learn.org/stable/modules/mixture.html.

Ikwu, Ruth. "Multi-Dimensional Structural Data Integration for Proactive Cyber-Defense." In *2017 IEEE International Conference on Cyber Situational Awareness, Data Analytics and Assessment Proceedings*. London: IEEE, June 2017.

Ikwu, Ruth Eneyi. "The Entangled Cyberspace: An Integrated Approach for Predicting Cyber-attacks." PhD thesis, Brunel University London, 2018.

Kumara, Harsha, Kalutarage, Sira Ahmed Shaikh, and Francis Lee Bu Sung. "Towards an Early Warning System for Network Attacks Using Bayesian Inference." In *2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing Proceedings*. New York: IEEE, November 2015. https://ieeexplore.ieee.org/document/7371513.

Raicu, Gabriel, and Sarah Lohmann. "Energy Security in the Era of Hybrid Warfare." SAS-163 Research Project Annual Workshop. Project EWS Concepts. Oberammergau, DE: December 2021.

Şeker, Ensar. "Use of Artificial Intelligence Techniques/Applications in Cyber Defense." Tallinn, EE: NATO CCD-COE, 2019. https://arxiv.org/pdf/1905.12556.

— 5 —

Microgrids:
The Future of Cyber Secure Energy Independence?

Sarah J. Lohmann

ABSTRACT: Energy insecurity and Russian-backed malicious cyber activity has impacted the European Continent in the lead-up to and the aftermath of the invasion of Ukraine. It is more crucial than ever that US military installations in Europe are able to produce their own energy, even if local grids fail. Malicious cyber intrusions for both the purpose of espionage and destruction of critical infrastructure are being used directly against Ukraine and its allies within NATO. This chapter examines possible solutions to that hybrid warfare through the use of microgrids for military installations.

Keywords: cyber threats, microgrid, energy independence, NATO, military installations, renewables

The severity of cyber threats to the power grid and electricity-dependent infrastructure has far-reaching implications for Mission Assurance policies and programs. Indeed, given the dependence of DOD force projection on civilian-operated ports, transportation assets, and other infrastructure, accelerating the restoration of grid-provided power will be of prime importance for mission assurance. . . . However, adversaries are increasingly threatening this infrastructure as a means to disrupt and degrade US warfighting capabilities.[1]

1. Paul N. Stockton, "Strengthening Mission Assurance against Emerging Threats: Critical Gaps and Opportunities," *Joint Force Quarterly* 95, no. 4 (2019): 24, https://paulnstockton.com/wp-content/uploads/2021/04/strengthening-mission-assurance-against-emerging-threats-critical-gaps-and-opportunities-for-progress.pdf.

What if mission-critical assets on a military installation were not able to function beyond a two-day timespan during a blackout caused by a local grid failure? What if bases using state-of-the-art equipment necessary for protecting the Alliance do not have the backup energy storage and production capability necessary for ensuring basic operations and mission readiness, should grid access be interrupted due to a cyber or kinetic attack? This chapter discusses the immediate threat to energy security on military installations in Europe posed both by shortages and cyberattacks on host nation grids. It proposes that new technologies (such as microgrids) can start creating urgently needed energy independence, even if a host grid fails, and recommends increasing backup capability in the interim.

The Problem

The introductory questions about critical infrastructure resilience are intended as a starting point for addressing mission readiness in the face of the current energy crisis. Cyberattacks on a host nation's grid have wide-ranging impacts on NATO and US military installations—from interrupting aviation and communications to stopping electricity and heat needed to keep operations going.

That is because the US military and NATO allied forces rely on host-country grids and electricity to power operations. In fact, MIT did an assessment for the Department of Defense on the use of foreign grids for US bases operating OCONUS which "strongly recommended that every US military base consider using host nation power" because "in every case, it was found that bases connected properly to host nation power grids would reduce the cost of energy for those bases, reduce fuel usage, and increase the base endurance."[2] While the MIT assessment explains how it has come to the current OCONUS practice, this reliance has the high potential to compromise the US mission.

The problem is, while relying on foreign grids saves money in the short term, it puts our national security at risk during a time when an adversary like Russia is actively attempting to compromise the industrial control systems of grids in the United States and Europe and partnering with China in targeted

2. *Guidance for DoD Utilization of Host Nation Power* (Lexington, MA: MIT Lincoln Laboratory/Sandia National Laboratories, October 2015), www.dtic.Mil/get-tr-doc/pd-f?AD=AD1034495.

hacking campaigns in Europe.[3] This study found that advanced critical energy infrastructure warning and cyber threat mitigation systems currently in place in most NATO member states are not adequate to ensure safety and resilience when emerging technologies are being integrated into energy systems. This problem is largely because cybersecurity applications have not yet been created for the new emerging technology systems being integrated with critical energy infrastructure. As is shown in the case studies of NATO member states to follow in the next section, there are large differences between NATO member states in cyber-mitigation capabilities and standards as pertains to critical energy infrastructure.

Russia and its agents have successfully penetrated energy networks in Europe and North America and deployed malware to undermine critical systems and infrastructure in the target country.[4] It is worth mentioning Germany here as a case study in Russia's penetration tactics, as Germany hosts more US troops than any other European country in NATO. According to the most recent statistics available, 35,221 US active-duty military are based in Germany, as compared to over 12,000 US troops in Italy and 9,000 in the United Kingdom.[5] In addition, there are 173,741 German *Bundeswehr* soldiers, with all but around 3,000 of those serving in Germany.[6] With Germany serving as a hub for NATO member troops, it has been and continues to be a hybrid target.

Germany has been a testing ground for the Russian-based hackers Berserk Bear's malicious cyber activities, from attacking a number of energy companies and attempting to intrude on Germany's grid in 2017 to its long-term efforts to compromise the supply chain of critical infrastructure such as the energy,

---

3. "Alert (AA22-110A) Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure," Cybersecurity and Infrastructure Security Agency (website), April 20, 2022, https://www.cisa.gov/uscert/ncas/alerts/aa22-110a; Nicole Lindsey, "Russia and China Can Cripple Critical Infrastructure in the United States," *CPO Magazine* (website), February 12, 2019, https://www.cpomagazine.com/cyber-security/russia-and-china-can-cripple-critical-infrastructure-in-united-states/; and Maxim Tucker, "China Accused of Hacking Ukraine Days before Russian Invasion," *Times* (website), April 1, 2022, https://www.thetimes.co.uk/article/china-cyberattack-ukraine-z9gfkbmgf.

4. Associated Press, "Russian Officials Charged in Years-Old Energy Sector Hacks," *U.S. News & World Report* (website), March 25, 2022, https://www.usnews.com/news/business/articles/2022-03-24/russian-officials-charged-in-years-old-energy-sector-hacks?msclkid=5fbb7759b8ee11ecb9487d9555eadb7f.

5. "Number of Active-duty United States Military Personnel in Europe in 2022, by Country," Statista (website), February 4, 2022, https://www.statista.com/statistics/1294271/us-troops-europe-country/.

6. "Anzahl der Soldaten und Soldatinnen bei der Bundeswehr von 2000 bis 2022," Statista (website), June 2022, https://de.statista.com/statistik/daten/studie/38401/umfrage/personalbestand-der-bundeswehr-seit-2000/; and "Anzahl der an internationalen Einsätzen beteiligten deutschen Soldaten der Bundeswehr," Statista (website), May 30, 2022, https://de.statista.com/statistik/daten/studie/72703/umfrage/anzahl-der-soldaten-der-bundeswehr-im-ausland/.

water, and power sectors up to the present time.[7] Germany's intelligence services have warned that the group's intention was to imbed malware permanently in IT networks and gain access to OT networks. The same hackers conducted an intelligence-gathering campaign on US energy companies and targets industrial networks.[8]

The problem is compounded when a grid is aging or has lack of energy supply, as is the case in a number of NATO countries, including Germany. Germany's Interior Ministry's federal audit found in 2021 that it is at heightened risk of grid blackouts through 2025.[9] This is due to an aging grid and the energy shortfall as renewables are not able to fill an energy supply gap. *Renewables* are defined by the *Oxford English Dictionary* as "a natural resource or source of energy that is not depleted by use, such as water, wind, or solar power."[10] The gap in energy was predicted by the Interior Ministry's audit in 2021 long before Russia invaded Ukraine, highlighting the fact that renewable technology was not yet advanced enough or producing enough supply to make up for nuclear plants being taken offline and coal needing to be phased out in line with Germany's goals to reduce carbon emissions by 65 percent by 2030 compared to 1990 emission levels.[11]

Hybrid warfare directed at an already unstable grid in the current environment could have devastating effects on Europe's economic powerhouse. As mentioned in the introduction, in the months since the Ukraine war started, Russia has also conducted cyberattacks against Germany's wind energy companies. These cyberattacks have caused one company to shut down its remote-control systems for wind turbines, another to shut down its IT systems, and another's wind turbines to be knocked completely offline.[12]

---

7. Reuters Staff, "German Intelligence Sees Russia behind Hack of Energy Firms," Reuters (website), June 20, 2018, https://www.reuters.com/article/us-germany-cyber-russia-idUSKBN1JG2X2; and Sean Lyngaas, "German Intelligence Agencies Warn of Russian Hacking Threats to Critical Infrastructure," CYBERSCOOP (website), May 26, 2020, https://www.cyberscoop.com/german-intelligence-memo-berserk-bear-critical-infrastructure/.

8. Lyngaas, "German Intelligence Agencies."

9. Marcus Wacket, "Germany's Energy Drive Criticized over Expense, Risk," Reuters (website), March 30, 2021, https://www.reuters.com/article/germany-energy-audit-idUSL8N2LS2RC.

10. *Oxford English Dictionary,* 2nd ed. (2022), s.v. "renewables."

11. "Indicator: Greenhouse Gas Emissions," Umwelt Bundesamt (website), March 15, 2022, https://www.umweltbundesamt.de/en/data/environmental-indicators/indicator-greenhouse-gas-emissions.

12. Joseph Henry, "Europe Cyberattack Results to 'Massive' Internet Outage; about 5,800 Wind Turbines Went Offline," Tech Times (website), March 5, 2022, https://www.techtimes.com/articles/272624/20220305/europe-cyberattack-results-massive-internet-outage-5-800-wind-turbines.htm; and Catherine Stupp, "European Wind-Energy Sector Hit in Wave of Hacks," *Wall Street Journal* (website), April 25, 2022, https://www.wsj.com/articles/european-wind-energy-sector-hit-in-wave-of-hacks-11650879000.

For US military installations, which depend on Germany's unreliable grid, and which have seen a 30 percent increase in force presence since the beginning of Russia's war on Ukraine, the question is not if bases will see grid failure, but when, how often, and for how long.[13] Backup systems and energy independence will be vital to mission success in this setting.

Germany is not the only NATO country facing such issues, nor is it the only country hosting US or NATO installation in Europe that should be prepared for grid blackouts to affect operations in the next six months to two years. A recent report by Microsoft's Digital Security unit shows that Russia-aligned cyber-threat groups were preparing to target organizations allied with Ukraine as early as March 2021. In fact, 93 percent of Russia-backed malicious activity seen on Microsoft's online services in 2021 was aimed at NATO member states—specifically the United States, the United Kingdom, Norway, Germany, and Turkey. These included cyber-espionage activities which could provide Russia with information on how the West would respond to the coming Russian invasion on both the military and humanitarian front, as well as targeted attacks on Ukraine's supply chain vendors.[14] More than 40 percent of the Russian-backed destructive cyberattacks were on Ukraine's critical infrastructure sector, including nuclear and transportation.[15] Knowing Russia is targeting the supply chain and critical infrastructure of Ukraine and its partners in NATO, independent energy resilience must be a top priority for military installations immediately.

Potential Solutions: Renewables-powered Microgrids and Mobile Microgrids

This section will examine the benefits and drawbacks to microgrids being used to provide installations with independent, non-hackable energy sources. A discussion of microgrids' usage and challenges will be followed by an assessment of lessons learned and recommendations.

13. Ryan Morgan, "US Troops Surpass 100,000 in Europe," American Military News (website), June 27, 2022, https://americanmilitarynews.com/2022/06/us-troops-surpass-100000-in-europe/; and Jim Garamone, "News: US to Deploy 3,000 Troops to Romania, Poland, Germany," Joint Base San Antonio (website), February 2, 2022, https://www.jbsa.mil/News/News/Article/2921087/us-to-deploy-3000-troops-to-romania-poland-germany/.

14. Digital Security Unit, "Special Report: Ukraine – An Overview of Russia's Cyberattack Activity in Ukraine" (Redmond, WA: Microsoft, April 27, 2022), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.

15. Digital Security Unit, "Special Report: Ukraine."

Microgrids are an alternative source of energy for military installations as they can island—or separate—if the main grid is attacked. A microgrid is a self-contained power system confined to a small geographic area. Microgrids have been increasingly implemented on US military installations due to their provision of independent energy and cost-saving and environmental advantages. In fact, while the US Navy plans for all its major installations to operate off the grid for two weeks by 2025 due to its microgrid implementation, the US Army announced a plan in February 2022 for each of its 130 bases worldwide to have a microgrid by 2035.[16] Likewise, in the NATO Secretary General's 2022 Climate Change and Security Impact Assessment, NATO listed microgrids as a climate-change mitigation tactic to be used by militaries to reduce military CO_2 emissions.[17]

However, for the purpose of this study, our main research question is not focused on whether grid implementation saves money or improves environmental protection, but on whether it improves cybersecurity and energy independence. Specifically, this chapter examines whether microgrids can provide the resilience military installations need when they island off foreign host grids, and if so, under which conditions they remain powered and cybersecure. To answer this question, several case studies will be examined.

At the Miramar Marine Corps Air Station Miramar in San Diego, California, the microgrid uses methane gas from a nearby landfill, photovoltaic and solar thermal energy, natural gas and diesel, and battery storage to stay powered. In the event of a blackout, the microgrid is expected to stay powered for 21 days, allowing flight line operations to continue. During its first Energy Resilience Readiness Exercise, all mission-critical operations were supported completely by the islanded grid on a workday—through on-site fuel sources.[18] Miramar's renewables have been shown to provide energy to the host grid, but not yet to the microgrid.

In what was touted as the 2019 Project of the Year for the DoD's Environmental Security Technology Certification Program, the Otis Air National Guard tested its microgrid islanding, relying on renewable

---

16. Elisa Wood, "Army to Equip All Bases with Microgrids by 2035 as Part of Carbon-free Electricity Goal," Microgrid Knowledge (website), February 9, 2002, https://microgridknowledge.com/army-microgrid-climate/.

17. Jens Stoltenberg, *The Secretary General's Report: Climate Change & Security Impact Assessment* (Brussels: NATO HQ, 2022), 9, https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/280622-climate-impact-assessment.pdf.

18. "Microgrid at Marine Corps Air Station Miramar," Marine Corps Installations Command, Marines (website), June 30, 2021, https://www.marines.mil/News/News-Display/Article/2677033/microgrid-at-marine-corps-air-station-miramar/.

energy sources, such as wind turbines.[19] It was also supposed to test cybersecure protection and operation of the grid while islanding. While the Otis Air National Guard Base microgrid was able to establish a cybersecure interface operation, it was only able to do so while tied to the main grid. Its microgrid was unable to island due to regulations around only one backup generator being allowed to be used per building or mission, and the single generators experienced power surges beyond what they could handle.[20] If renewables are unable to be utilized while islanded with its microgrid, and cybersecure operation of the grid is only a given while connected to the main grid, it cannot serve as a model in the current grid insecure environment in Europe during active hybrid warfare without compromising national security.

Two other projects are worth briefly mentioning due to their high potential, though their islanding claims have not yet been tested by a natural disaster or cyberattack. The Parris Island, South Carolina, microgrid at the US Marine Corps Recruit Depot has 5.5 megawatts of solar photovoltaic power and a 4 megawatts battery-based energy storage system. The grid has its own integrated control system and can conduct islanding and fast load-shedding capabilities. The load shedding and islanding are an improvement over the Otis microgrid. While the Parris Island microgrid's islanding capabilities are regularly tested, the Department of Energy comments in its "lessons learned" that: "Cybersecurity is also increasingly important and should be considered and implemented at the start of the project."[21] If cybersecurity is not implemented from the first day of a microgrid's active life, security has already been compromised.

Finally, in what could be considered a model for future projects, a microgrid built for Fort Belvoir, Virginia, Army installation, both included cybersecurity on the front end and successfully islanded. The cybersecurity standards of the microgrid met the Risk Management Framework, the National Institute of Standards and Technology Special Projects 800-53 and 800-82 and the North American Electric Reliability Corporation Critical Infrastructure Protection. The Fort Belvoir successful tests demonstrated something the others had not. Not only was it able to island during normal workday

19. Paul Roege, "4 Lessons Learned from the Otis Microgrid Project," *Typhoon HIL* (blog), June 8, 2021, https://info.typhoon-hil.com/blog/4-lessons-learned-from-the-raytheon-technologies-otis-microgrid-project.

20. David H. Altman, "Hybrid Micro-grid with High Penetration Wind for Islanding and High Value Grid Services," ESTCP Project EW-201606, Raytheon Integrated Defense Systems, vii.

21. Elisa Wood, "Military Microgrids: Four Examples of Innovation," Microgrid Knowledge (website), December 3, 2019, https://microgridknowledge.com/military-microgrids-four-examples/; and "Project Profile: Marine Corps Recruit Depot Parris Island – 3.5-MW CHP + Microgrid" (US Department of Energy Southeast CHP TAP, July 2021), https://chptap.ornl.gov/profile/121/MCRDParrisIsland-Project_Profile.pdf.

conditions but also during an unforeseen contingency event when a generator stopped working because of a large load. The microgrid was able to keep working without loss of power and is now considered to be a model for US Army standards, which call for bases to be able to provide for their mission-critical operations for 14 days. One thing to note, though, is that unlike the previous case studies mentioned, the energy sources were fuel-based and did not include renewables. The Fort Belvoir microgrid included three fixed natural-gas generators and four 400-kilowatt mobile diesel generators.[22]

In recently published modeling research, the authors used the successes and lessons learned from bases such as Fort Belvoir, Parris Island, and Japan's Showa Research Base, which isolated a microgrid in Antarctica, to simulate operation scenarios to optimize the conception and design of mission-critical microgrids used for military installations. Its test case was the Alcântara Space Center. There, the off-grid simulation showed that it would be possible to island the microgrid and still guarantee the power supply and operational security of the space center, using algorithms to address the energy generation and demand balance and to deal with unexpected contingencies. Launch campaigns were not possible, however, without the use of dispatchable sources, such as a source of electricity like a power plant.[23]

22. "Mission-Critical Military Base Enhances Resiliency with S&C's Microgrid Control System," S&C Electric Company, November 9, 2020, https://www.sandc.com/globalassets/sac-electric/documents/sharepoint/documents---all-documents/case-study-2000-1002.pdf?dt=637843708562560430.

23. César Augusto Santana Castelo Branco et al., "Mission Critical Microgrids: The Case of the Alcântara Space Center," *Energies* 15 (2022): 3–4, 22–24, 3226, https://www.mdpi.com/1996-1073/15/9/3226/htm.

Lessons Learned and a Way Forward

These results underscore the research cited thus far, which is that each facility has unique energy generation and storage needs which must be considered when optimizing islanding and cybersecurity. In addition, other lessons learned from the case studies include the need to ensure regulations around backup generators and battery storage fit with national security needs, that renewable technology can contribute power to the microgrid once islanded, and cybersecurity is included for microgrids even in the test phase.

One proposal to address the challenges of the unique energy generation and storage needs of diverse bases is with a mobile microgrid, which could be stored and used for backup purposes. While Fort Belvoir has served as a success story for the use of mobile microgrids, it did not incorporate renewables into its microgrid project. A study was done for DoD installations testing a standard mobile microgrid that can carry an average 10-kilowatt load and that could be transported in an International Standards Organization triple container that is 8 feet by 6 feet, 5 inches by 8 feet and is not more than 10,000 pounds. The design was modeled and simulated over the US Army's 14-day resilience standard to see if the battery storage provided, together with photovoltaic and generator power, can bring mission-critical assets back online during an emergency.[24]

The purpose was to see if a mobile microgrid could reduce fuel consumption associated with diesel generators, especially in situations such as large-scale combat operations, to reduce a footprint on the battlefield and so that there is a lower logistics demand. This simulation was examined to see if such a mobile microgrid could provide an immediate independent energy solution for combat forces with little access to fuel. The scenario provides power to supply formations, and the mobile microgrid is located with the division operations center. When the operations center needs to relocate, the mobile microgrid is disconnected, and the solar photovaltaics (PV)—the microgrid control unit—and the emergency diesel generator are loaded back into a flatbed truck and staged for movement.[25]

24. Daniel W. Varley, Douglas L. Van Bossuyt, and Anthony Pollman, "Feasibility Analysis of a Mobile Microgrid Design to Support DoD Energy Resilience Goals." *Systems* 10, no. 3 (74), https://doi.org/10.3390/systems10030074.

25. Varley, Van Bossuyt, and Anthony Pollman, "Feasibility Analysis."

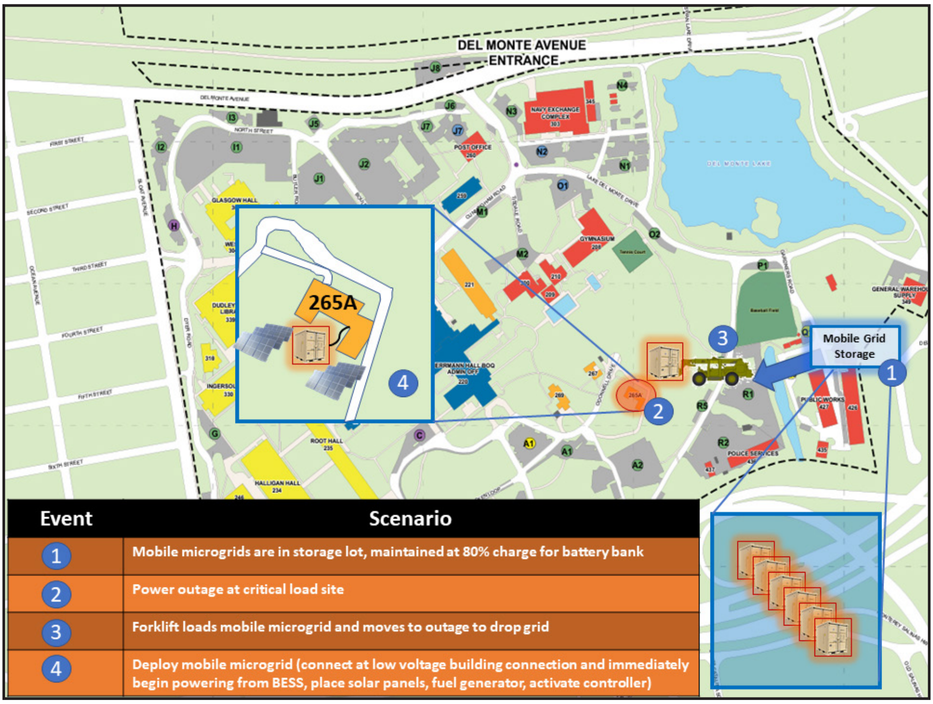

Figure 5-1. Concept of operations for installation of critical load backup power from a mobile microgrid

Used with permission of Douglas Van Bossuyt, Naval Postgraduate School. Originally published in: Varley, Van Bossuyt, and Pollman, "Feasibility Analysis."

The purpose was to see if a mobile microgrid could reduce fuel consumption associated with diesel generators, especially in situations such as large-scale combat operations to reduce a footprint on the battlefield and so that there is a lower logistics demand. This simulation was examined to see if such a mobile microgrid could provide an immediate independent energy solution for combat forces with little access to fuel. The scenario provides power to supply formations, and the mobile microgrid is located with the division operations center. When the operations center needs to relocate, the mobile microgrid is disconnected, and the PV, the microgrid control unit and the emergency diesel generator is loaded back into a flatbed truck and staged for movement.[26]

While the system modeled did reduce reliance on the generator by 37 percent, and the study concluded that a standardized mobile microgrid has advantages that a customized single-load microgrid does not, the assumptions made in the study call for field testing before the mobile microgrids are used in combat.

26. Varley, Van Bossuyt, and Pollman, "Feasibility Analysis."

First, while both winter and summer data were used for the PV in the modeling over a 14-day period, it "did not conduct a detailed accounting of temperature, wind, and other environmental considerations" that could affect PV and the microgrid control system. In addition, the 10-kilowatt load that the microgrid can handle is on the low end for what DoD installations need to carry.[27] However, the modeling of both the mobile microgrid, the Alcântara Space Center, and the very real successes of Fort Belvoir provide promise for the increased use of microgrids on military installations in Europe in the near future.

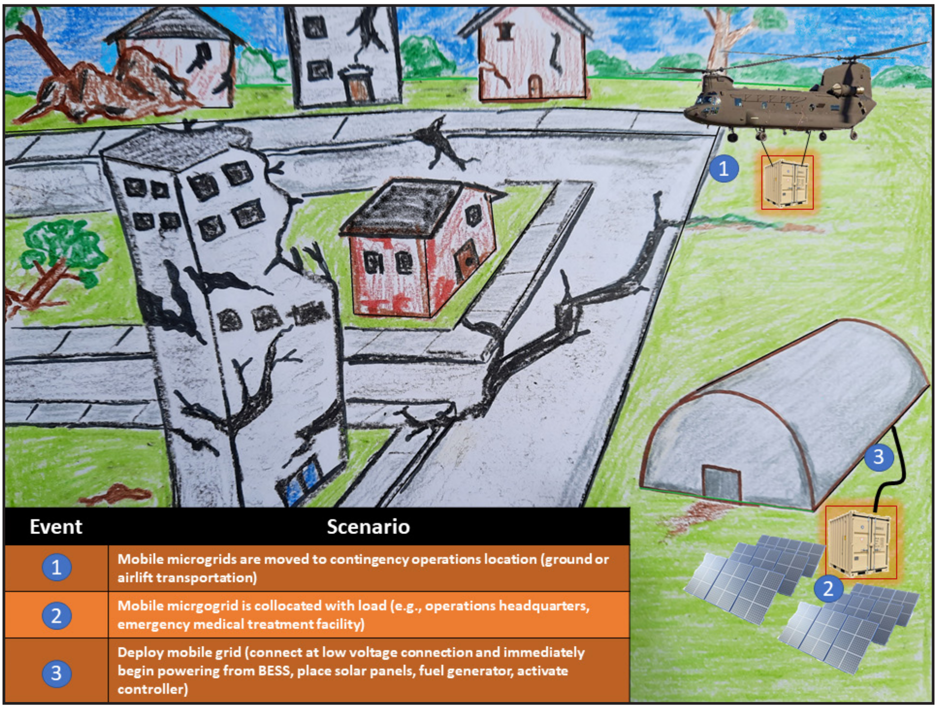

Figure 5-2. Mobile microgrid is airlifted to contingency operations location and can be powered there.
Used with permission of Douglas Van Bossuyt, Naval Postgraduate School. Originally published in: Varley, Van Bossuyt, and Pollman, "Feasibility Analysis."

Before these lessons learned can be transferred to other US military installations in Europe, however, there are three factors that must be considered no matter where the microgrids are being implemented: 1) the regulative process, 2) ensuring microgrids have the power supply they need to be able to island from the host nation grid completely, and 3) ensuring cybersecurity is built into the process from the beginning.

27. Varley, Van Bossuyt, and Pollman, "Feasibility Analysis."

First, the regulative process must be addressed. Part of the challenge with microgrids is their cumbersome approval process. The average amount of time for approval for a US microgrid project is 407 days. That is because each entity that wants to install a microgrid is considered the same as a utility, which falls under the distributed generation facility regulations, with the same amount of paperwork as a massive coal plant.[28] This period is short in comparison to the regulative approval process for some US installations overseas. Foreign regulation of the grid installation and maintenance of the microgrids and the high cost of doing so makes their funding and construction cumbersome, often delaying much-needed projects with red tape before they can ever get started. Microgrid code, power purchase agreements, and unbundling regulations can all stand in the way of a quick implementation of a microgrid.

Recent recognition of the regulation challenge, however, is leading to a new legal framework. For example, within the European Union, nation states are not subjected to unbundling regulations separating the supply from the operation of transmission and distribution as long as they are serving less than 100,000 connected customers. France, Finland, Austria, the Czech Republic, and Flanders also have streamlined processes for gaining approval of closed distribution networks.[29] While additional NATO countries are considering creating streamlined regulative processes due to the current energy process, the US Army and others planning to use microgrids as their energy generator in the near future must calculate the long wait times for the multilevel approval process into their implementation schedule.

Second, power supply must be addressed. As the case studies have shown, while fuel was a reliable power source for the microgrids, renewables such as PV had mixed results and require more field study. While there have been gains in mixed use, such as wind and solar supplemented with diesel and natural-gas generators, renewable technology alone is not yet at a point where it can provide the amount of power needed by installations.[30]

28. Renee Cho, "Microgrids: Taking Steps toward the 21st Century Smart Grid," Columbia Climate School (website), April 18, 2017, https://news.climate.columbia.edu/2017/04/18/microgrids-taking-steps-toward-the-21st-century-smart-grid/.

29. World Business Council for Sustainable Development (WBCSD), *Microgrids for Commercial and Industrial Companies* (Geneva: WSCSD, November 2017), 22–23, https://docs.wbcsd.org/2017/11/WBCSD_microgrid_INTERACTIVE.pdf.

30. Timothy Renahan, "Realizing Energy Independence on U.S. Military Bases," *Joint Force Quarterly* 103, no. 4 (2021): 62–65, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-103/jfq-103_62-65_Renahan.pdf?ver=sQI3ZQ2RqerA6g8Aqkwbdg%3d%3d.

Beyond ensuring energy independence in the future, backup generators are needed urgently at US and NATO bases now—and sometimes more than currently allotted. According to a Pew Trust study on energy on US bases, over the 20 years of a generator's life, the average base has a 50/50 chance of experiencing a week-long outage, and it is very likely that a base will have an outage of one to three days. Current policy, however, only allows the backup of "critical loads," which often do not include R & D laboratories and industrial facilities, which would give the military exponential costs if they were not backed up.[31] Preparedness will mean assessing whether each base has enough backup generators on hand to provide secure protection for the coming blackout seasons for the next four winters and that they also have provided for the diesel and natural gas they will need in the interim until renewable technology can be developed to power the microgrids.

Third, cybersecurity needs to be built in on the front end of the microgrid process, or the microgrid, which is an independent power generator in and of itself, could become a target. A recent Naval Postgraduate School study warned: "microgrids can be a more attractive and likely target due to the importance of their mission and national security value."[32] As shown in several of the US-based case studies, cybersecurity was not included, for example, in the design in Parris Island or able to be sustained while islanded at Otis Air Base. This is a challenge in the microgrid models being produced by NATO allies and European militaries as well. While many of these add an extra layer of vulnerabilities, as their microgrids are connected to smart grids, a study by the NATO Energy Security Centre of Excellence found that European militaries' prototype systems for mobile military camps often lacked cybersecurity considerations.[33]

The study found that cybersecurity was completely missing from the design process in prototype smart-grid systems connecting to microgrids in the prototypes assessed. Various military installation smart grids connecting to microgrid prototypes were examined which were being tested by Canada, NATO, the NATO Science for Peace and Security Organization, the European

31. Jeffrey Marqusee, Craig Schultz, and Dorothy Robyn, *Power Begins at Home: Assured Energy for U.S. Military Bases*, commissioned by the Pew Charitable Trusts (Reston, VA: Noblis, January 12, 2017), https://www.pewtrusts.org/~/media/assets/2017/01/ce_power_begins_at_home_assured_energy_for_us_military_bases.pdf.

32. Christopher J. Peterson et al., "Analyzing Mission Impact of Military Installations Microgrid for Resilience," *Systems* 9, no. 3 (69), https://doi.org/10.3390/systems9030069.

33. Vytautas Butrimas, *Assessment Study of Cybersecurity of Smart-grid Technologies Employed in Operational Camps* (Vilnius, LT: NATO Energy Security Centre of Excellence, August 11, 2021), https://enseccoe.org/data/public/uploads/2021/11/vb-cyber-asses-study-v1dot2dot3-oct-1-2021-cyber-sg-for-mil-camps.pdf.

Defense Agency, and the Dutch military. They all had varying degrees of success at combining energy sources between fuel and solar and wind power. In these cases, they connected to a microgrid with a smart grid, which is a two-way communication system between intelligent electric devices to monitor and control the generation and distribution of electricity.[34] Without cybersecurity built in on the front end, a cyberattack on a grid sensor could be "a single source of failure that can severely affect the safe, reliable and efficient application of renewable energy and smart-grid technologies."[35]

Areas for Further Research

As the energy crisis continues to intensify across NATO countries in the wake of the Ukraine war, military installations, especially in Europe, are preparing for increased energy independence of fuel supply and grid stability. Civilian populations, however, are expected to be equally impacted by fuel supply shortages and grid blackouts for the next three years. In the wake of this energy crisis, further research is needed on how military installations can be prepared for how energy independence on installations could impact the civilian population when there are shortages and should develop a resilience plan that would take into account both national security concerns and local shortages.

In the case studies examined in this chapter, two bases with microgrids were designed for providing for both military and civilian needs during blackouts. The microgrid installation at the Miramar Marine Corps Air Station was able to provide the electricity needed for both the base and for local communities in the San Diego area during the heat wave in summer 2021, reducing the total number of blackouts in the area.[36] Otis Air National Guard Base's microgrid was likewise designed to meet all of the base's needs while islanded because of the wind power and battery storage it is connected to, and also to provide service to a regional grid operator, providing for energy needs across the region in eastern Massachusetts.[37] As mentioned earlier, in practice, the microgrid has not yet been able to island apart from the grid, so sufficient storage will continue to be an area for research for future resilience design.

34. Butrimas, *Smart-grid Technologies Employed in Operational Camps*, 3, 12–16.

35. Butrimas, *Smart-grid Technologies Employed in Operational Camps*, 18.

36. "Microgrid at Miramar."

37. Wood, "Military Microgrids."

While Miramar and Otis have state-of-the-art grids, most military installations, whether in the United States or abroad, do not have the same level of technology. That means that while US bases continue to strive toward energy independence through microgrids going forward, few are at a point of development where they can provide the energy needed for military bases apart from local grids. For the few that are able to provide energy independence to military installations when local communities do not have access to power, national security concerns will need to be addressed in any further research about providing energy to surrounding civilian communities that could be desperate to access that power.

Unlike the examples of Miramar and Otis grids, which were designed to provide electricity to local civilian communities in the United States, any supply of power from US military installations abroad to foreign civilian populations brings with it questions of access, legal concerns, cost, and security impact. These topics would need to be researched and policy decisions made ahead of considering any provision to the broader foreign community. Nevertheless, the main question for most bases through at least 2025 will remain how to ensure that military installations come to a point of resilience in securing the most mission vital assets independently through energy provision and storage without relying on local grids.

Conclusion

Tests and modeling of microgrids on and for military installations in the United States and Europe show that, if constructed correctly, they can provide soldiers with an independent energy source that can island from host nations grids—and thus limit exposure to cyberattacks. Microgrids themselves, however, can become targets and put entire mobile military units at risk if cybersecurity is not built into the design of the microgrid. Renewables have shown some success at decreasing fuel dependency, but further field testing is required to ensure this can be done safely and reliably. Finally, the main inhibitor to the use of microgrids on military installations in Europe is overregulation. If European countries are able to work toward decreasing this regulatory inhibitor, microgrids can be in place sooner to power NATO's missions going forward.

Select Bibliography

"Alert (AA22-110A) Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure." Cybersecurity and Infrastructure Security Agency (website). April 20, 2022. https://www.cisa.gov/uscert/ncas/alerts/aa22-110a.

Butrimas, Vytautas. *Assessment Study of Cybersecurity of Smart-grid Technologies Employed in Operational Camps*. Vilnius, LT: NATO Energy Security Centre of Excellence, August 11, 2021. https://enseccoe.org/data/public/uploads/2021/11/vb-cyber-asses-study-v1dot2dot3-oct-1-2021-cyber-sg-for-mil-camps.pdf.

Branco, César Augusto Santana Castelo et al. "Mission Critical Microgrids: The Case of the Alcântara Space Center." *Energies* 15 (2022). https://www.mdpi.com/1996-1073/15/9/3226/htm.

Marqusee, Jeffrey, Craig Schultz, and Dorothy Robyn. *Power Begins at Home: Assured Energy for U.S. Military Bases*. Commissioned by the Pew Charitable Trusts. Reston, VA: Noblis, January 12, 2017. https://www.pewtrusts.org/~/media/assets/2017/01/ce_power_begins_at_home_assured_energy_for_us_military_bases.pdf.

Peterson, Christopher J. et al. "Analyzing Mission Impact of Military Installations Microgrid for Resilience." *Systems* 9, no. 3 (69). https://doi.org/10.3390/systems9030069.

Renahan, Timothy. "Realizing Energy Independence on U.S. Military Bases." *Joint Force Quarterly* 103, no. 4 (2021). https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-103/jfq-103_62-65_Renahan.pdf?ver=sQI3ZQ2RqerA6g8Aqkwbdg%3d%3d.

Stockton, Paul N. "Strengthening Mission Assurance against Emerging Threats: Critical Gaps and Opportunities." *Joint Force Quarterly* 95, no. 4 (2019). https://paulnstockton.com/wp-content/uploads/2021/04/strengthening-mission-assurance-against-emerging-threats-critical-gaps-and-opportunities-for-progress.pdf.

Stoltenberg, Jens. *The Secretary General's Report: Climate Change & Security Impact Assessment*. Brussels: NATO HQ, 2022. https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/280622-climate-impact-assessment.pdf.

— Section 3 —

Case Studies

– Case Studies –

Western and Central Europe

The case studies presented in this chapter include five NATO nations: France, Belgium, the Netherlands, Germany, and Poland. Of the five countries listed in this section, France is the only one considered to be energy independent, relying mostly on its many nuclear facilities for power. Renewable energy infrastructures have been implemented across Europe with varying degrees of success. They now account for approximately 30 percent of power produced across this region, but many nations are still dependent on imported energy via Russia. Questions have been raised, however, regarding whether the development of new technology is outpacing the ability to secure these new technologies from infrastructure cyber threats.

The nations in the Western and Central Europe regions are the most cyber hardened of the European nations. Cyber threats are developing as rapidly as the technologies created to guard against them. France and the Netherlands, especially, have made great strides in advancing network security systems, with well-connected Internet of Things capabilities secured by reliable, modern network systems. Since the start of the Ukraine invasion, Western and Central European countries have nevertheless suffered cyberattacks by Russian hacker groups on emerging technology such as wind farms.

— 6 —

France

Shuo Zhang and Erin Hodges

ABSTRACT: France has cemented its status as a leader in international cybersecurity by creating some of the most comprehensive cybersecurity policies in Europe and by being a net exporter of energy, having gained full energy independence. This independence gives France autonomy over most of its power usage and distribution, making its electrical grid secure, but its rapid transition to a smart-grid system connected via Internet of Things (IoT) technologies has raised questions of whether development is occurring so rapidly that security is being left behind. The French infrastructure suffers thousands of cyberattacks annually from sources across the globe, including state and non-state actors, and compliance with updated security regulations is not universally enforced.

Keywords: Paris Call for Trust and Security in Cyberspace, cyber defense pledge, cyber norm initiative, Black Hat Europe, French electricity transmission network, Energetic Bear, Enedis, cert.fr

Introduction and Energy Landscape

France has established itself as a leader in both global and national cybersecurity practices, ranking in the top 10 for both metrics according to the National Cybersecurity Index.[1] In 2018, France initiated the "Paris Call for Trust and Security in Cyberspace" based around nine principles for cybersecurity. This initiative has been widely supported in the public and private sectors, including in the European Union (EU),

1. Paola Velasco, "France," National Cyber Security Index (website), March 3, 2021, https://ncsi.ega.ee/country/fr/.

Canada, the United States, and more than 700 private-sector organizations.[2] Because of this expertise, France has taken an active role in supporting and promoting other cybersecurity initiatives in organizations, including NATO, the UN, and the G7.[3] Most notably, it is a member of the UN's Group of Governmental Experts (GGE) on international cybersecurity issues, hosted NATO's first Cyber Defense Pledge Conference in May 2018, and hosted the G7 meeting that established the Cyber Norm Initiative, which has been central to the international cyber stability framework.

Until the Russian invasion of Ukraine, France regularly communicated with the Kremlin on issues of strategic security, including in cyberspace, particularly following Russian interference in the 2017 presidential elections.[4]

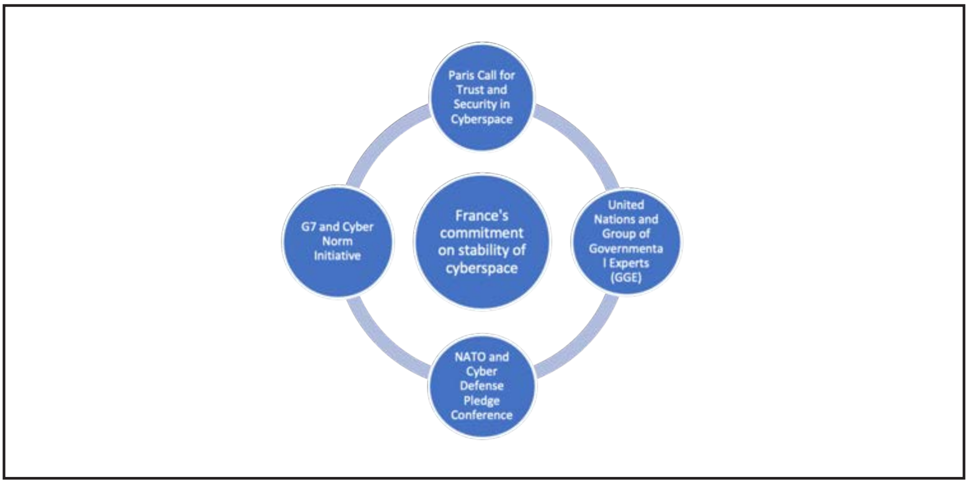

Figure 6-1. France's role in international cybersecurity
Source: Shuo Zhang

According to the World Energy Trilemma Index 2020, France ranked fifth with its combined scores in energy security, equity, and sustainability, but it is outside the top 10 when measuring energy security alone.[5]

2. "Paris Call for Trust and Security in Cyberspace," Paris Call (website), November 11, 2021, https://pariscall.international/en/supporters.

3. "France Diplomacy: France and Cyber Security," Ministry for Europe and Foreign Affairs (website), May 2019, https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/.

4. Juliette Faure, "Macron's Dialogue with Russia: A French Attempt to Fix the European Security Architecture," Russia Matters (website), May 21, 2021, https://russiamatters.org/analysis/macrons-dialogue-russia-french-attempt-fix-european-security-architecture.

5. Oliver Wyman, "World Energy Trilemma Index 2020," World Energy Council (website), https://www.oliverwyman.com/content/dam/oliver-wyman/v2/media/World-Energy-Trilemma-Index-2020-Report.pdf.

While France is less dependent than its neighbors on gas imports from Russia, these imports still make up 17 percent of its gas consumption. In addition, France has recently faced limited electricity generation due to maintenance issues with its nuclear reactors.[6] To deal with its energy shortage, France is calling for reducing consumption by 10 percent over the next two years. France remains, however, a net exporter of electricity, Europe's second-largest energy consumer, and the second-largest nuclear energy generator in the world.[7] As France has limited supply of fossil energy resources, it imports most of its natural gas and oil and all of its coal. France has developed its nuclear energy industry to decrease its reliance on fossil fuels. As of January 2021, about 70 percent of French electricity comes from nuclear energy (with about 17 percent being from recycled nuclear fuel). The government hopes to reduce this to 50 percent by 2035.[8] Moreover, following its energy transition law of 2015, France is attempting to draw 40 percent of its energy production from renewable sources by 2030.[9]

Most renewable energy in France is drawn from hydropower though it is increasing usage of wind (onshore and offshore) and solar photovoltaic systems.[10] Smaller-scale areas of production of renewable energy include biomass combustion and geothermal. Oil imported from Russia ($2.92 billion), the Netherlands ($1.68 billion), Belgium ($1.52 billion), Saudi Arabia ($1.38 billion), and Spain ($1.2 billion) accounts for about 50 percent of French oil usage.[11] As of March 2022, France has announced plans to end oil and gas imports from Russia completely by 2027.[12]

The transition toward renewable energy will inevitably lead to changes in electricity metering, transmission, and distribution. With the increased

6. Dominique Vidalon and Leigh Thomas, "France Working on Contingency Plans as Energy Crisis Looms," Reuters (website), June 27, 2022, https://www.reuters.com/business/energy/france-is-working-energy-contingency-plans-says-finance-minister-2022-06-27/.

7. "France," US Energy Information Administration (EIA) (website), August 2016, https://www.eia.gov/international/analysis/country/FRA.

8. "Nuclear Power in France," World Nuclear Association (website), January 2021, https://www.world-nuclear.org/information-library/country-profiles/countries-a-f/france.aspx.

9. Clara Bauer-Babef, "It's Crunch Time for France's Tumultuous Renewable Energy Debate," Euractiv (website), August 26, 2021, https://www.euractiv.com/section/energy/news/its-crunch-time-for-frances-tumultuous-renewable-energy-debate/.

10. "Renewable Energy in France; What You Should Know," Hive Power (website), June 7, 2021, https://hivepower.tech/renewable-energy-in-france-what-you-should-know/.

11. "Refined Petroleum in France, 2020," Observatory of Economic Complexity (website), https://oec.world/en/profile/bilateral-product/refined-petroleum/reporter/fra.

12. Reuters Staff, "France Wants to End Russia Gas and Oil Imports by 2027 – PM Castex," Reuters (website), March 16, 2022, https://www.reuters.com/world/europe/france-wants-end-russia-gas-oil-imports-by-2027-pm-castex-2022-03-16/.

usage of independent power producers, decentralized production, and renewable energies, the power system will change from highly centralized to a more decentralized, and smart grids and energy storage will play crucial roles.[13]

While the majority of French electricity usage is internally controlled and is transitioning toward decentralized renewable sources, these transitions increase French reliance on smart grids, IoT technologies, 5G connectivity, and artificial intelligence mapping through digital twin technologies and will create more vulnerabilities from cyber threats.

Emerging Technologies: Expansion of Smart-grid Infrastructure, IoT, and 5G

Since 2016, France has focused on drastically expanding its use of smart grids for low- and medium-voltage delivery points. By the end of 2021, the largest distribution network in France hopes to have 35 million low-voltage delivery points equipped with smart meters.[14] These Linky smart meters are estimated to cost 1–2 euros per household monthly over the course of 10 years but are expected to save about 50 euros annually. About 10 percent of the 4.5 billion euros project cost will be used to develop an IT system for the grids.[15] It should be noted that France houses and provides significant funding to the SuperGrid Institute, which does research and design to move offshore renewable energy efficiently to wide areas of use, often far from generation, to promote large-scale optimization.

In September 2020, Schneider Electric partnered with the telecommunications company Orange France to equip its Le Vaudreuil factory outside of Paris with a 5G network, which is believed to be the first use of a private 5G network in an industrial environment. The increased speed from 5G networks is anticipated to improve production efficiencies and augmented reality used for system maintenance activities. The 5G network will connect a robot plant guide and a remote user to complete plant visits to minimize travel time and costs of in-person inspections and reduce the

13. Deloitte Conseil, *European Energy Market Reform Country Profile: France* (Zurich: Deloitte Conseil, 2015), https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Energy-and-Resources/gx-er-merket-reform-france.pdf.

14. Claire Volkwyn, "Fast Forwarding the Energy Transition in France," Smart Energy International (website), October 29, 2019, https://www.smart-energy.com/regional-news/europe-uk/fast-forwarding-the-energy-transition-in-france/.

15. Volkwyn, "Fast Forwarding."

carbon footprint of plant upkeep.[16] Furthermore, a digital map of the plant will be available for inspection, reflecting real-time data.

In addition to 5G, IoT plays a significant role in digitalization. The IoT applications enable all components of the smart grids with IP addresses and two-way communication. A smart grid involves power generation, power transmission, power distribution, and power utilization, and IoT can be applied to these four subsystems. In France, the long-range IoT station is a smart-grid solution developed by Kerlink for machine-to-machine and IoT service operators aiming to run on an independent network.[17]

Furthermore, IoT technology will play a role in the development of microgrids (small-scale smart grids that are semiautonomous, fully islanded, or autonomous), allowing small energy networks to be involved in local production via photovoltaic panels, miniature wind turbines, and fuel cells. The IoT will be an essential factor toward realizing diversity in the energy mix, and it will contribute toward decentralization, allowing supply to regions with poor network coverage (for example, isolated rural zones).[18]

Energy Cyber-related Vulnerabilities

As France's energy transition to renewable energy is expected to accelerate, smart grids will play a major role in realizing France's renewable energy goals. Despite their benefits, the use of smart grids entails cyber challenges. During the Black Hat Europe 2014 conference, two cybersecurity professionals demonstrated that it was possible to hack some smart meters despite the encryption of ingoing and outgoing communications.[19] France has reduced many of these concerns, however, with its smart-meter expansion by transferring smart-meter data through electric and telephone networks rather than the Internet.

16. "Press Release: Orange and Schneider Electric Run Industrial 5G Trials in French Factory," Orange (website), September 28, 2020, https://www.orange.com/en/newsroom/press-releases/2020/orange-and-schneider-electric-run-industrial-5g-trials-french-factory.

17. "Semtech LoRa Platform Selected by KERLINK for First Internet of Things Long-Range Gateway," Device Management Forum (website), https://www.devicemanagement.org/imported-news/semtech-lora-platform-selected-by-kerlink-for-first-Internet-of-things-long-range-gateway/.

18. Laurent Felix and Xavier Metz, *Liberty, Equality, . . . Responsibility? IoT for People, a Driver of Value Creation in France* (Paris: Wavestone/Group Caisse des Dépôts/La Poste, 2018), https://www.wavestone.com/app/uploads/2018/05/IoT-for-people.pdf.

19. Gabrielle Desarnaud, *Cyber Attacks and Energy Infrastructures: Anticipating Risks* (Paris: Études de l'Ifri, January 2017), https://www.ifri.org/sites/default/files/atoms/files/desarnaud_cyber_attacks_energy_infrastructures_2017_2.pdf.

In 2018, there were more than 4,300 cyberattacks on the French Electricity Transmission Network (RTE).[20] With digitalization, the incorporation of IoT and 5G with smart grids is inevitable. According to the European Parliament, "development of smart energy has also led to exponential growth of networked intelligence throughout the energy grids and also consumer premises."[21] Together with decentralization and diversification of energy technologies, the growth of digital technologies like IoT and 5G can expand the potential surface for cyberattacks in energy systems. Hence, cyberattacks can now target people, products (physical and data infrastructures), and processes (system information flow).[22]

Energetic Bear

In 2014, approximately 250 energy companies in the United States and Western Europe were infected by a malware known as Energetic Bear.[23] The industrial control systems (ICS) were affected, and the malware, similar to that used in the Stuxnet attack, allowed the attackers to monitor energy consumption in real time or attack physical systems like power plants, wind turbines, and gas pipelines.[24] Since the group behind Energetic Bear is suspected to have ties to Russia, it is important to be aware of potential vulnerabilities relating to ICS, especially since Energetic Bear has an active presence in France.[25]

As smart grids are considered a form of ICS, it is important to understand the vulnerabilities of smart grids. Smart grids enable transitions to an open, largely decentralized, and digital infrastructure. They are now more exposed to cyberattacks, however, from communication networks and computer applications, resulting in severe destructions to the electricity network.[26] There are three main cyber challenges for smart grids. First, a high complexity

---

20. Patrice Mallet and Hicham Kadiri, "Risk of Cyber Security Attacks on Smart Grid," BearingPoint (website), February 27, 2019, https://www.bearingpoint.com/fr-fr/blogs/energie/risk-of-cyber-security-attacks-on-smart-grid/.

21. International Energy Agency (IEA), *Digitalization & Energy* (Paris: IEA, 2017), https://iea.blob.core.windows.net/assets/b1e6600c-4e40-4d9c-809d-1d1724c763d5/DigitalizationandEnergy3.pdf.

22. IEA, *Digitalization and Energy*.

23. Desarnaud, *Cyber Attacks and Energy Infrastructures*.

24. Sam Jones, "Energy Companies Hit by Cyber Attack from Russia-Linked Group," *Financial Times* (website), June 30, 2014, https://www.ft.com/content/606b97b4-0057-11e4-8aaf-00144feab7de.

25. Sam Jones, "Energy Companies Hit by Cyber Attack from Russia-Linked Group."

26. European Cybersecurity Organisation (ECSO), *Energy Networks and Smart Grids: Cybersecurity for the Energy Sector* (Brussels: ESCO, November 2018), https://ecs-org.eu/documents/publications/5fdb2673903c6.pdf.

level and volume of interconnected components require security solutions that prevent domino effects, particularly when a large number of components are compromised. Second, resource-constrained legacy energy systems with very long lifetimes may be unable to integrate with new components and new security requirements. Finally, an increase in attack surfaces because of new data interfaces, for example, new and connection-oriented meters, collectors, and other smart applications (like IoT) creates additional potential entry points for attackers.[27] Thus, smart grids' components—from smart meters to power-plant relays, including software components and supervisory control and data acquisition (SCADA) systems that monitor these components—can be vulnerable targets for cyberattacks.

Since smart grids are the digitalization of energy infrastructure, it is important to understand that the connection of any physical device to the Internet will involve some digital security risks. The digital security risks posed by IoT are similar to those related with ICS.[28] In the case of smart grids, the attackers could exploit IoT devices' vulnerabilities to move into smart grids remotely. The vulnerabilities embedded in the smart grid can be easily exploited to cause malfunctions in the electric-power system.

Intrusion Campaign on Centreon

In 2021, France identified an intrusion campaign with affiliation to the Russian military intelligence agency GRU that targeted Centreon, a French software company. The campaign began in late 2017 and continued until 2020.[29] The campaign had numerous similarities with previous cyberattacks attributed to Sandworm, which is notorious for conducting consequent intrusion campaigns before aiming at specific targets that suit its strategic interests inside the victims' pool. The attack was a result of Internet-exposed systems via the use of a P.A.S. web shell and an Exaramel backdoor to gain control of the Centreon system and its nearby network.[30] Although only users of an outdated open-source version were affected, the campaign served as a crucial warning since Centreon's major customers

27. ESCO, *Energy Networks and Smart Grids*.

28. Pooja Anand et al., "IoVT: Internet of Vulnerable Things? Threat Architecture, Attack Surfaces, and Vulnerabilities in Internet of Things and Its Applications towards Smart Grids," *Energies* 13, no. 18 (2020): 4813, https://doi.org/10.3390/en13184813.

29. Laurens Cerulus, "France Identifies Russia-linked Hackers in Large Cyberattack," *Politico* (website), February 15, 2021, https://www.politico.eu/article/france-cyber-agency-russia-attack-security-anssi/.

30. Maria Henriquez, "French Cybersecurity Agency Warns of Intrusion Campaign Targeting Centreon," *Security* (website), February 18, 2021, https://www.securitymagazine.com/articles/94629-french-cybersecurity-agency-warns-of-intrusion-campaign-targeting-centreon.

include Électricité de France (EDF) and Total. The campaign could possibly result in a detrimental cyberattack to France's energy sector, which would impact several French energy companies. Moreover, the attack type has also shown the vulnerability of attacks on suppliers whose software needs regular updates and patching.

Since the use of 5G networks will increasingly revolve around software, risks from security flaws can increase because of suppliers' poor software development processes, allowing malicious actors to insert backdoors to the products. The mobile network operators' dependencies on suppliers can also increase exposure to risks, increasing the number of attack paths that can be manipulated by malicious actors and thereby increasing the possible severity of the attacks' impacts.[31] Additionally, the 5G risk landscape merges traditional IP-based threats with the all-5G network and insecure legacy (2/3/4G) threats.[32] The most sensitive information is conveyed via core network functions, and impacts to the core networks could potentially compromise the integrity, availability, and confidentiality of the entire 5G network services.[33] Amongst the possible malicious actors, non-EU states or state-backed actors are most likely to target 5G networks, and their attacks are deemed the most serious.

Other Notable Cyberattacks

During the COVID-19 pandemic, the number of cyberattacks in France increased fourfold, with 200 large-scale cyberattacks across 12 areas of critical infrastructure, including health, defense, and banking.[34] In 2021, two French hospital groups were affected by ransomware attacks in less than a week.[35] Energy as a critical sector could be targeted in France as it has been in other parts of the world.

31. NIS Cooperation Group, *Cybersecurity of 5G Networks: EU Toolbox of Risk Mitigating Measures* (Brussels: European Commission, January 29, 2020), https://ec.europa.eu/newsroom/dae/redirection/document/64468.

32. European Union Agency for Cybersecurity (ENISA), *ENISA Threat Landscape for 5G Networks*, ed. Marco Lourenço and Louis Marinos (Athens: ENISA, November 2019), https://doi.org/10.2824/49299.

33. NIS Cooperation Group, *Cybersecurity of 5G Networks*.

34. David Keohane and Peggy Hollinger, "Pandemic Brought Surge in French Cyber Attacks, Warns Thales CEO," *Financial Times* (website), April 5, 2021, https://www.ft.com/content/70e1c40d-acc8-4e8e-8ce3-3e0d9901358a.

35. France 24, "Cyber Attacks Hit Two French Hospitals in One Week," *France 24* (website), February 16, 2021, https://www.france24.com/en/europe/20210216-cyber-attacks-hit-two-french-hospitals-in-one-week.

It is imperative to understand that the ease of connectivity by digitalization using 5G and IoT could also further intensify the effects of cyberattacks on smart-energy applications by making it easier to infiltrate the systems for cascading effects.

Mitigation

Since 2008, France has identified cyber threats as a significant concern for its national security, and in 2009 it established the National Cybersecurity Agency (ANSSI) to handle cybersecurity incidents of significant state concern.[36] In 2013, the Military Programming Law (MPL) was passed, marking the first legal milestone for cybersecurity requirements. The legislation called on 200 operators of vital importance (OVI), whose function is necessary for the security and resilience of France, and drew from an existing list established in 1998.[37] Energy sectors were included as OVIs. These companies must provide ANSSI with a list of critical-information systems, implement a security policy using an accredited information system, create a detailed map of both physical equipment and network configurations, and notify ANSSI in case of any cybersecurity incident. In return, the Operational Center for the Security of Information Systems (COSSI), a branch of ANSSI, will attempt to support the afflicted OVI technically and run cyber forensics to prevent similar attacks to other companies.[38] COSSI specializes in identifying vulnerabilities in current systems, defining response strategies, and analyzing, monitoring, and responding to cyber threats 24 hours a day as the government's Computer Emergency Response Team (CERT-FR).[39] The emergency response team works as the main international point of contact for all cyber incidents affecting France.[40]

Beyond informational technologies, ANSSI has been certifying the security of industrial control systems like program logic controllers,

---

36. *French National Digital Security Strategy* (Paris: France Republic, October 16, 2015), https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf.

37. "The French CIIP Framework," ANSSI (website), https://www.ssi.gouv.fr/en/cybersecurity-in-france/ciip-in-france/.

38. Desarnaud, *Cyber Attacks and Energy Infrastructures*.

39. Robert S. Dewar, ed., *National Cybersecurity and Cyberdefense Policy Snapshots* (Zurich: Center for Security Studies, September 2018, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports_National_Cybersecurity_and_Cyberdefense_Policy_Snapshots_Collection_1.pdf.

40. Melissa Hathaway et al., *France: Cyber Readiness at a Glance* (Arlington, VA: Potomac Institute for Policy Studies, September 2016), https://potomacinstitute.org/images/CRI/CRI_France_Profile_PIPS.pdf#page=9.

which change system dynamics based on input received from the system itself. Finding (or creating) products that are secure by design will take significant time, so IT cybersecurity remains paramount to cybersecurity.

As mentioned above, Enedis, France's primary energy supplier, has also avoided some cyber vulnerability through ensuring consumer data sent from smart meters is encrypted and sent to an Enedis data center via non-Internet channels. These data are then isolated. Return communication from data centers are sent from tamper-proof hardware known as *security modules*, which are regulated under ANSSI.[41] While these means are more secure than others, all connected objects with digital functions are still vulnerable to cyberattacks.

Strengths and Weaknesses

Based on France's cybersecurity blueprint, France has a relatively strong system established for ensuring security of its critical infrastructures. The French method features heavy involvement of energy companies during the establishment of ministerial policies and regulations, offering tailored responses catered to specific needs. Overall, this method has helped establish trust between the French authorities and the OVIs. The EBIOS method recommended by ANSSI will be able to forge interactions between different functions within an organization, encompassing the entire life cycle. By having appropriate risk analyses, this method can potentially lead to adequate security measures, adjusting to local needs and corresponding challenges.[42] Risk mitigations will allow identification of sensitive components within the system. Mitigation strategies (such as a defense-in-depth strategy) that delay the cyber threat are able to enhance protection against unknown threats, decreasing the scope and alleviating the impact.[43]

While the methods are relatively useful in risk mitigations, the traditional risk-assessment process centered on impact and likelihood of threats may have some weaknesses. The usual method of evaluating a system's security is to identify the attack tactics and understand which

41. Desarnaud, *Cyber Attacks and Energy Infrastructures*.

42. French National Agency for the Security of Information Systems (ANSSI), *Managing Cybersecurity for Industrial Control Systems* (Paris: ANSSI, 2012), https://www.ssi.gouv.fr/uploads/2014/01/Managing_Cybe_for_ICS_EN.pdf.

43. ANSSI, *Managing Cybersecurity*.

system components may be compromised.[44] The increase of attacks on IoT, however, together with the increase in availability of advanced attack tools, means traditional risk assessment methods may have difficulty keeping up with emerging threats and utilizing automated and dynamic security methods. Risk-assessment methods focused on attacks may incur high costs for creating secure IoT systems during application and frequent updates on a final system. It is also important to note that even though the CSPN is used widely in France, it is only recognized in France.[45]

Recommendations

With the emergence of malign state and non-state actors, a further increase in cyber-related attacks toward energy infrastructure is on the rise. As France is a major player in economic, political, and military fields and has positioned itself as a mediator in the Ukraine crisis, it will likely continue to be a target for cyberattacks. The following are recommendations.

Security Classification Standards

France should use a new security classification standard focused on systems' functionalities, such as exposure and protection mechanisms. This approach is different from the traditional, risk-based approach, with attacks being a major part of the security evaluation. This approach will allow engineers and designers to have a more concrete standard on security when building critical infrastructure. Unlike the certification method, which is applied after the system is created, the new approach can be applied during the design phase to build secure critical infrastructure (such as advanced metering infrastructure). The classification standards will have goals to be accomplished by engineers in their security designs, and the evaluation will offer guidelines for system implementation to meet required security requirements. The new classification can also be used in addition to the traditional approach, especially when attacker models have to be considered during value-driven evaluations.[46]

44. Manish Shrestha et al., "A Methodology for Security Classification Applied to Smart Grid Infrastructures," *International Journal of Critical Infrastructure Protection* 28 (March 2020), https://doi.org/10.1016/j.ijcip.2020.100342.

45. Hans Baars et al., *Smart Grid Security Certification in Europe: Challenges and Recommendations* (Athens: ENISA, December 2014), 67, https://www.enisa.europa.eu/publications/smart-grid-security-certification-in-europe.

46. Manish et al., "Methodology for Security Classification."

The new security classification standards will aim to achieve the following:

- Provide a set of usual traits, particularly for IoT systems with common traits (communication, composition, attack surfaces, interaction, and after-effects), so it will be easier for security professionals and management officials to recognize risks and safety measures required for new system security, and to have a fast synopsis of the criticality of the systems they are handling.[47]

- Categorize complex systems into predefined groups according to security requirements to analyze the criticality of a system or subsystem. This will also diagnose exposure in terms of which functionality surface may be prone to attacks and would combine the attacks' aftereffects and exposure to attackers.

- Enhance security assurance and transparency on security, building trust between stakeholders involved in the energy sector.

For companies, this new approach will assist in decision making during the system design phase when choosing the most suitable technology and equipment from the vendors.

For end users, the new approach will allow a high-level overview of the security system, enabling them to make better informed decisions on secure system selection. Information regarding exposure and safeguard mechanisms can assist end users, especially users with limited technical skills, in understanding the security level of their product or system, preventing them from using products with weak security features.[48]

Energy Sector Case Study Scenarios

France should consider creating specific case study scenarios tailored to the energy sector. France has cybersecurity plans established. The plans, however, feature general cybersecurity systems guidelines instead of having different guidelines specifically tailored to each industry. While the protocols for cyberattacks may be similar, the stakes in each industry may be different, with different impacts and stakeholders. The growing

47. Manish et al., "Methodology for Security Classification."

48. Manish et al., "Methodology for Security Classification."

trend of new advanced technologies like 5G and IoT may increase the need to have early warning systems or risk mitigations tailored to critical energy infrastructure. Additionally, the presence of legacy energy systems may require additional security requirements and more flexibility during integration with new technologies and components.

The specific case-study scenarios will aim to achieve the following:

- Serve as a framework/guideline for agencies and companies related to the energy sector and to set up tailored early warnings or risk mitigations for applications, such as smart grids, that have incorporated advanced technologies.

- Supplement the current risk scenarios for mitigation methods by helping to understand the scenarios regarding the use of resource constrained legacy systems and establish relevant mitigations when incompatibilities occur, which may include creating suitable patches for outdated systems.

Secure-by-Design ICS Components

Availability and cost are significant limiting factors in selecting secure-by-design ICS components. To ensure the selection of truly designed cybersafe products, purchasers must scrutinize suppliers and ensure secure implementation, installation, and maintenance throughout the lifetime of the system or product.[49] ANSSI should continue to provide up-to-date certifications for as many available products as possible.

Additionally, the certification process should include a series of recommendations for updates to legacy systems that pose a significant threat to a system's cybersecurity. Many distributed control systems and PLCs have been in service for decades and do not meet the security requirements of modern ICS technologies. These updates should focus on migration or modernization projects.[50]

49. Larry O'Brien, "Secure-by-Design Industrial Products Are Increasingly Important," *Control Engineering* 2 (December 2020), https://www.controleng.com/articles/secure-by-design-industrial-products-are-increasingly-important/.

50. O'Brien, "Secure-by-Design Industrial Products."

Conclusion

France is prominently positioned as a leader in cybersecurity and energy security. Its national cybersecurity policies provide an excellent framework for other nations, and its continued participation in global forums will be instrumental in developing widespread industrial cybersecurity policies. While it has not been immune to cyber intrusions, France continues to develop impressive early warning and mitigation strategies that could be aided by critical energy infrastructure mitigation methods and guidelines.

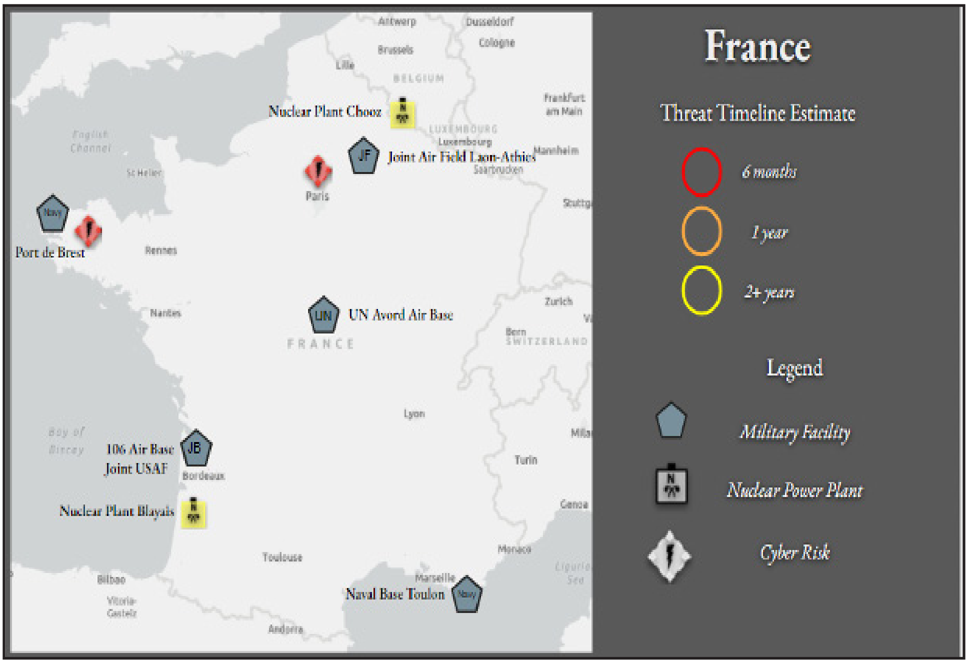

Figure 6-2. Map of France's threat timeline estimate (six months indicates likely attack vector in 2022, one year by 2023, two+ years by 2024 or later)
Credit: Ryan Fisk and Samira Oakes

Location	Reason for Threat Priority and Timeline
Paris	Expect an ICS attack on the Paris sector of the RTE network in the next six months due to technical vulnerabilities in smart grids and elevated tensions with Russia.
Port de Brest	ICS or DDoS attack on both important port terminal and logistical hubs used by the French military within six months due to recent attacks by Russia in neighboring countries.
Chooz and Blayais Nuclear Plants	Expect disinformation attacks and DDoS attacks in two+ years due to Russia's goal of undermining independent European sources of energy as it reduces its import of Russian fossil fuels.

Select Bibliography

Pooja, Anand et al. “IoVT: Internet of Vulnerable Things? Threat Architecture, Attack Surfaces, and Vulnerabilities in Internet of Things and Its Applications toward Smart Grids.” *Energies* 13, no. 18 (September 15, 2020). https://doi.org/10.3390/en13184813.

Desarnaud, Gabrielle. *Cyber Attacks and Energy Infrastructures: Anticipating Risks*. Paris: Etudes de l’Ifri, January 2017. https://www.ifri.org/sites/default/files/atoms/files/desarnaud_cyber_attacks_energy_infrastructures_2017_2.pdf.

Faure, Juliette. “Macron’s Dialogue with Russia: A French Attempt to Fix the European Security Architecture.” Russia Matters (website). May 21, 2021. https://russiamatters.org/analysis/macrons-dialogue-russia-french-attempt-fix-european-security-architecture.

“France Diplomacy: France and Cybersecurity.” Ministry for Europe and Foreign Affairs (website). May 2019. https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/.

French National Digital Security Strategy. Paris: France Republic, October 16, 2015. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf.

Henriquez, Maria. “French Cybersecurity Agency Warns of Intrusion Campaign Targeting Centreon.” Security (website). February 18, 2021. https://www.securitymagazine.com/articles/94629-french-cybersecurity-agency-warns-of-intrusion-campaign-targeting-centreon?v=preview.

NIS Cooperation Group. Cybersecurity of 5G Networks: EU Toolbox of Risk Mitigating Measures. Brussels: European Commission, January 29, 2020. https://ec.europa.eu/newsroom/dae/redirection/document/64468.

Volkwyn, Claire. “Fast Forwarding the Energy Transition in France.” Smart Energy International (website). October 29, 2019. https://www.smart-energy.com/regional-news/europe-uk/fast-forwarding-the-energy-transition-in-france/.

— 7 —

Belgium

Ryan Fisk

ABSTRACT: The majority of Belgium's energy is currently supplied by nuclear power, but this source is to be phased out by 2035, and no feasible domestic replacement exists. With the EU voting on July 6, 2022, to label nuclear power green energy, Belgium has more possibilities. Right now, domestic renewable energy sources such as wind farms only produce about 10 percent of Belgium's energy, and Belgium has become largely reliant on foreign energy sources—such as pipelines from the UK and Germany, which are experiencing their own energy crises—to bridge the gap in domestic energy needs. Additionally, divided policy interests in the Belgian government have created roadblocks to the creation and implementation of comprehensive security policies to govern new, rapidly evolving technologies, such as the Belgian infrastructure's Industrial Internet of Things (IIoT), leading to outdated security measures and making these technologies more vulnerable to cyberattacks.

Keywords: nuclear power, wind farms, Elia, SCADA, ALEGrO, Cyber Security Coalition, industrial Internet of Things/IIoT, Brabo, energy independence, renewable energy

Introduction and Energy Landscape

Belgium, as the home of the NATO and European Union (EU) headquarters and one of the first NATO member states, holds a unique position within the Alliance. The country has a federal government and three administrative regions: Flanders, Wallonia, and Brussels. The two main languages spoken are Flemish (Dutch) and French. Belgium is bordered by NATO allies: France to the southwest, the Netherlands to the northeast, Germany to the east, and Luxembourg to the southeast. The North Sea is on its northeastern border.

Currently, the principal source of energy, by far, is nuclear.[1] Until recently, more than 50 percent of Belgium's energy supply had been produced among seven nuclear reactors distributed throughout the country. A noticeable percentage of energy consumption is also currently provided by natural-gas products, but it appears future policy intends to reduce that share in favor of renewable energy sources.

In addition to nuclear power, a large offshore wind farm has been developed in the North Sea within the Belgian exclusive economic zone (EEZ) bounds. It currently provides roughly 10 percent of the total domestic energy production.[2] Policy measures are in place to increase the share of energy sourced from renewables in the market, but how those renewable sources will materialize is unclear, aside from a second large wind farm in an area similar to the first. The current North Sea wind farm is a conglomeration of individual wind farms operated by various corporations: Mermaid, Northwester II, Belwind, Nobelwind, Seastar, Northwind, Rentel, C-Power, and Norther. These farms comprise one area of the territory designated for wind power. The other large farm will be developed in the coming years in another Belgian EEZ location. While some of the farms use a communal transmission system to the coast, others have their own transmission lines. All, however, connect to the national electrical grid.

Belgium has a single manager of the electrical grid, Elia, which manages the entire country. Elia is responsible for the domestic grid, but it is also the group that manages connections to the transmission lines of utility companies for external countries. Elia is part of a larger organization, Elia Group, which also manages a transmission system operator in Germany. As such, Elia Group and its TSOs are actors with major roles in the increasing interconnectivity of European electricity.

It is also important to note that the Central European Pipeline System (CEPS), originally intended for use by NATO but later expanded to include uses for civilians, transits Belgium. Jet fuel at the Brussels airport

1. "Country Nuclear Power Profiles 2019 Edition: Belgium (Updated 2018)," International Atomic Energy Agency (website), 2018, https://www-pub.iaea.org/MTCD/publications/PDF/cnpp2019/countryprofiles/Belgium/Belgium.htm.

2. "Belgian Offshore Platform," Belgian Offshore Platform (website), n.d., https://www.belgianoffshoreplatform.be/en/.

is supplied by CEPS.[3] In times of conflict, the military use is guaranteed priority; in a worst-case scenario, this could lead to an aircraft fuel shortage.

The largest immediate vulnerability in the Belgian energy landscape comes from the projected domestic energy deficit and the increasing dependence on external sources for energy. The deficit has become clear to the federal government: the 10 percent of energy coming from renewables is not enough to make up for the over 50 percent from nuclear power scheduled to be phased out by 2025. In order to make up for the decreasing share of domestic production, the Belgian federal government has completed, and is in the process of agreeing to several import policies from external countries (primarily Germany, the United Kingdom, and the Netherlands) through a 10-year development plan from 2015–25.

The import infrastructure arrangement from Germany is designated ALEGrO. A collaboration between Elia and a German grid operator, Amprion, ALEGrO stands for Aachen Liège Electricity Grid Overlay. A roughly 90-kilometer underground cable, it connects an Amprion-operated station located in Oberzier, Germany, to an Elia-operated station in Lixhe, Belgium.[4] ALEGrO is significant because it is the first direct transmission line from Germany to Belgium, and Germany will soon provide a major source of electricity during the winter. Use of the line began in November 2020.

The import plan from the United Kingdom is designated NEMO. Similar to ALEGrO, it is the first direct transmission line between the United Kingdom and Belgium. NEMO's line is both subsea and underground and connects Richborough in the United Kingdom to Herdersbrug in Belgium.[5] The Belgian station is again operated by Elia, and the British side is operated by Siemens, which is headquartered in Germany. Operation of NEMO began in 2019. It is also important to note that Siemens has planned a transmission line between the United Kingdom and Denmark called the Viking Link.

NEMO holds particular significance in the Belgian energy landscape. In addition to the new interconnection between the United Kingdom and Belgium, NEMO included the coordination of construction (by Elia) of the Stevin Line, a main line for routing the energy produced by the wind

3. "Central Europe Pipeline System (CEPS)," North Atlantic Treaty Organization, 2017.

4. Joëlle Bouillon, "ALEGrO," Amprion (website), n.d., https://www.amprion.net/Grid-expansion/Our-Projects/ALEGrO/.

5. "We Connect Europe: Nemo Link Supplies Electricity across Borders," Siemens Energy (website), n.d., https://www.siemens-energy.com/global/en/news/magazine/2020/intereuropean-hvdc-link-nemolink.html.

farm in the North Sea to the coast and then further inland. The Stevin Line is connected in the North Sea to a modular offshore grid, which serves as a junction for the energy produced by the individual wind farms. The line then travels from its offshore origin to substations on the coast. Once the electricity reaches the coast, it can be routed to the NEMO Line for electricity exchange between the United Kingdom and Belgium.

Brabo is the import plan from the Netherlands. Brabo consists of three subprojects, all taking place at the Port of Antwerp.[6] Brabo II increases the capacity of the local grid and was intended to prepare for Brabo III: two underground transmission lines and one overhead transmission line that connect the Belgian grid to the Netherlands. Due to the proximity of Antwerp to the border of the Netherlands, these lines are not long. Commissioning of Brabo III is targeted for 2024.

This increase in projects shows a palpable shift from independent domestic energy production to a reliance on external sources of energy while the proportion of domestic renewable production increases in volume. The dependence on external sources is a vulnerability. Should circumstances outside Belgian political control reduce the incoming supply, the country could be at risk of a significant energy shortage because it will no longer have the capacity to produce enough energy on its own. It would be advantageous for new connections to be made with NATO allies. An increasing Alliance-wide interdependency lacks redundancy, however, and, as such, may become a target.

In addition, as discussed below, this vulnerability is compounded by the fact that Internet of Things–enabled critical infrastructure is being developed across Belgium and the NATO alliance as a whole. If, for example, a hostile actor discovered a zero-day exploit in the control software of an Internet of Things–enabled electrical transmission line from the North Sea, it could interrupt transmission at dangerous times, such as a moment of high reliance on renewables due to low import capacity from other countries.

Emerging Technology: Internet of Things

The Internet of Things (IoT) refers to the increasing interconnectivity of devices to each other and to the Internet and often materializes in the integration of "smart" devices into a domestic environment.

6. "Brabo III," Elia Group (website), n.d., https://www.elia.be/en/infrastructure-and-projects/infrastructure-projects/brabo-lll.

The development of IoT, however, has been in parallel with the development of the Industrial Internet of Things (IIoT). The IIoT functions with the same concept as IoT but as the name suggests, is integrated into industry, utilities, and critical infrastructure. With increasing connectivity, comes increasing vulnerability. What makes IIoT so consequential is that, when it is integrated into critical infrastructure, it becomes a new avenue for hybrid threats to threaten energy security. For example, an IIoT-integrated supervisory control and data acquisition controller (SCADA), the industrial control system (ICS) used to supervise and control large sets of critical infrastructure like power plants and the electrical grid, can now be compromised through the Internet or through malware uploaded to the host network. Penetrating SCADA by cyberattack is not a new phenomenon; this method was the basis of the 2010 Stuxnet attack on the Natanz nuclear facility in Iran.[7] There is a major difference, however, between that attack and how an attack on an IIoT-enabled SCADA controller would be executed. The Iranian SCADA was airgapped, ran on only wired connections, and had to be penetrated through a physical input. In an IIoT-integrated environment that may no longer be the case if an actor is able to exploit a vulnerability in a part of the environment that is connected to the SCADA controller.

Belgium has multiple IoT/IIoT initiatives that have developed in recent years. The first is "Digital Wallonia," a region-wide effort to digitize Wallonia, with IoT/IIoT as a major focus. Managed by the Digital Agency, in turn supervised by the vice president of Wallonia, it focuses on digital and IoT integration into business and public service as well as public technology education and IIoT integration into critical infrastructure. Digital Wallonia has initiated a cybersecurity project intended to improve the security of IoT integration, but the more vulnerable nature of IoT will be a barrier to making critical infrastructure completely secure.

Flanders has a project of a similar nature referred to as the Smart Energy Region initiative.[8] This project is more an alliance between companies than a designated organization with paid employees such as Wallonia. There is still an organizing body, however, the Flux 50, intended to facilitate cooperation between the businesses and corporations that make up the Smart Region initiative. The areas that Flux 50 has prioritized coordination efforts on are 1) energy harbors, 2) microgrids, 3) multi-energy solutions at a district level (an effort to diversify renewable energy sources and something that would

7. Kim Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History," Wired (website), July 2011, https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/.

8. "The Digital Industry in Flanders," Flanders Investment and Trade (website), n.d., https://www.flandersinvestmentandtrade.com/invest/en/sectors/digital-society.

be extremely valuable in ensuring continuity of energy supply), 4) energy Cloud platforms, and 5) intelligent renovation. Several IoT-focused research centers are also located within Flanders.

In multiple cities in Flanders, an IIoT-connected water management system is already in place. Water-Link, a utility company serving over 600,000 people and responsible for urban sewer systems in roughly 10 cities, contracted a smart water management system to increase efficiency.[9] The management system is less of a control system and more of a monitoring system and involves placing several thousand sensors and communication modules in underground hydrants. Data from these sensors are evaluated for loss of water in order to minimize waste and maximize efficiency. While this system does not have the capability to manage water flow, a cyberattack could still cause damage by spoofing incoming data and causing panic over a perceived water shortage, for example. It also raises the question of the vulnerability of IIoT-systems that *are* capable of control, instead of exclusively monitoring them. A cyberattack that could cause a water (or electrical, gas, or oil) shortage could be exceptionally damaging. Belgium does not yet appear to have integrated IIoT into enough of its critical infrastructure to have that security problem, but it needs to be aware of the potential risk as it continues IIOT integration.

The third region, the Brussels-capital region, does not appear to have any region-wide initiatives to integrate IoT into business or industry. Its status as a center of European politics, however, has led it to be the location for many efforts and conferences regarding IoT adoption. It would be unsurprising to see an initiative develop in the future. These initiatives would require a greater degree of security due to the possibility that IIoT exploitation could be used to disrupt NATO or EU operations, for example.

As Belgium undergoes its energy transition, it is very clear that IIoT will be integrated into a greater share of Belgian infrastructure. Several North Sea wind farms (such as Nobelwind and Belwind) have already laid the groundwork for IIoT-connected infrastructure through the implementation of LTE networks.[10] Management sensors are already operational, and it would be reasonable to expect that a larger suite of data-collection oriented sensors and more control-oriented IIoT integration will be in place in the future.

9. Bagaar, "Waterlink: Smart Water Management," Bagaar (website), n.d., https://www.bagaar.be/work/waterlink.

10. "Keeping Belgian North Sea Wind Farms Connected," Power Technology (website), October 8, 2020, https://www.power-technology.com/sponsored/keeping-belgian-north-sea-wind-farms-connected/.

Industrial Internet of Things integration into current and future North Sea wind farms need to be approached with caution. Already, actors have probed Belgian ICS vulnerabilities, and IIoT integration would dramatically increase the number of potential methods of attack. In 2013 and 2014, an APT titled Dragonfly (also known as Energetic Bear) launched malware attacks against targets that were connected to ICS throughout Europe and the United States.[11] One of the companies, Ewon, was a Belgian firm that develops remote-access technology for ICS. In an even more relevant twist, Ewon also develops software to manage IIoT.[12] This includes IoT-enabled programmable logic controllers integral to SCADA controllers in wind farms; it would be reasonable to expect to see these in the North Sea, for example. Dragonfly is thought to be of Russian origin, and the techniques used in its 2013 malware, Havex, are similar to the techniques used in the 2020 SolarWinds hack. The fact that ICS on renewables in Belgium have probably already been explored by APTs should be considered when deciding how much IIoT, and the number of vulnerabilities, should be integrated into an increasingly important source of domestic energy production.

One critical aspect of Belgian IIoT is how Elia will attempt to integrate it into its nationwide electrical grid. As the sole grid manager, how it approaches the security aspect of its monitoring, management, and control will have significant impact on the ability of hostile actors to disrupt the consistent supply of energy regardless of whether it is imported from an international source or if it is produced domestically. Elia has already created "The Nest," a digital laboratory open to all Elia employees in which they can experiment with IoT and artificial intelligence (AI) on the condition that all prototyping be in the pursuit of a greater digitalization of Elia systems. Development programs like this are where increased innovation meets increased security risks.[13]

While the integration of IoT into domestic Belgian infrastructure has the potential to impact the energy security of the country, the increasing cross-border energy importation from Germany, in particular, will create new vulnerabilities. Germany is the fourth-largest investor in IoT technologies for both consumer and industrial purposes; should a hostile actor exploit a vulnerability in the German energy supply, it could directly affect the energy supply to Belgium as well.

---

11. Paul Roberts, "Industrial Control Vendors Identified in Dragonfly Attack," *Security Ledger* (website), July 4, 2014, https://securityledger.com/2014/07/industrial-control-vendors-identified-in-dragonfly-attack/.

12. "IoT Solutions," Ewon (website), n.d., https://developer.ewon.biz/content/iot-solutions.

13. "The Nest, Our Digital Laboratory," Elia Group (website), n.d., https://innovation.eliagroup.eu/projects/the-nest-our-digital-laboratory/.

Vulnerabilities and Potential Trajectories for Hostile Influence

As the headquarters of NATO and the EU, Belgium has the potential to be targeted by criminal activity or an APT for a larger number of reasons than its international stance or domestic policies. While it does not produce major activity in the offensive cyber realm, Belgium's status as a host and participant in these organizations could create motivation for a more intense Russian hybrid warfare campaign waged against Belgium or its geopolitical neighbors regardless of the potential for retaliation. Crippling Belgium would undermine the leadership and proper functioning of NATO and the EU, a long-standing Russian policy objective.

Hybrid one-off attacks or a full campaign in Belgium could take a number of forms and exploit a number of vulnerabilities. As mentioned previously, the most conspicuous vulnerability is the significantly reduced production of domestic energy and the dramatically increasing dependence on external sources when nuclear power is phased out. Belgium would not need to be involved in a direct conflict to begin to see threats to its energy security appear; it would only need to be in proximity to one. In a direct attack on Belgium, the many new transmission lines entering the country could become a target, which could be devastating if attacks on multiple lines were to be executed in concert. The practice of stockpiling exploits is now common, and Russia or another actor could spend a significant amount of time finding flaws or zero-days in new renewable ICS or substations and could deploy them all at the same time.

While a vulnerability is already inherent to the Belgian dependence on external sources, this risk is compounded by some outside sources, like Germany, that are already dependent on external sources for energy. A domino effect is possible. If a source to a source of Belgium lost power, it could affect Belgium and the NATO alliance as a whole.

A second major vulnerability is the near-future integration of IIoT into critical infrastructure and a lack of a national, comprehensive policy plan to address the inherent potential for exploitation. It appears Flanders and Wallonia have a weighty effort to digitize their economy and infrastructure but less of a plan to ensure their security. The IoT's reputation is one of increased convenience but also decreased cybersecurity. The IoT vulnerabilities are widespread and common, as evidenced in the 2021 discovery of the Transmission Control Protocol/IP vulnerabilities that affected an estimated 100 million devices.[14] As IIoT infrastructure grows in popularity, Flanders, Wallonia, and the Belgian federal government will need to conduct more thorough reviews of the critical infrastructure that IIoT can be integrated into.

A holistic analysis of hybrid threat vectors should also address the potential for social disruption and the exploitation of social divisions. As evidenced by the 2016 Russian active-measures style campaign, it is a real threat that has only been amplified by the increasing use of social media. Again, the headquartering of NATO and the EU in Brussels increases the likelihood of disruption.

The primary social divides within Belgium are regional and linguistic, which seed several other potentially exploitable divisions.[15] Flanders, which speaks Dutch, has a large right-wing movement and two right-wing separatist parties. Wallonia, on the other hand, speaks French and tends to vote more on the left. This divide is significant: both regions have a major degree of political autonomy, and social interaction is conducted in separate spheres—with different languages and a regional, not national, media focus. Brussels is the exception and has a more diverse population, though the urban areas speak mostly French. An immediate effect of this division is that it influences the dynamic of elections and the formation of coalition governments. National elections often fail to form viable parliamentary coalitions, and a caretaker government is often a reasonable expectation as was the case from 2018 to 2020.

A second division involves immigration into the country. Mirroring the language and regional split, the right-wing movement in Flanders employs significant anti-immigrant rhetoric.[16] A case in point was a September 2020 rally in Brussels of nearly 4,500 attendees. While the purpose of the rally was to protest the incoming coalition government, much of the advertising for it was centered around immigration to Flanders. In addition, a major factor in the collapse of the 2018 parliamentary coalition was a reaction

14. Lily Hay Newman, "100 Million More IoT Devices Are Exposed—and They Won't Be the Last," *Wired* (website), April 23, 2021, https://www.wired.com/story/namewreck-iot-vulnerabilities-tcpip-millions-devices/.

15. Cecil Meeusen, Joris Boonen, and Ruth Dassonneville, "The Structure of Prejudice and Its Relation to Party Preferences in Belgium: Flanders and Wallonia Compared," *Journal of the Belgian Association for Psychological Science*, November 2017, https://www.psychologicabelgica.com/article/10.5334/pb.335/.

16. Gabriela Galindo, "Outrage after Car Brandishing Nazi Symbols Joins Vlaams Belang Protest," *Brussels Times* (website), September 28, 2020, https://www.brusselstimes.com/133244/outrage-after-car-brandishing-nazi-symbols-joins-vlaams-belang-protest.

to a federal policy that agreed to a UN convention regarding European migrant burden-sharing.[17]

To hybrid actors, these seams are exploitable. Through APT 28/ Fancy Bear, Russia has already demonstrated its disinformation campaigns are based around domestic political circumstances, as in the 2016 US presidential election and the suspected 2017 Macron document dump immediately preceding French elections.

Exploiting social divisions is not the most likely path to reduce the supply of energy, but a large-scale hybrid campaign could use the two in concert. At the same time that a cyber intrusion compromises the critical infrastructure importing electricity from outside countries, a hack-and-dump of relevant, sensitive documents could inflame tensions between Dutch- and French-speaking groups. In addition, synthetic media distribution (like deepfakes) and a disinformation campaign could be launched to further the goal. Compounded with an already volatile situation due to a sudden energy deficit, Belgium could experience significant unrest if this situation were to become feasible.

Early Warning and Mitigation

The three bodies responsible for the management of cybersecurity in Belgium are the Belgian Centre for Cyber Security (CCB), the federal Computer Emergency Response Team (CERT), and the Cyber Directorate of the General Intelligence and Security Service (SGRS). Belgium's CERT is designated CERT.be and is administered by the CCB. In addition to internal coordination between these three organizations, they also interface with a significant number of other relevant stakeholders: NATO, the federal police, and the State Security Service (the VSSE, a civilian intelligence service, distinct from the SGRS). In a practical domestic response scenario, the primary response bodies are CERT.be and the CCB, with support provided by SGRS.

Brought under supervision of the CCB in 2014, CERT.be is responsible for reactive measures to a cyber intrusion or disruption and is also responsible for managing the development and administration of the country's early

17. Matt Apuzzo and Monica Pronczuk, "After 2 Years of Paralysis, Belgium Forms a (Very Fragile) Government," *New York Times* (website), October 1, 2020, https://www.nytimes.com/2020/10/01/world/europe/belgium-government-coalition.html.

warning system (EWS).[18] Its stated mission is to "detect, observe, and analyze online security problems, and to inform various target groups accordingly." Services are provided to essential organizations and businesses: critical infrastructure, utilities, and government. Nonessential businesses and the general public have the ability to utilize a limited part of CERT.be's services, but the majority of information is reserved for organizations with the largest impact on public functioning and safety. Of note, parts of the EWS functioning do not appear publicly available and are unable to be included here.

The CERT.be EWS is a voluntary service primarily intended to be utilized by essential organizations and businesses. The CCB refers to these organizations as Organizations of Vital or Special Interest (OSI), and they are the intended users of the EWS. The EWS in its current form has been in operation since roughly 2016. It is accessible through a portal and contains a malware information-sharing platform, anti-phishing and anti-spear-phishing resources, and a frequently updated list of bad domains. In addition, CERT.be will distribute notifications in the event of a significant development, like a recently discovered zero-day of consequence or an emergency.

Of the information that can be obtained and based on the capabilities discussed above, CERT.be appears designed to anticipate mostly routine criminal activity. It is unclear whether it would be able to preempt a targeted, APT-level attack successfully. It would be reasonable, however, to surmise that the SGRS has the capability to handle the response, or potentially the prevention of a potential attack, of a suspected nation-state actor.

The coordination between Belgian cyber threat-mitigation organizations can be illustrated in the wake of a massive DDoS attack that occurred on May 4, 2021, and continued into May 5. It targeted Belnet, a major ISP that hosts the websites of the Belgian parliament and government agencies, universities, and research institutes.[19] The DDoS saturated Belmont's servers at roughly 11:00 a.m., downing the various websites of roughly 200 customers, including multiple parliamentary and government websites. A DDoS is a relatively uncomplicated attack to carry out, so its origins could have come from any level, and no attribution has been made as of this writing. Of note, the commencement of the attack coincided

18. "Service Definition Document," CERT.be (website), January 2019, https://www.cert.be/en/service-definition-document.

19. "Update: The Belnet Network Is Again Available, Our Teams Remain Vigilant," Belnet (website), May 5, 2021, https://belnet.be/fr/nouvelles-evenements/nouvelles/update-reseau-belnet-a-nouveau-disponible-nos-equipes-restent.

with the appearance of a witness to give testimony to the parliament regarding alleged abuse of Uyghurs in the PRC.[20]

As soon as Belmont detected its servers being flooded, it immediately contacted the CCB. The CCB activated the response function of CERT.be and began a dialogue with SGRS. Details of how the three collaborated to stop the attack and what methods they used are not easily available, but the majority of effects were eliminated within a day.

While CERT.be is the official operational cyber-response organization, Belgium also has a forum, the Cyber Security Coalition, that brings public agencies, private corporations, and academia together to pursue a national-level culture of cybersecurity and best mitigation practices. Judging by organizations that are a party to the forum, it appears the Cyber Security Coalition has been relatively successful in creating a national-level discourse; organizations like the SGRS, CERT.be, Belnet, the armed forces, Digital Wallonia, and a large number of private companies are all members.[21] It is also notable that Huawei is also a member of the Cyber Security Coalition but Elia is not, and there is no explanation immediately evident.

It is important to note that the coordination between and the proper functioning of these organizations have not always been domestic priorities. Belgium was delayed in adopting the provisions of the NIS directive and was nearly brought to court by the European Commission for noncompliance.[22]

Policy Recommendations

As renewable energy becomes the primary source of energy and is increasingly connected to the Internet through IIoT, an increasing number of exploitation options will open up to hostile actors. While EWS may prevent the success of some attacks on critical infrastructure and renewables, some of these will likely succeed. In order to ensure continuity of supply, domestic sources of energy production should be diversified

20. Sarah Coble, "Cyberattack on Belgian Parliament," Info Security (website), n.d., https://www.infosecurity-magazine.com/news/cyberattack-on-belgian-parliament/.

21. "Cyber Security Capability," Cyber Security Coalition (website), n.d., https://www.cybersecuritycoalition.be/about/focus-groups/.

22. "Shaping Europe's Digital Future – Cybersecurity: Commission Urges Belgium, Hungary and Romania to Comply with Their Obligations Regarding Operators of Essential Services," European Commission (website), October 30, 2021, https://digital-strategy.ec.europa.eu/en/news/cybersecurity-commission-urges-belgium-hungary-and-romania-comply-their-obligations-regarding.

as much as realistically feasible. A large and varying supply will complicate an attack, and a redundant system is the best way to ensure continuous supply.

Expanding Renewable Energy

One of the ways Belgium could be successful in creating redundancy in its energy supply chain is by expanding to other sources of renewables outside the North Sea wind farm. Solar, hydro, and tidal energy could all have a place in increasing the number of targets that a cyberattack would have to target in order to do the most damage. As European interdependence grows, diversification could be an advantage for the Alliance as well. Just as other countries will export to Belgium, Belgium will export to them. Should the primary source of generation in Belgium be compromised, it could no longer provide that benefit to the energy security of the Alliance as a whole.

Tailored EWS Capabilities

The EWS should be redesigned to include three new features. The capabilities of the system in its current state are more suited to typical criminal activity than a threat from an APT. As nation-state level hostile activity increases in cyberspace, an EWS better tailored to politically motivated, targeted intrusions is necessary to prevent severe damages to Belgium's critical infrastructure and energy security.

First, it should include a greater number of relevant stakeholders. While the current system of selecting organizations based on their perceived value to the functioning of society is an important step, the EWS should also include a larger number of those charged with protecting critical infrastructure and responding to cyber threats—the armed forces, the SGRS, and the VSSE for example (if they are not already members). Providing real-time information to those tasked with response will facilitate more informed, and thus more effective, prevention and mitigation actions.

Second, it should be redesigned to incorporate more broad and cross-cutting factors into its analysis of threats. Information gleaned from cyberspace is not the sole way of determining the origin of potential threats; activity in cyberspace often mirrors geopolitical activity, so the analysis of political factors should be included in a next-generation EWS. While, of course, no attribution has been made, an EWS with a political analysis capability may have been more successful at anticipating and preventing the DDoS of the parliament on the day testimony was given regarding abuse of Uyghurs in China.

Third, the EWS can serve as a facilitator to further solidarity among NATO allies. Given increasing energy interconnectivity, the security of one is a part of the security of all. A next-generation EWS should be capable of sharing and receiving information from other systems in NATO member states. An improved information flow will highlight trends and threats that may only be discernible with a holistic view. Hybrid threats, especially those that engage in deliberate threshold manipulation, may only be visible at an Alliance-level unit of analysis as compared to a state-level unit of analysis.

Fourth, an effort should be made to increase transparency in the decision-making process and execution of cybersecurity policy. The most effective functioning of any EWS system may be compromised by a corporate fear to share sensitive information regarding technical specifications or breaches that occur on corporate systems. Finding a compromise by giving corporations or utilities and policymakers a seat at the table, however, as compared to dictating cybersecurity policy, may be the only way to find a truly workable solution with the most potential to understand business realities and succeed at the same time in creating more robust cyber defenses. In addition, transparency helps build norms for best practices. If businesses are able to observe other businesses operating with cybersecurity as a priority, they are more likely to follow suit.

Increased Information Sharing

The Cyber Security Coalition, discussed previously, is an excellent step in achieving a higher degree of information sharing. Bringing an increasing number of stakeholders to national-level discussion has the potential to make a real difference. The utmost effort should be made to bring the corporations that supervise the increasing share of domestic renewable production to the table, like those operating the current and future North Sea wind farms. In addition, Elia, as one of the most critical organizations to Belgian energy security on the forefront of national energy innovation, should be party to the Coalition. The company most likely has as much to teach as it does to learn and would serve as an incredibly valuable resource to increasing cyber resilience as a whole.

Comprehensive Technology Standards and Regulations

The last recommendation is that security be built into all aspects of renewables development. In the near future, renewables will produce an ever-increasing majority of the energy supply. Renewable technology has not yet become a top-tier target, but that may change. In order to ensure the future security of Belgium's energy supply, now is the time to create and enforce comprehensive standards and regulations for this critical infrastructure.

Conclusion

Even prior to the Russian invasion of Ukraine, Belgium has been in a state of energy transition. Struggling to recuperate a domestic energy deficit caused by the planned phaseout of nuclear power—which provides over 50 percent of Belgium's energy supply—Brussels has partnered with Germany, the Netherlands, and the United Kingdom to integrate its electricity grid with its neighbors. This interconnectivity provides vulnerabilities, especially considering Germany's reliance on energy imports from hostile actors (such as the Russian Federation). In addition, the growing Industrial Internet of Things leaves increasingly large swaths of critical infrastructure prone to attack from a single entry point. To better address these vulnerabilities, Belgium can expand renewable energy, redesign its early warning system to prioritize APT threats and broaden its scope, increase information sharing with national stakeholders, and implement comprehensive technology security standards.

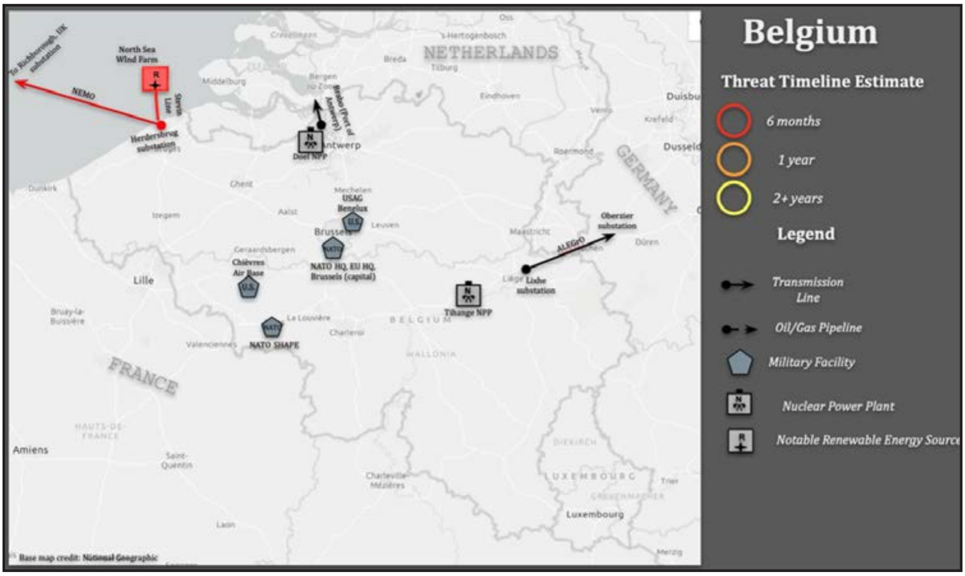

Figure 7-1. Map of Belgium's threat timeline estimate (six months indicates likely attack vector in 2022, one year by 2023, two+ years by 2024 or later)
Credit: Ryan Fisk and Lucas Cox

Location	Reason for Threat Priority and Timeline
North Sea Wind Farm and the Stevin Line	Disinformation attacks and DDoS attacks on wind farm within six months as it becomes a major source of domestic energy production and as it reduces its import of Russian fossil fuels.

Select Bibliography

Apuzzo, Matt, and Monica Pronczuk. "After 2 Years of Paralysis, Belgium Forms a (Very Fragile) Government." *New York Times* (website). October 1, 2020. https://www.nytimes.com/2020/10/01/world/europe/belgium-government-coalition.html.

"Belgian Offshore Platform." Belgian Offshore Platform (website). n.d. https://www.belgianoffshoreplatform.be/en/.

"Country Nuclear Power Profiles, 2019 Edition. Belgium (Updated 2018)." International Atomic Energy Agency (website). n.d. https://www-pub.iaea.org/MTCD/publications/PDF/cnpp2019/countryprofiles/Belgium/Belgium.htm.

Galindo, Gabriela. "Outrage after Car Brandishing Nazi Symbols Joins Vlaams Belang Protest." *Brussels Times* (website). September 28, 2020. https://www.brusselstimes.com/133244/outrage-after-car-brandishing-nazi-symbols-joins-vlaams-belang-protest.

Meeusen, Cecil, Joris Boonen, and Ruth Dassonneville. "The Structure of Prejudice and Its Relation to Party Preferences in Belgium: Flanders and Wallonia Compared." *Journal of the Belgian Association for Psychological Science*. November 2017. https://www.psychologicabelgica.com/article/10.5334/pb.335/.

"Shaping Europe's Digital Future – Cybersecurity: Commission Urges Belgium, Hungary and Romania to Comply with Their Obligations Regarding Operators of Essential Services." European Commission (website). October 30, 2021. https://digital-strategy.ec.europa.eu/en/news/cybersecurity-commission-urges-belgium-hungary-and-romania-comply-their-obligations-regarding.

— 8 —

Germany

Sarah J. Lohmann and Christopher Clyde

ABSTRACT: Germany has pledged to become energy independent by 2050 by supporting renewable energy sources. Despite this pledge, until now, Germany has imported the majority of its energy from foreign sources, especially Russia. As experts predicted, Germany has now made itself dependent on an unreliable energy partner, driving up oil and gas prices and creating energy insecurity in the country. In addition, the grid and new energy sources such as wind farms have been exploited through cyberattacks. Germany has produced multiple proactive policies governing cyber threat mitigation to include research into early warning systems and the formation of a new branch of the military directed specifically at securing cyberspace. Its cybersecurity for critical energy infrastructure, however, has not been significant enough to thwart significant cyberattacks by Russia.

Keywords: Nord Stream II, industrial control systems/ICS, cyberattacks, Russian pipeline, energy independence, renewable energy, early warning, Ukraine

Introduction

While the invasion of Ukraine has left most NATO nations unified in that member states want to wean themselves off Russian oil and gas sooner rather than later, the renewable technology that could serve as an energy substitute in the nation paying the most for Russian energy is too underdeveloped to solve the problem in the next two years. Instead, Germany has increased its coal usage since Russia's invasion of Ukraine, and it has increased the amount it has paid for Russian gas.[1] While commitments to accelerate the development of renewable technologies such as wind and solar are laudable, malicious actors are already taking advantage of their cyber vulnerabilities to create greater energy insecurities associated with the emerging technologies.[2]

Germany is Europe's economic powerhouse and the largest importer of Russian gas in the first months of the war.[3] At the same time, Germany is a major distributor of Russian gas to other NATO countries. But attempts to divide Germany from its NATO allies around issues such as the certification of the now-bankrupt Nord Stream 2 gas pipeline, which planned to deliver gas from Russia to Germany without transiting Ukraine were part of the broader Russian hybrid warfare.[4] Using the pipeline as a bargaining chip to escalate conflict with Ukraine, Moscow has manipulated Europe's energy dependencies in its favor—to silence dissent and to inflict economic and political costs on those who do not.

A German embargo on Russian energy imports or a Russian cessation of delivery will have lasting impact on Germany and Europe, as Germany is the European Union's (EU) leading economic power. The Bundesbank warned on April 22 that a gas embargo alone would thrust Germany into a recession and cause the GDP to shrink by 2 percent.[5] Goldman Sachs estimated that if Russia stopped all pipeline exports to Europe, the continent would see a 2.2 percent decrease in GDP, and Germany a 3.4 percent decrease.[6]

Note: Research from this chapter was published in altered form by the author in: Sarah Lohmann, "Russian Gas, Green Technology, and the Great Sacrifice," *Georgetown Journal of International Affairs* (website), June 23, 2022, https://gjia.georgetown.edu/2022/06/23/russian-gas-green-technology-and-the-great-sacrifice%EF%BF%BC/.

1. Morgan Meaker, "Coal Threatens a Comeback as the EU Pulls Away from Russian Oil," Wired (website), March 17, 2022, https://www.wired.com/story/green-transition-russia-ukraine/.

2. Catherine Stupp, "European Wind-Energy Sector Hit in Wave of Hacks," *Wall Street Journal* (website), April 25, 2022, https://www.wsj.com/articles/european-wind-energy-sector-hit-in-wave-of-hacks-11650879000/.

3. Dipaneeta Das, "Germany the Top Buyer of Russian Gas at $9.5 Billion Since War Began in Ukraine," *Republic World* (website), April 28, 2022, https://www.republicworld.com/world-news/europe/germany-the-top-buyer-of-russian-gas-worth-9-dot-5bn-since-war-began-in-ukraine-report-articleshow.html.

4. Zoe Strozewski, "Nord Stream 2 Pipeline Owner Files for Bankruptcy, Releases Workforce," *Newsweek* (website), March 1, 2022, https://www.newsweek.com/nord-stream-2-pipeline-owner-files-bankruptcy-releases-workforce-1683820.

5. Phillip Olterman, "Ban on Russian Gas Would Plunge Germany into Recession, Warns Bundesbank," *Guardian* (website), April 22, 2022, https://www.theguardian.com/business/2022/apr/22/russian-gas-ban-germany-recession-bundesbank.

6. Elliot Smith, "Goldman Predicts What Will Happen to Europe's Economy if Putin Shuts off the Gas Taps," *CNBC* (website), March 11, 2022, https://www.cnbc.com/2022/03/11/goldman-predicts-what-will-happen-to-europes-economy-if-putin-shuts-off-gas.html.

As of this writing, around half of Germany's gas and hard coal imports and one-third of its oil imports are from Russia, meaning Germany relies on Russia for one-third of its total energy consumption.[7] As part of its green transition, Germany planned to close its last nuclear power plant this year and shut down another 6.4 gigawatts of coal capacity by 2023.[8] The green transition is part of the German government program Energiewende, which provides specific, measurable energy benchmarks through 2050.[9] Compared with a base year of 1990, German government emission targets are 40 percent cut in greenhouse gas emissions by 2020, 65 percent by 2030, 88 percent by 2040, and net neutrality by 2045.[10] These goals, however, mean that even before the Ukraine crisis, Germany was facing an energy shortage as it worked toward the discontinuation of coal and nuclear usage. Even before it vowed to wean itself off Russian imports, the nuclear discontinuation alone meant Germany would face a shortage of 4.5 gigawatts of energy between 2022 and 2025.[11]

Although renewables, that is, sources of energy not depleted by use, such as water, wind, or solar power, provide 16 percent of Germany's energy demand, they cannot quickly fill the more than 30 percent gap in energy supply left by turning off the nuclear reactors and suspending Russian energy imports.[12] In addition, Germany's renewable energy sector has been vulnerable to cyberattacks since the invasion of Ukraine. Any attacks on Germany's critical infrastructure and economy are thus being felt much more deeply across the Alliance. Most recently, as mentioned in the introduction to this book, 11 gigawatts of German wind power generation

7. Rüdiger Bachmann et al., "What If? The Economic Effects for Germany of a Stop of Energy Imports from Russia," EconTribute, Policy Brief no. 028, March 7, 2022, https://www.econtribute.de/RePEc/ajk/ajkpbs/ECONtribute_PB_028_2022.pdf.

8. "Kraftwerksliste," Bundesnetzgentur (website), May 31, 2022, https://www.bundesnetzagentur.de/DE/Fachthemen/ElektrizitaetundGas/Versorgungssicherheit/Erzeugungskapazitaeten/Kraftwerksliste/start.html.

9. Thomas Klaus et al., *2050: 100% – Energy Target 2050: 100% Renewable Electricity Supply* (Dessau-Roßlau, DE: Umweltbundesamt, July 2010), https://www.umweltbundesamt.de/sites/default/files/medien/378/publikationen/energieziel_2050_kurz.pdf.

10. Zahi Badra, "Germany Announces 65% Emissions Reduction by 2030 and Climate Neutrality by 2050," Climate Scorecard (website), July 9, 2021, https://climatescorecard.org; and "German Position on the Fit for 55 Package," Bundesregierung (website), May 27, 2021, https://www.bundesregierung.de.

11. Markus Wacket, "Germany's Energy Drive Criticized over Expense, Risk," Reuters (website), March 30, 2021, https://www.reuters.com/article/germany-energy-audit-idUSL8N2LS2RC.

12. Bachman et al. "What If?"

was paralyzed by a failure in satellite communication systems in February 2022, which has been attributed to a Russian cyberattack.[13]

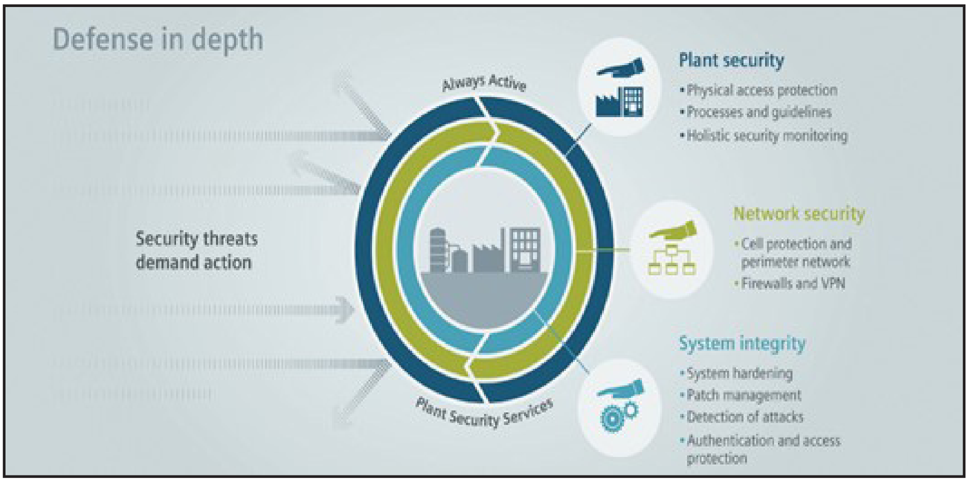

Figure 8-1. Defense-in-depth for ICS networks and the OT systems those networks support, with the Siemens SNOK IDS solution providing an early warning system for detecting attacks to strengthen system integrity[14]

In addition, on April 12, another cyberattack against German wind-energy company Deutsche Windtechnik caused the company to shut down the remote-control systems of 2,000 wind turbines for a day.[15] The pro-Russian government ransomware group Conti launched a cyberattack against another turbine maker, Nordex SE, and forced the company to shut down its IT systems.[16]

Cyberattacks on Germany's critical energy infrastructure are not new. In the past, these have also included attacks on Germany's industrial control systems. From a cyber intrusion at a German steel mill in 2014 to cyber surveillance gathering activities on German electric grid operators beginning

13. Marian Willhun, "Satellite Cyber Attack Paralyzes 11GW of German Wind Turbines," *PV Magazine* (website), March 1, 2022, https://www.pv-magazine.com/2022/03/01/satellite-cyberattack-paralyzes-11gw-of-german-wind-turbines/; and Joseph Henry, "Europe Cyberattack Results to Massive Internet Outage; About 5,800 Wind Turbines Went Offline," Tech Times (website), March 5, 2022, https://www-techtimes-com.cdn.ampproject.org/c/s/www.techtimes.com/amp/articles/272624/20220305/europe-cyberattack-results-massive-internet-outage-5-800-wind-turbines.htm.

14. Davinder Harcharan, Siv Hilde Houmb, and Erlend A. Engum, *How to Safeguard Sophisticated Operational Technology for Targeted, Highly Dangerous Cyber Threats*, white paper (Norcross, GA: Siemens, 2018), https://assets.new.siemens.com/siemens/assets/api/uuid:be9b0c7d-2afa-463a-bb31-fd53ba7525f9/snok-white-paper.pdf.

15. Stupp, "European Wind Energy."

16. Stupp, "European Wind Energy."

in 2017, malign actors continue to test Germany's cybersecurity weaknesses while evading detection.

What Solutions Are There?

Improve Cyber Early Warning

Early warning systems (EWS) of the future must protect sophisticated next-generation networks, develop models for behavioral analysis and learning algorithms, and define normal behavior patterns and anomalies.[17] Siemens/Secure-NOK® SNOK® Network Anomaly Detection solution, or simply SNOK, is a digital early warning system designed to detect cyber intrusions. It uses software to identify anomalous behavior patterns in the network to disrupt an attack before it occurs. The EWS targets suspicious activity to detect threats from anomalies in parameters to unusual CPU usage. SNOK then alerts a compromised ICS network's operators to the attack and provides data to inform a countermeasure decision. The program analyzes attack patterns through machine learning and then provides a counter before the interruption becomes a threat.[18]

The National Cybersecurity Centre of Excellence (NCCoE) Engineering Laboratory, partnered in the "Capability Assessment for Securing ICS" assessed SNOK capabilities.[19] The NCCoE assessed that 15 different behavior anomaly detection (BAD) categories and anomaly scenarios were successfully detected, demonstrating that BAD techniques can serve as a critical element for securing and sustaining ICS operations. NCCoE likewise assessed SilentDefense, CyberX, and OSIsoft Early Warning Systems using up to 16 differing BAD categories and anomaly scenarios that produced similarly successful results to SNOK.[20] The increasing importance and challenges of EWS cannot be understated, considering the billions of devices, vast amounts of data, and virtualization of services. Cybercriminals conduct digital reconnaissance to find and exploit network and infrastructure vulnerabilities and challenge

17. Mario Golling and Björn Stelte, "Requirements for a Future EWS-Cyber Defence in the Internet of the Future," *Proceedings of 3rd International Conference on Cyber Conflict* (*ICCC*) (Tallinn, EE: ICCC, 2017), https://www.researchgate.net/publication/229034186_Requirements_for_a_future_EWS-Cyber_Defence_in_the_internet_of_the_future.

18. Siv Hilde Houmb, "Secure-NOK: Unprecedented Industrial Cybersecurity Monitoring," CioReview (website), 2020, https://cybersecurity.cioreview.com/vendor/2017/secure-nok#.

19. Houmb, "Secure-NOK."

20. James McCarthy et al., *Securing Manufacturing Control Systems: Behavioral Anomaly Detection*, NISTIR Report 8219 (Washington, DC: US Department of Commerce/National Institute of Standards and Technology, July 2020), https://doi.org/10.6028/NIST.IR.8219.

traditional intrusion detection protocols. Further, the ability to correlate data to a threat, find the intrusion source, and the computer forensic capabilities of a government or corporation often limit cyber defense professionals' ability to protect or offer a response option.[21]

The project Early Warning and Intrusion Detection System Based on Combined AI Methods (FIDeS), Event Monitoring Enabling Responses to Anomalous Live Disturbances (EMERALD), ARAKIS, and the Worldwide Observatory of Malicious Behaviors and Attack Threats (WOMBAT) are all early warning and intrusion detection software based on combined AI methods used in Germany.[22] These methods are defined further in chapter 4. Table 8-1 illustrates an overview of EWS requirements and how each system is equally challenged to meet cyber defense requirements. The relationship and dependency between formerly stand-alone systems and networks create complexities not yet experienced, and therefore developing appropriate EWS to counter each complexity has become increasingly difficult.

As stated in chapter 4, these challenges can be countered with a new generation of infrastructure modeling and virtualization while combining artificial intelligence and machine learning to ensure the cyber mitigation method is specific to the type of energy infrastructure and that new types of attacks are repelled before they do damage.

21. Golling and Stelte, "Future EWS-Cyber Defence."

22. Golling and Stelte, "Future EWS-Cyber Defence."

Table 8-1. Capabilities of state-of-the-art EWS technologies
Source: Golling and Stelte, "Future EWS-Cyber Defence."

Requirements	FIDeS	EMERALD	ARAKIS	WOMBAT
Extended flow handling				
Sophisticated correlation of data	X	X		X
Comprehensive reasoning model				
Traffic volume independency	X	X	X	X
End-system independency	X	X	X	X
Payload-independent analysis				
Safeguarding mobile devices				
Virtualized environment/clouds				
Spontaneous network behavior				

As cyber intrusions evolve, becoming more sophisticated, the difficulty in protecting digitized critical infrastructure increases. Infrastructure must operate 24 hours a day, sevendays a week, without disruption. Digital infrastructure protection will require agile and responsive early warning systems embedded with defense-in-depth capabilities to monitor and detect network intrusions adequately and react to threats in near real time before the attack occurs. Effectively monitoring and detecting cyber intrusions via layered, in-depth defenses provides cyber defense professionals the requisite time and awareness to assess risk and develop potential response options.

Improve Non-hackable Energy Independence

Germany's state-of-the-art nuclear reactors, which provided 13 percent of Germany's electricity last year, already exist.[23] While no one has suggested extending the controversial nuclear reactors' operations to be a permanent solution, Germany's Free Democrats have proposed reactivating nuclear for the short term. This is tricky as it will require a new legislative mandate, and new fuel rods.[24] The Greens, who are part of the ruling coalition, are still

23. Kate Connolly, "Can Germany Function without Vladimir Putin's Gas?" *Guardian* (website), February 25, 2022, https://www.theguardian.com/world/2022/feb/25/can-germany-function-without-vladimir-putins-gas.

24. Claus Hecking et al., "Germany's Alternatives to Putin's Gas," *Spiegel International* (website), March 9, 2022, https://www.spiegel.de/international/business/lng-imports-and-nuclear-power-a-look-at-germany-s-alternatives-to-putin-s-gas-a-4e10b1fd-0828-4a0a-9183-f2fd38d4dfe1.

averse to the idea, though reviving nuclear would provide an emissions-free domestic solution. Another immediate solution is to expand the use of biogas, which today could immediately replace 5 percent of Russian gas imports.[25]

While the German government aims to increase renewables, renewable power companies, especially those responsible for wind and updating grids, are skeptical that they can produce at the speed the government is asking of them.[26] Licensing challenges, supply-chain issues, and a lack of workers hinder an accelerated increase in renewables.

On April 7, the government rolled out the "biggest energy policy reform in decades," which plans for the country to move to a 100 percent renewable power supply by 2035.[27] To make this utopian vision a reality, Germany will need to provide incentives for the education of personnel in the renewables field, cut down its famous bureaucracy around licensing, update its grid networks, and ensure more domestic supply of renewable technology parts.

Today, the war in Ukraine rages as Germany continues to pump funds into Moscow's war chest, paying them $9.5 billion for gas since the start of the war.[28] By comparison, Russia has earned $66.5 million in gas revenue total since the war began with 71 percent coming from the European Union.[29] In the short term, it may be time to consider nuclear energy and biogas as immediate options to bolster Germany's energy independence.[30] This could also allow the country time to develop renewables and the ability to defund Moscow's war efforts.

25. Benjamin Wehrmann, "Q&A: How Can Renewables Enable Germany's Energy Independence Push?," Clean Energy Wire (website), April 12, 2022, https://www.cleanenergywire.org/news/qa-how-can-renewables-enable-germanys-energy-independence-push.

26. Wehrmann, "Q&A."

27. Wehrmann, "Q&A."

28. Dipaneeta Das, "Germany the Top Buyer of Russian Gas Worth $9.5bn since War Began in Ukraine: Report," *Republic World* (website), April 28, 2022, https://www.republicworld.com/world-news/europe/germany-the-top-buyer-of-russian-gas-worth-9-dot-5bn-since-war-began-in-ukraine-report-articleshow.html.

29. Das, "Top Buyer of Russian Gas"; and *Express Tribune* staff, "Russia in Receipt of $63B for Fossil Fuels since Start of War," Coverpage (website), April 28, 2022, https://coverpage.org/russia-in-receipt-of-63b-for-fossil-fuels-since-start-of-war/.

30. Wehrmann, "Q&A."

Conclusion

If the German government continues to import Russian energy, it will need to be honest with its public about what protracted dependence on Russia will mean not just for the Ukraine, but for Europe's security as an adversary moves its territorial boundaries closer to NATO's Eastern flank. Cyberattacks on Germany's critical energy infrastructure will continue and will likely increase on its emerging technology in the near future until a new generation of cyber early warning systems are developed. Malign influence campaigns, now already affecting Germany's gas market, will affect Germany's gas and oil until Germany becomes more energy independent. In the meantime, Germany's public should be informed about what a more than 30 percent reduction in supply will mean for private households, German industry, and the EU economy. This reduction is likely to be felt in the homes and businesses of citizens from Berlin to Riga for years to come.

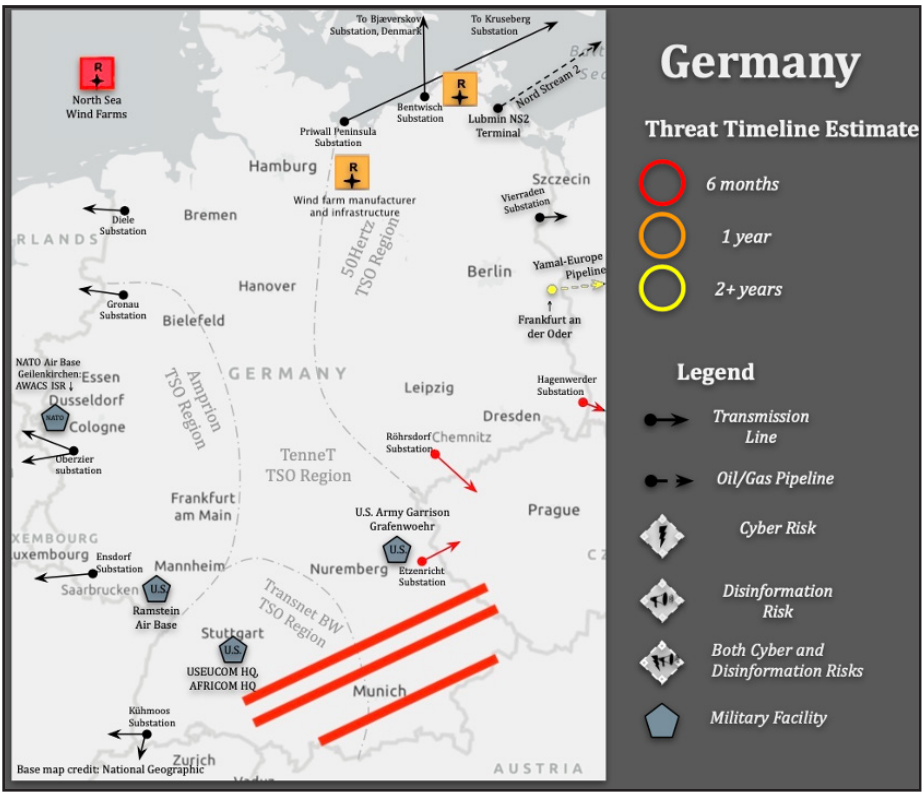

Figure 8-2. Map of Germany's threat timeline estimate (six months indicates likely attack vector in 2022, one year by 2023, two+ years by 2024 or later)
Credit: Ryan Fisk and Lucas Cox

Location	Reason for threat priority and timeline
North Sea Wind Farms	Germany's wind farms have been a Russian target in the first months of the war. Expect continued disinformation campaigns and cyberattacks on the remote-control systems of wind turbines for the next six months due to Russia's goal of undermining Germany's sources of energy as it reduces its import of Russian fossil fuels.
Southern Germany Grid Instability	During the energy transition, the power supply to the southern part of Germany—in the Transnet BW region and part of the TenneT region—is not reliable due to unpredictable wind and solar, and an aging grid that is vulnerable to cyberattack. Occasional blackouts are to be expected to start in 2022.
Wind Farm Infrastructure	ICS attacks within one year, as manufacturer Enercon has already had its KA-SAT communications system attacked and as wind energy becomes increasingly important for Germany's energy independence.
Yamal-Europe Pipeline	Russia has repeatedly halted gas flows through the Polish segment of the pipeline, which is partially owned and operated by Gazprom, and the flow has been reversed to deliver fuel to Poland. The eastbound gas flow also stopped July 5, 2022. Should the gas flow be reactivated, it will remain vulnerable to Russian retaliation via disinformation and the supply chain due to its importance and control by Gazprom.

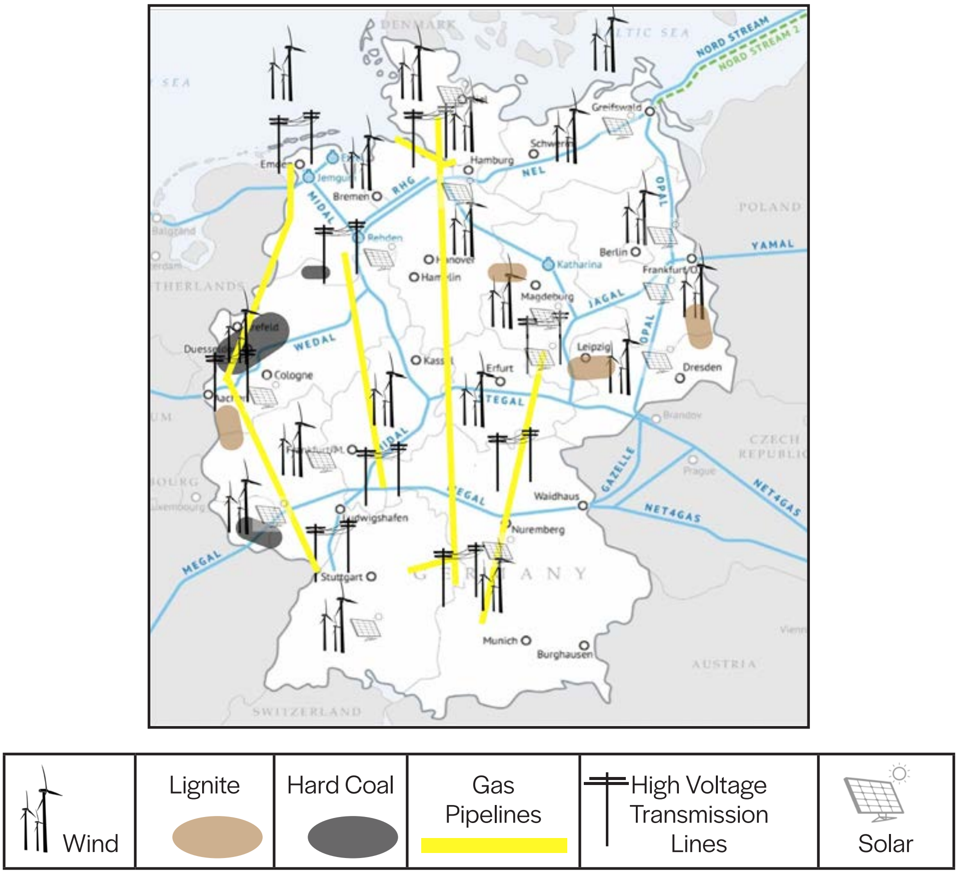

Figure 8-3. Germany's energy sources
Image Source: GazProm, https://www.gazprom.com/projects/germany/;
original source: Colonel Chris Clyde

Select Bibliography

Golling, Mario, and Björn Stelte. "Requirements for a Future EWS-Cyber Defence in the Internet of the Future." *Proceedings of 3rd International Conference on Cyber Conflict* (*ICCC*). Tallinn, EE: ICCC, 2017. https://www.researchgate.net/publication/229034186_Requirements_for_a_future_EWS-Cyber_Defence_in_the_internet_of_the_future.

Harcharan, Davinder, Siv Hilde Houmb, and Erlend A. Engum. *How to Safeguard Sophisticated Operational Technology for Targeted, Highly Dangerous Cyber Threats*. White paper. Norcross, GA: Siemens, 2018. https://assets.new.siemens.com/siemens/assets/api/uuid:be9b0c7d-2afa-463a-bb31-fd53ba7525f9/snok-white-paper.pdf.

Hecking, Claus et al. "Germany's Alternatives to Putin's Gas." *Spiegel International* (website). March 9, 2022. https://www.spiegel.de/international/business/lng-imports-and-nuclear-power-a-look-at-germany-s-alternatives-to-putin-s-gas-a-4e10b1fd-0828-4a0a-9183-f2fd38d4dfe1.

Houmb, Siv Hilde. "Secure-NOK: Unprecedented Industrial Cybersecurity Monitoring." CioReview (website). 2020. https://cybersecurity.cioreview.com/vendor/2017/secure-nok#.

Klaus, Thomas et al. *2050: 100% – Energy Target 2050: 100% Renewable Electricity Supply*. Dessau-Roßlau, DE: Umweltbundesamt, July 2010. https://www.umweltbundesamt.de/sites/default/files/medien/378/publikationen/energieziel_2050_kurz.pdf.

"Kraftwerksliste." Bundesnetzgentur (website). May 31, 2022. https://www.bundesnetzagentur.de/DE/Fachthemen/ElektrizitaetundGas/Versorgungssicherheit/Erzeugungskapazitaeten/Kraftwerksliste/start.html.

McCarthy, James et al. *Securing Manufacturing Control Systems: Behavioral Anomaly Detection*. NISTIR Report 8219. Washington, DC: US Department of Commerce/National Institute of Standards and Technology, July 2020. https://doi.org/10.6028/NIST.IR.8219.

Stupp, Catherine. "European Wind-Energy Sector Hit in Wave of Hacks." *Wall Street Journal* (website). https://www.wsj.com/articles/european-wind-energy-sector-hit-in-wave-of-hacks-11650879000.

— 9 —

Netherlands

Brenton M. Riddle

ABSTRACT: Despite measures taken in recent years to adopt renewable energy sources, the Netherlands remains a net energy importer, reliant on foreign pipelines for the bulk of its power. This net energy deficit is a major problem, coupled with a rising concern over the speed of green energy infrastructure adoption, which is potentially outpacing the ability to secure said infrastructure. The Netherlands has devoted resources toward smart grid and Internet of Things adoption. Overall, the Netherlands is cyber hardened, devoting resources to advancing and securing its cyber systems and staying competitive in guarding against cyberattacks.

Keywords: sea port security, renewable energy security, Amsterdam Internet Exchange, Groningen gas field, smart grid, TenneT

Introduction

The Netherlands is well-positioned to be a leader at the energy-hybrid warfare nexus. Since the turn of the decade, the Netherlands has increasingly utilized innovative technologies within its critical infrastructure systems, including smart grids, the Internet of Things (IoT), and renewable energy power generation. In a model of asymmetric cyberwarfare, these new technologies, brought on by a commitment to decarbonizing state and civil operations, become vulnerabilities to critical energy infrastructure (CEI). For this case study, CEI encompasses the processes of energy generation, transmission, distribution, and consumption. Targeting critical infrastructures with cyberattacks is a low-cost, high-yield effort for malign actors to disrupt and destabilize civilian lives and entire nations.

In a world of increasing interconnectedness, improving cybersecurity of infrastructure is essential to ensuring national security and avoiding possible cascading effects in critical sectors across the region, including health care, water management, and military operations. In this changing and interdependent world, the Netherlands is a gateway between the international community and the European Union. Schiphol Airport is one of the busiest airports for international passengers and cargo in the European Union; outside Asia, the port of Rotterdam is the largest seaport in the world, and the Amsterdam Internet Exchange (AMS-IX) is the world's largest Internet exchange in connected peers and third-largest in daily traffic.[1]

With its neighbors, the Netherlands shares extensive cross-border and subsea oil and gas pipelines and electrical connections.[2] Fortunately, the Netherlands and its historic commitment to cybersecurity, resilience, and crisis management has positioned it well to address the heightened threats associated with an electrifying, digitizing, and connected world. Geopolitically, the primary challenge to efficient, secure, and affordable energy in the Netherlands is the 2022 phaseout of the Groningen gas field, the largest gas field in Europe and the 10th-largest in the world. The 2018 decision to phaseout resulted in the Netherlands becoming a net importer of natural gas for the first time in several decades. Beyond this, the looming threat to Dutch energy security is one from cyberspace. The Netherlands belongs to most countries in the international community, which have a rate of embedding information and communication technology (ICT) into CEI that far outpaces the adoption of risk mitigation safeguards and adapted security protocols.

The operation of the electrical grid and the integration of smart-grid technology are the emerging technologies that require the most attention in order to future-proof Dutch critical energy infrastructure. This case study provides context for the Dutch cyber and energy landscapes and makes recommendations toward developing a NCSC toolkit for critical energy infrastructure operators, relying on IT/OT engineers' expertise, and gaining NCSC-sponsored awareness for certification.

1. Melissa Hathaway and Francesca Spidalieri, "The Netherlands: Cyber Readiness at a Glance," Potomac Institute (website), May 2017, https://potomacinstitute.org/images/CRI/FinalCRI20NetherlandsWeb.pdf.

2. "The Netherlands 2020 – Energy Policy Review," International Energy Agency (website), September 2020, https://www.iea.org/reports/the-netherlands-2020.

Dutch Energy Mix

At present, the Dutch energy mix is dominated by fossil fuels. As of 2019, natural gas held the largest share of the Dutch total primary energy supply (TES) at 45 percent, followed by oil (36 percent) and coal (9 percent).[3] Only minor shares (8 percent) of the Dutch total energy supply come from renewable energy and carbon-neutral sources, including solar, wind, and biowaste.

In December 2019, the Netherlands passed the 2019 Climate Act, which reimagined the Dutch energy market, existing energy infrastructure, and overall greenhouse gas (GHG) emissions to be in line with international objectives, of which it was falling behind.[4] The act sets out an ambitious goal of achieving a 49 percent reduction of GHG emissions (based on 1990 levels) by 2030 and 95 percent by 2050.[5] Using the collaborative Dutch polder model—a consensus-based method of economic and social policy making—and drawing together 100+ stakeholders, a coalition of Dutch policymakers and business leaders created a framework for reaching Climate Act objectives titled the 2019 Climate Agreement. This intranational agreement contained emission reduction targets and measures for five sectors: electricity, industry, the built environment, mobility, and the natural environment.[6] The 2019 Climate Act and Agreement are the most recent energy policies passed in the Netherlands.

Also in December 2019, the Netherlands passed a separate law phasing out coal-fired power generation by January 1, 2029.[7] Additional phaseout projects are also occurring in nuclear and natural gas. A full phaseout of the sole Dutch nuclear generator—the 485-megawatt Borselle plant generating 3.5 percent of Dutch total energy supply (TES)—is expected by 2033.[8] Furthermore, regional earthquakes in 2018 and 2019 caused by excessive drilling inspired the Dutch government to strategize a phaseout of the Groningen gas field by 2022. The Groningen gas field produces a chemical variety, known as L-gas, which is different from most commercially available gas in the international market (H-gas). As a result, the Netherlands has two LNG pipeline systems throughout the country.

3. "Netherlands 2020 – Energy Policy Review."
4. "Netherlands 2020 – Energy Policy Review."
5. "Netherlands 2020 – Energy Policy Review."
6. "Netherlands 2020 – Energy Policy Review."
7. "Netherlands 2020 – Energy Policy Review."
8. "Netherlands 2020 – Energy Policy Review."

Despite this, until the low-carbon transition is complete, natural gas is expected to remain the primary Dutch energy source because it remains favorable over dirtier petroleum products and has existing infrastructure.

The 2019 Climate Act set an objective of 100 percent CO_2-free electricity generation by 2050. Accordingly, the Netherlands is transitioning to electricity generation with wind, solar, and biomass projects, most of which are subsidized by the government's stimulation of sustainable energy production and climate transition funding schemes.[9] Under the Climate Agreement, intermittent renewable energy sources (IRES), those that are stochastic and associated with variable weather, are expected to increase from 12 percent in 2018 to nearly 70 percent by 2030. Beyond solar and wind, the use of biomass—making up 61 percent of all renewable energy—and waste electrical power generation is expected to increase in share as well .[10]

Geopolitical and Cyber Concerns

As a result of rapid investment in renewable energy production and the phasing out of natural gas and other fossil fuels in the Dutch energy mix, the Netherlands faces several distinct energy security vulnerabilities. Now, as a net importer of natural gas because of the ongoing phaseout of Groningen, the Netherlands was relying on Norway, Russia, Germany, and the United Kingdom to meet its gas demands.[11] This presents geopolitical challenges and leaves the nation reliant on other countries for its energy needs. This challenge has only escalated in the wake of the Ukraine invasion, with Russia cutting off gas to the Netherlands because it refused to pay in rubles.[12] Furthermore, the transition to renewable energy production as the dominant energy source brings additional vulnerabilities. The stochastic nature of renewable energy sources can, in various weather conditions, lead to scarcity and grid imbalances across the nation, impacting energy

9. Sophie Dingenen, "Electricity Regulation in the Netherlands," Lexology (website), November 6, 2018, https://www.lexology.com/library/detail.aspx?g=d3b6b42e-fd53-42d0-aba9-9727f6026093.

10. "Netherlands – Energy," Privacy Shield Framework (website), n.d., https://www.privacyshield.gov/article?id=Netherlands-Energy.

11. "Netherlands 2020 – Energy Policy Review"; and Assia Elgouacem and Peter Journeay-Kaler, *The Netherlands' Effort to Phase Out and Rationalise Its Fossil-Fuel Subsidies* (Paris: Organisation for Economic Co-operation/International Energy Agency, September 2020), 43, https://www.iea.org/reports/the-netherlands-effort-to-phase-out-and-rationalise-its-fossil-fuel-subsidies.

12. Anna Cooban, "Russia Is about to Shut Off Some of Germany's Gas," *CNN* (website), May 31, 2022, https://www.cnn.com/2022/05/31/energy/russia-shell-germany-gas-shut-off/index.html.

security.[13] These transitions also create cyber-specific vulnerabilities within the nation's energy infrastructure:

- **Malicious intrusions**. As demand for and reliance on electricity increases, so too does the potential for malign actors to infiltrate the Dutch electrical grid. Furthermore, as the grid becomes increasingly digitized, adopts modern renewable energy production facilities online, and manages the grid via ICS/SCADA management software, additional vulnerabilities arise for malign actors to exploit.
- **Smart-grid and IoT vulnerabilities**. A part of digitization includes additional investments in end-user and monitoring technology to enhance the nation's smart grid. Relying on IoT technology, new interconnected points of intrusion are introduced into the electrical grid, allowing malign actors to disrupt CEI nationwide from a single local access point. For example, a recent cyber intrusion into the oil facilities in the Amsterdam-Rotterdam-Antwerp (ARA) trading hub has demonstrated the vulnerabilities of an integrated cross-border IT network.[14]

Emerging Technology

The Netherlands' electricity grid is divided into high-voltage (>110 kilovolt [kV]) transmission, operated by TenneT, the sole transmission system operator (TSO) in the Netherlands, and low-voltage transmission, operated by seven regional distribution system operators (DSOs).[15] While the high-voltage grid connects energy producers to the grid and manages international grid-to-grid transmission, low-voltage DSOs connect the grid to individual households and businesses. "The [Dutch] transmission system has over 22,500 kilometers of lines operated at 110 kV, 150kV, 220kV, and 380kV; more than 450 substations; nine cross-border interconnectors; and a rapidly expanding offshore grid."[16]

13. Dingenen, "Electricity Regulation."

14. "Belgium Investigates Cyberattack on Energy Companies," DW (website), February 3, 2022, https://www.dw.com/en/belgium-investigates-cyberattack-on-energy-companies/a-60651892.

15. Dingenen, "Electricity Regulation."

16. "Netherlands 2020 – Energy Policy Review."

Both TSOs and DSOs are under government regulation as a result of their designation as Operators of Essential Services (OES).[17] The Electricity Act of 1998 establishes the duties of TSOs and DSOs while the Dutch Unbundling Act prohibits both from owning subsidiaries that operate or sell electricity to the grid.[18] These ensure that TSOs and DSOs focus on protecting the security of the physical electrical infrastructure while 25 electricity producers and 35 electricity retailers in the Dutch electrical energy landscape focus on meeting the nation's electricity needs.[19]

The Netherlands shares land and/or sea electrical grid connections with Belgian, British, Danish, German, and Norwegian transmission grids.[20] BritNED, NorNED, and COBRA electrical sea cables connect the Netherlands to the United Kingdom, Norway, and Denmark, respectively.[21]

Germany is the largest electricity trading partner of the Netherlands and was planning on phasing out nuclear and coal production in favor of renewables. From 2019 to 2025, cross-border interconnector capacity is expected to grow from 7.05 gigawatts to 10.8 gigawatts through the construction of additional cross-sea cables and overhead lines.[22]

The Netherlands has renewable energy targets to meet in 2023, 2030, and 2050. In 2018, amongst International Energy Agency (IEA) member countries, the Netherlands was ranked as one of the countries with the lowest share of total final energy consumption (TFEC) coming from renewables. Looking at TFEC, renewable energy has historically addressed demand in the electricity, heat, and transport sectors. The Dutch transport sector remains dominated by fossil fuels, however, the nation is quickly building its electric vehicle (EV) infrastructure. The current goal is to have 1.7 million charging points across the country by 2030.[23] A major obstacle to renewable energy expansion in the Netherlands is that large-scale solar and wind projects are hard to implement in a populous nation.

17. Irene Kamara et al., *The Cybersecurity Certification Landscape in the Netherlands after the Union Cybersecurity Act*, Final Report (Tilburg, NL: National Cyber Security Centre of the Netherlands/Tilburg Institute for Law, Technology, and Society, July 2020), https://www.ncsc.nl/binaries/ncsc/documenten/rapporten/2020/oktober/2/the-cybersecurity-certification-landscape-in-the-netherlands-after-the-union-cybersecurity-act/NCSC_CYBERCERT_FinalReport__20200730.pdf.

18. Kamara et al., *Cybersecurity Certification*.

19. "Netherlands – Energy."

20. Dingenen, "Electricity Regulation in the Netherlands."

21. Dingenen, "Electricity Regulation in the Netherlands."

22. "Netherlands 2020 – Energy Policy Review."

23. "Netherlands 2020 – Energy Policy Review."

As a result, TenneT has projected an eight billion euro infrastructure expenditure to provide subsidies to municipalities that initiate residential photovoltaic (PV) projects and expand offshore grid connections in line with the Dutch government's Offshore Wind Roadmap.[24] By 2030, it is expected that 70 percent of Dutch electricity generation will come from renewables.[25]

The International Energy Agency provides a breakdown of how energy is currently utilized across the country: in 2018, total electricity demand was 114.0 terawatt hours. The services/other sector was the largest consumer (41 percent), followed by industry (32 percent), driven by chemical and petrochemical demand. The remainder of demand came from the residential (20 percent), energy (5 percent), and transport (2 percent) sectors. Transport demand came from electrified rail (76 percent) and electric road transport (24 percent).[26] Estimates from the Central Bureau of Statistics show that electricity demand reached an all-time high of 121 terrawatt hours in 2019. The Netherlands has an extensive rail network that is almost completely electrified. The country is a global leader in electric vehicle (EV) deployment and EV charging infrastructure, with around 200,000 registered EVs and over 50,000 EV charging stations in 2019.

Smart-grid Technologies

The smart grid is often referred to as a cyber-physical system. Digitization of the electrical grid garners increased attention as a promising method to increase efficiency. The Netherlands has become an incubator for smart-grid technology innovation in the past decade, most notably by creating the Intelligent Grids Innovation Programme, which has supported the work of 94 pilot programs integrating smart-grid technology into residential districts, city centers, and industrial estates across the country.[27] Many of the pilot programs are focused on integrating smart technologies like IoT meters and sensors into (micro)grids to evaluate their impact on efficient energy use, often in conjunction with the implementation of electric vehicle charging ports. Smart management systems and IoT devices make use of open networks to coordinate electrical consumption with local DSOs to create projections

24. "Netherlands 2020 – Energy Policy Review."

25. "Netherlands 2020 – Energy Policy Review."

26. "Netherlands 2020 – Energy Policy Review."

27. Cihan Gerceket et al., "A Comparison of Households' Energy Balance in Residential Smart Grid Pilots in the Netherlands," *Applied Sciences* 9 (15): 2993, July 25, 2019, https://doi.org/10.3390/app9152993.

more accurately, allowing producers to efficiently ramp up or down production according to demand.

Vulnerabilities in the Cyber Landscape

The Netherlands is a technologically advanced nation; nearly 100 percent of households have broadband connection.[28] Furthermore, the Netherlands is a top-10 exporter of ICT, host to the Amsterdam Internet Exchange (AMS-IX), and claims 6 percent of its GDP comes from the Internet economy.[29] This reliance on Internet devices and the electricity that powers them makes Dutch CEI a prime target for malign actors. Furthermore, the rapid digitization of the Netherland's CEI increases cyber vulnerabilities by increasing points of entry and interconnectivity of systems. A 2020 report commissioned by the Dutch government identified critical processes as high-value assets increasingly targeted by malign state actors and cybercriminals.[30]

While this case study focuses on vulnerabilities present in the electrical grid and associated IoT smart-grid technology, additional consideration should also be given to other critical infrastructure in the Netherlands, namely, that of LNG pipelines and Delta Works. Delta Works is a series of water-related construction projects (for example, flood defenses, sluice gates, bridges, and tunnels) that prevent flooding in the Netherlands which has more than 26 percent of its land mass below sea level. The unique situation makes water management a national security concern. Many Delta Works projects are digitally operated and employed during times of sea rise, ocean storms, and flooding. Ensuring the successful operation of such mechanisms, specifically from cyber intrusion, is actively being investigated by the Dutch state.[31]

Natural gas and its associated infrastructure are other prime targets for malign actors deserving of consideration. The Netherlands extensive gas infrastructure consists of "over 200 onshore and offshore production sites,

---

28. "Netherlands – Energy."

29. Melissa Hataway and Francesca Spidalieri, "The Netherlands: Cyber Readiness at a Glance"; and "Netherlands – Energy."

30. National Cyber Security Centre (NCSC), *NCSC Research Agenda 2019–2022* (Hague: NCSC, October 2020), https://english.ncsc.nl/binaries/ncsc-en/documenten/publications/2020/oktober/29/ncsc-research-agenda-2019-2022/200203_NCSC+Onderzoeksagenda+A4+EN+web.pdf.

31. "Digitale dijkverzwaring: cybersecurity en vitale waterwerken Rapport," Algemene Rekenkamer, March 28, 2019, https://www.rekenkamer.nl/publicaties/rapporten/2019/03/28/digitale-dijkverzwaring-cybersecurity-en-vitale-waterwerken.

136,632 kilometers of pipelines, and connections to 95 percent of households, most commercial properties, numerous industrial sites, and gas-fired power plants."[32] Geopolitically, the Netherlands' housing of the Title Transfer Facility (TTF), Europe's largest gas trading hub, reflects its ongoing active participation in LNG and international cooperation for security of supply.[33] Much like the electrical grid, the transition to ICS in LNG systems opens vulnerabilities to be exploited by sophisticated attackers. As seen with the US Colonial Pipeline, defensive posturing measures must be taken at all levels of CEI operation, including accounting systems.[34]

Compromised cybersecurity can result in distributed denial of service (DDoS), ransomware attacks, and theft of end-user information.[35] The 2015 attack on Ukraine's power grid and the temporary shutdown of the US Colonial Pipeline in 2021 reflect the risk posed by grid digitization. A report by the Dutch Scientific Council for Government Policy (WRR) asserts that the adoption of ICT technologies is outpacing the adoption of protective measures in its systems. This same report claimed the Netherlands was insufficiently prepared for cyber incidents, noting the government has centered cyber resilience in their work and let crisis management and cyber disruption preparedness fall to the wayside. This level of unpreparedness was exploited in the ARA attack mentioned above and can be replicated on a larger scale in the future.[36]

Electricity Grid: ICS/SCADA and International Cooperation

Functioning power grids underpin domestic livelihoods, industry, and national operations, making them prime targets for malign foreign actors and requiring state-directed investment in the security of those grids.

32. "Netherlands 2020 – Energy Policy Review."

33. Lucia Van Geuns and Irina Patrahau, "Gas Supply Security in the Netherlands," *HCSS* (blog), March 2, 2021, https://hcss.nl/report/gas-supply-security-in-the-netherlands-geopolitical-and-environmental-dilemmas/.

34. Mike Hoffman and Tom Winston, "Cyber Attack: Recommendations Following the Colonial Pipeline Ransomware Attack," *Dragos* (blog), May 11, 2021, https://www.dragos.com/blog/industry-news/recommendations-following-the-colonial-pipe line-cyberattack/.

35. Tucker Bailey, Adam Maruyama, and Daniel Wallance, "The Energy-Sector Threat: How to Address Cybersecurity Vulnerabilities," McKinsey & Company (website), November 3, 2020, https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-energy-sector-threat-how-to-address-cybersecurity-vulnerabilities.

36. NCSC, *Research Agenda 2019–2022*.

In the Netherlands, distributed denial of service (DDoS) is the largest cyberattack concern, with 919 attacks registered in 2019.[37]

An important distinction in electrical infrastructure is the difference between Information Technology (IT)—software like e-mail, cloud computation, and document sharing—and Operational Technology (OT)—physical infrastructure like monitors, sensors, and screens. A growing concern is the inherent vulnerability associated with the convergence of IT with OT, as most modern industrial power grids (electrical, oil, and gas) are managed using industrial control systems (ICS) and supervisory control and data acquisition (SCADA).[38] Together, they improve the interoperability and control-of-flow capabilities of grid operators, providing real-time data and remote-control functions. The interoperability of ICT and electrical is an example of IT-OT convergence where improving control-flow mechanisms and demand-management has the unintended consequence of increasing the number of entry points for malign actors. The growing concern over this topic comes from the increased accessibility and controllability over previously analog industrial control systems used in the movement of energy resources via the Internet and IP addresses.

The Cybersecurity Assessment of the Netherlands identified EKANS, a ransomware raising red flags in the cyber world, as a pressing concern for which ICS/SCADA systems could be vulnerable, requiring mitigation and security measures.[39] The concern with EKANS is that unlike previous ransomwares, it has the ability to target ICS-essential software specifically, halt vital functions, and encrypt underlying data.[40] The emergence of EKANS reflects the technological savviness of cybercriminals and therefore the need for OESs to develop protective measures.[41]

A 2020 report completed in collaboration with the Hague Security Delta performed a system analysis of all ICS/SCADA in use within the Netherlands—including non-grid uses—and identified several vulnerabilities:

37. NCSC, *Research Agenda 2019–2022*.

38. J. M. Ceron et al., *Online Discoverability and Vulnerabilities of ICS/SCADA Devices in the Netherlands* (Enschede, NL: University of Twente, June 21, 2019), https://ris.utwente.nl/ws/portalfiles/portal/124347608/wodc_report_scada_final.pdf.

39. NCSC, *Research Agenda 2019–2022*.

40. Andy Greenberg, "Mysterious New Ransomware Targets Industrial Control Systems," Wired (website), February 3, 2020, https://www.wired.com/story/ekans-ransomware-industrial-control-systems/.

41. Dragos Inc., "EKANS Ransomware and ICS Operations," *Dragos* (blog), February 3, 2020, https://www.dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/.

- Shodan [a search engine that provides metadata about Internet-connected systems], make[s] it extremely easy for potential attackers to find ICS/SCADA devices. [Scanning tools, like Shodan, are increasingly used by cyber criminals to identify vulnerable entry points.]
- [A]t least [1,000] ICS/SCADA devices in the Netherlands are exposed on the Internet.
- Around [60] of these devices have multiple vulnerabilities with a high security level.
- Several well-known and relatively easy-to-deploy measures exist that help to improve the security of these ICS/SCADA devices.[42]

Vulnerabilities in these systems also occur as a result of coordination challenges between public and private entities as well as transnational system operators. Despite cybersecurity centralization efforts, there still remains a great deal of institutional overlap between several Dutch ministerial bodies overseeing the implementation of cybersecurity measures. The court of audit noted cybersecurity protocols vary amongst ministries and asserted that information security throughout the Dutch central government is still not to standard.

Smart-grid Technologies: Points of Entry, Supply Chain, and Certification

As a cyber vulnerability, IoT devices (smart meters, smart thermostats, energy monitors) are all points of access that increase the overall surface vulnerability of energy systems by putting Internet-enabled, grid-integrated devices in the homes, businesses, and industry operations of end-users.[43] Unmonitored and under-protected, the integration of IoT devices into the energy grid at the producer and consumer present incredible risks to Dutch energy security. Common vectors of attack on the smart grid include advanced persistent threats (APTs), attack trees, phishing, DDoS, malware, and data theft.[44]

42. Ceron et al., *Online Discoverability and Vulnerabilities.*

43. Kamara et al., *Cybersecurity Certification*.

44. Dharmesh Faquir et al., "Cybersecurity in Smart Grids, Challenges and Solutions," *AIMS Electronics and Electrical Engineering* 5, no. 1 (2021): 24–37.

The Dutch Ministry of the Interior and Kingdom Relations (AIVD) and Military Intelligence and Security Service (MIVD) are particularly concerned over the security and supply of new ICTs.[45] A cyberattack on embedded ICT-enabled technology within a grid—which can range in size from end-user sites and DSO-operated substations—can have wide-ranging impacts. Performing security analysis on IoT devices, the Dutch Radio Communications Agency determined that most devices were not at an acceptable level. On their metric, "17 of the 22 devices studied scored between 'mediocre' and 'very poor' when it came to basic security and privacy."[46] The installation of foreign-manufactured, unregulated, and uncertified technologies in CEI presents clear national security risks, giving foreign malign actors unrestrained access to extremely sensitive systems.

This draws into question the regulatory standards and certifications required for grid-integrated technology. Increasingly complex global supply chains force most ICT producers to integrate some type of third-party technology and software, often from foreign companies. Work to mitigate the risks associated with sourcing ICT products, services, and processes is demonstrated in the 2019 Union Cybersecurity Act (CSA), which expands the scope of ENISA and tasks the agency with bolstering an EU-wide ICT certification framework.[47] At present, the Dutch adaptation bill for national implementation remains in draft form. Without it, standards like NTA 8130 for smart meters and ISA99 and IEC62443 for OT-security would be suggestions rather than mandatory for TSOs, DSOs, and suppliers.[48] When passed, the adaptation law is expected to delegate the role of national cybersecurity certification authority to the Radio Communications Agency and create a framework for national accreditation and conformity assessment bodies.[49]

Mitigation and Early Warning Systems

Until recently, the Netherlands maintained a decentralized approach on cybersecurity; individual ministries and organizations were responsible for implementing their own policies and practices. With the adoption

45. Ministry of the Interior and Kingdom Relations, *AIVD Annual Report 2019* (Hague: General Intelligence and Security Service), September 3, 2020, https://english.aivd.nl/publications/annual-report/2020/09/03/aivd-annual-report-2019.

46. NCSC, *Research Agenda 2019–2022*.

47. Kamara et al., *Cybersecurity Certification*.

48. Kamara et al., *Cybersecurity Certification*.

49. Kamara et al., *Cybersecurity Certification*.

of Network and Information Systems (Security) Act (WBNI), the National Cybersecurity Centre (NCSC-NL) and Cybersecurity Incident Response Team (CSIRT-DSP) are now given centralized responsibility over cybersecurity and acting as the single point of contact for cyber incidents and information-pooling in the Netherlands. In addition to its operational roles, the NCSC is responsible for setting the government-funded research agenda in the cyber realm. This has resulted in close partnerships with research organizations. Research out of The Hague Security Delta (HSD) and the Dutch Scientific Council for Government Policy (WRR) cover all topics including ICS/SCADA vulnerabilities, creation of national test beds, and future certification schemes.

Information regarding a nation's cyber defenses and early warning systems are intentionally kept secure and limited. Given this restraint, little information on early warning systems embedded in Dutch government infrastructure is publicly accessible. Some traces of early warning system usership, however, can be found for private energy companies embedded in the Dutch electrical grid. The trend here is that cybersecurity measures and monitoring software programs are increasingly created and managed by third-party entities like Dragos, IBM, or Nozomi Networks and then paid for as a service by energy companies. The reliance on private entities as the managers of critical infrastructure security is worrisome and presents another vulnerability to be carefully considered. In the year 2015, the Dutch had nationwide cyber-risk defenses that included "Taranis" and "Beita," but it is unclear now whether these are still in operation. Taranis was "an open-source software used by several other CERTs" that used to collect, analyze, and publish warnings about ICT vulnerabilities, while the 'Beita' program consist[ed] of a number of honeypots and a network of sensors installed at government organizations to monitor automatic Internet attacks."[50]

Beginning in 2016 as a pilot program, and having since expanded, the national detection network (NDN) seems to be the Dutch government's most recent development in early warning system installation. The NDN serves Dutch institutions and CEI-operating companies by providing advance warning of threats through 24/7 data analysis informed by sensors and probes installed extensively throughout government networks.[51] The function is to raise awareness before intrusion, detecting real-time indicators of compromise (IoC) and advanced persistent threats (APTs). When threats are

50. Hathaway and Spidalieri, "Netherlands: Cyber Readiness."

51. Sergei Boeke, "National Cyber Crisis Management: Different European Approaches," *Governance* 31, no. 3 (July 2018): 449–64, https://doi.org/10.1111/gove.12309.

identified, NDN members are notified immediately and respond accordingly. The NDN is still growing in scope; at full operation the NDN will connect 250 organizations.[52] The most recent national cybersecurity agenda indicated increased funding for the effort to future-proof CI networks.[53]

The Netherlands participates in various interagency partnerships and exercises to foster information-sharing and crisis-response strategies. Primary allies in the field of cyber defense have been EU and NATO member states. Collaboration has been exhibited through multinational joint exercises such as the EU Cyber Europe exercise, NATO Cyber Coalition and Cyber Atlantic exercises, and the US Department of Homeland Security's Cyber Storm.[54] Reflecting the increased interconnectedness of the European power grid and the Netherlands as a hub for these energy transfers, the nation has also agreed to participate in ongoing information-sharing efforts and international networks in the cyber realm. These include NATO's malware information-sharing platform (MISP), the European Network and Information Security Agency (ENISA), the energy-specific European Network for Cybersecurity (ENCS), the EU CSIRT Network, Forum of Incident Response and Security Teams (FIRST), and the International Watch and Warning Network (IWWN).[55]

In line with recommendations made by The Dutch Advisory Council on International Affairs (AIV) and the Advisory Committee on Issues of Public International Law (CAVV), the Netherlands has developed its offensive and defensive cyber capabilities side-by-side since 2011. The Dutch Ministry of Defense houses the Joint Sigint Cyber Unit (JSCU) and Dutch Defense Cyber Command, the operational unit and strategizing body, respectively, for leveraging cyberwarfare tactics. In mid-2014 the maturity of Dutch offensive cyber capabilities was reflected when it was revealed that the JSCU had infiltrated the computer networks of Russian hacker group Cozy Bear.[56] In subsequent press statements, the Ministry of Defense announced that Cyber Command could be deployed for offensive tasks "such as disrupting or disabling enemy networks and systems such as phones

---

52. Hathaway and Spidalieri, "Netherlands: Cyber Readiness."

53. *National Cybersecurity Agenda – A Cyber Secure Netherlands* (Amsterdam: National Cyber Security Centre Ministry of Justice and Security, April 20, 2018), https://english.ncsc.nl/publications/publications/2019/juni/01/national-cyber-security-agenda.

54. Hathaway and Spidalieri, "Netherlands: Cyber Readiness."

55. Hathaway and Spidalieri, "Netherlands: Cyber Readiness."

56. Max Smeets, "The Netherlands Just Revealed Its Cybercapacity. So What Does That Mean?" *Washington Post* (website), February 8, 2018, https://www.washingtonpost.com/news/monkey-cage/wp/2018/02/08/the-netherlands-just-revealed-its-cybercapacity-so-what-does-that-mean/.

and computers, but also weapon or fuel systems or aircraft altitude meters."[57] Over the past five years, the Netherlands has demonstrated transparency about its active offensive cyber capabilities and adopted a posture that breaks from many of its European neighbors. The development of offensive capabilities has made the Netherlands a unique player operating in the cyberwarfare domain. These capabilities may act as a deterrent and allow the Dutch Defense Ministry to prevent an escalation of conflict with malign actors before cyberattacks begin impacting the physical world.

Recommendations

This case study's analysis of available open-source literature reflects the need for the Netherlands to direct attention toward cyber challenges in the energy hybrid-warfare nexus. Because of digitization and electrification, state-sponsored malign actors motivated to perform espionage and influence, disrupt, or sabotage Dutch security now have more entry points to do so. The 2021 Dark Side infiltration of the United States' Colonial Pipeline draws attention to how national security has historically been balanced with critical infrastructure operators and the need to readdress the complex relationship for the future. In the cyber world, the question is not *if* an attack will happen, but *when*. Ensuring that resilience measures, mitigation methods, and avenues of communication exist prior to a crisis is fundamental.

Much remains unknown for how the Dutch cyber landscape will take shape in the years to come in response to the increased cyber threats and attacks worldwide, implementation of new national certification standards and policies, and the emergence of public-private information-sharing platforms. Amidst these changes, there are three actionable recommendations to improve overall cyber resilience in critical energy infrastructure. The recommendations will be evaluated on the following criteria: (1) the degree of interagency and transnational coordination required, (2) the degree to which CEI cybersecurity threats are neutralized or minimized, and (3) associated implementation costs.

NCSC Toolkit for Critical Energy Infrastructure Operator

The NCSC should maintain a toolkit specific to CEI that consists of all national and international cyber-related expectations and requirements, information-sharing and dissemination platforms and organizations, and a "cyber compass for energy." This would be an energy sector-specific

57. Lilly Pijnenburg Muller, *Military Offensive Cyber-capabilities: Small-state Perspectives*, Policy Brief 1, (Oslo: Norwegian Institute of International Affairs, January 2019), https://www.jstor.org/stable/resrep19882.

version of the NCSC's existing cyber compass toolkit, outlining trends in cyberspace so preemptive action could be taken by relevant stakeholders. More specifically, the toolkit should address topics of IT/OT convergence, ICS/SCADA operations, vulnerabilities associated with renewable energy technologies and the phaseout of fossil fuel infrastructure, and internal safeguards (for example, VPNs, firewalls, training to avoid e-mail phishing). Paired with mandatory reporting and benchmark accountability measures, Dutch energy system operators, producers, and suppliers provided with this toolkit can implement cyber secure infrastructure and crisis management protocols that meet government expectations. Currently, there is no centralized and publicly recognized checklist or toolkit of this kind provided by a Dutch ministry.

Developing a toolkit of this caliber would have low to moderate upfront implementation costs, require only moderate coordination, and would have the potential to be a low-effort but highly effective tool for improving the cybersecurity of OES. A small team dedicated to the work of this project, working in collaboration with the NCSC Energy-ISAC (for which many OES are members), could assemble and disseminate this toolkit. The NCSC taking the lead on this is beneficial because they have existing relationships with all the OES in the energy sector.

Rely on IT/OT Engineers' Expertise

The NCSC should create permanent positions for engineers working in IT/OT convergence to join teams at NCSC headquarters focused on cyber-physical resilience. Bringing trained computer and network engineers into the policymaking realm could prove invaluable to future-proofing the energy cybersecurity landscape. To reflect the ongoing IT/OT convergence, other members of the roundtable discussions could include cyber policymakers and cyber-ICT experts. Such a group would address the knowledge-gap that exists at NCSC on ICS/SCADA technology.[58] Permanent positions in NCSC designated for senior engineers with experience bringing ICT online would provide NCSC with a permanent repository of technical expertise. As the Netherlands centralizes more of its cyber efforts and oversight through the NCSC, more opportunities exist for the teams to grow in scope and for publications on CEI to be better informed.

This recommendation would be moderate-to-high in implementation costs and would require medium-to-high coordination. Implementation costs associated with this recommendation would be tied to onboarding and salaries

58. Kamara et al., *Cybersecurity Certification*.

of permanent employees. Because engineers hold critical technical knowledge on how IT/OT convergence occurs and how networks, physical equipment, and energy all connect, the payoff in potential effectiveness could be extremely high. Permanent engineer positions could produce high effectiveness as they would be on staff and could intervene in policy making with technical expertise regularly.

NCSC-sponsored Awareness Raising and Training for ICT Certification

This recommendation is an echo of a recommendation presented in “The Cybersecurity Certification Landscape in the Netherlands after the Union Cybersecurity Act,” a report conducted by the Tilburg Law School and funded by the NCSC.[59]

The NCSC should leverage its position as a hub for cybersecurity and its preexisting relationships with major stakeholders in CEI to raise awareness of the benefit to getting ICT certified. Preexisting relationships and trust with all energy-related TSOs, DSOs, suppliers, and producers positions the NCSC as one of very few entities that can influence their operations. The NCSC can use existing communication channels through the Energy-ISAC to frame certification as a positive and necessary step toward improving security and system resilience rather than it being solely a legal obligation. Informational training could be organized and attended by conformity assessment body (CAB) practitioners and auditors who can explain the intricacies of the certification scheme. In this way, the NCSC acts as a platform connecting its partner organizations to the resources they need to ensure system resilience as they digitize more operations. This recommendation is made with consideration given to the Union Cybersecurity Act and upcoming Dutch policy implementing national standards and certification schemes. Ensuring CEI operators are knowledgeable on certification schemes for ICT will increase their overall voluntary willingness to invest resources in meeting these standards.

Criteria

Having the NCSC assume an active role in guiding partner organizations, specifically those in CEI, through the certification process would pose moderate implementation costs and high coordination requirement and have immeasurable impacts on the degree to which it improves cyber resilience. The NCSC would need to coordinate with experts from conformity assessment bodies to ensure certifications are standardized across use

59. Kamara et al., *Cybersecurity Certification*.

cases, relevant stakeholders are contacted and involved, and information is disseminated via appropriate channels. This cooperation would be resource intensive requiring monetary and time investment from multiple agencies as well as energy TSOs, DSOs, suppliers, and producers.

Conclusion

The Netherlands is a mature actor in the cyber domain that must not let up its efforts to mitigate cyberattacks during a time of rapid electrification and digitization. In a world of increasing interconnectedness, improving cybersecurity of infrastructure is essential to ensuring national security and avoiding possible cascading effects in critical sectors across the region, including health care, water management, and military operations. The operation of the electrical grid and the integration of smart-grid technology are emerging technologies that require attention to future-proof Dutch critical energy infrastructure. The growing use of scanning tools and ransomware techniques by cyber actors is threatening industrial mechanisms tied to energy infrastructure. Deterring malign actors' ability to compromise increasingly system-integrated ICS/SCADA is crucial in a high-tech, interconnected country like the Netherlands. Beyond bolstering its offensive cyber capabilities, the Netherlands has several actionable steps it can take to improve the cyber defense mechanisms of its national security apparatus. I recommend developing an energy sector-specific NCSC toolkit (relying on engineer expertise on IT/OT convergence) and raising awareness for the benefits of certification.

Figure 9-1. Map of the Netherlands threat timeline estimate (6 months indicates likely attack vector in 2022, 1 year by 2023, 2+years by 2024 or later)
Credit: Ryan Fisk and Lucas Cox

Location	Reason for Threat Priority and Timeline
The Hague: National Cybersecurity Centre and European Cybercrime Centre	These organizations are constantly targeted with cyberattacks every day. As they investigate Russian activity—and because the Netherlands has a notable offensive cyber capability—DDoS, ICS, or disinformation attacks are expected to continue during the Ukraine conflict for the next six months.
Port of Rotterdam	ICS or DDoS attacks on port infrastructure could be likely within six months as the Port of Rotterdam is a significant location for NATO troop and equipment mobility in the context of elevated tensions with Russia.
Schiphol Airport	Schiphol Airport is supplied with jet fuel by CEPS, the NATO-operated pipeline. Expect the airport to be vulnerable for the next year due to the airport's importance as a hub and its role as a NATO pipeline terminal in the midst of geopolitical tensions.
Groningen Gas Field	Expect disinformation operations within one year due to current importance for European energy and contentious debate over its health and environmental consequences on which Russia can capitalize.
Offshore Wind Farms	Without adequate cybersecurity protection, the wind farms could become a target in the next six months due to size of impact on Europe. This is one of the world's largest wind farms and accounts for an increasing amount of British energy sources. The few energy infrastructures that have been attacked to date have been wind farms in neighboring Germany.
Borssele Wind Farms	Not as prominent or important as German wind farms that have experienced cyberattacks, but satellite usage and rising importance of renewables could see targeting within the next year as the Netherlands weans itself off of Russian energy.

Select Bibliography

Elgouacem, Assia, and Peter Journeay-Kaler. *The Netherlands's Effort to Phase Out and Rationalise Its Fossil-Fuel Subsidies*. Paris: Organisation for Economic Co-operation/International Energy Agency. September 23, 2020. https://www.oecd.org/fossil-fuels/publicationsandfurtherreading/2020-OECD-IEA-review-of-fossil-fuel-subsidies-in-the-Netherlands.pdf.

Faquir, Dharmesh et al. "Cybersecurity in Smart Grids, Challenges and Solutions." *AIMS Electronics and Electrical Engineering* 5, no. 1 (2021).

Gercek, Cihan et al. "A Comparison of Households' Energy Balance in Residential Smart Grid Pilots in the Netherlands." *Applied Sciences* 9 (15). July 25, 2019. https://doi.org/10.3390/app9152993.

Kamara, Irene et al. *The Cybersecurity Certification Landscape in the Netherlands after the Union Cybersecurity Act, Final Report*. Tilburg, NL: National Cyber Security Centre of the Netherlands/Tilburg Institute for Law, Technology, and Society. July 2020. https://www.ncsc.nl/binaries/ncsc/documenten/rapporten/2020/oktober/2/the-cybersecurity-certification-landscape-in-the-netherlands-after-the-union-cybersecurity-act/NCSC_CYBERCERT_FinalReport__20200730.pdf.

Koninkrijksrelaties, Ministerie van Binnenlandse Zaken en. 2020. "AIVD Annual Report 2019." Jaarverslag. September 3, 2020. https://english.aivd.nl/publications/annual-report/2020/09/03/aivd-annual-report-2019.

Muller, Lilly Pijnenburg. *Military Offensive Cyber-capabilities: Small-state Perspectives*. Policy Brief 1. Oslo: Norwegian Institute of International Affairs. January 2019. https://www.jstor.org/stable/resrep19882.

National Cyber Security Centre (NCSC). NCSC Research Agenda 2019–2022. Hague: NCSC, October 2020. https://english.ncsc.nl/binaries/ncsc-en/documenten/publications/2020/oktober/29/ncsc-research-agenda-2019-2022/200203_NCSC+Onderzoeksagenda+A4+EN+web.pdf.

National Coordinator for Security and Counterterrorism Ministerie van Justitie. "National Cybersecurity Agenda – A Cyber Secure Netherlands." National Cybersecurity Centre, June 1, 2019. https://english.ncsc.nl/publications/publications/2019/juni/01/national-cyber-security-agenda.

National Cybersecurity Agenda – A Cyber Secure Netherlands. Amsterdam: National Cyber Security Centre Ministry of Justice and Security, April 20, 2018. https://english.ncsc.nl/publications/publications/2019/juni/01/national-cyber-security-agenda.

— 10 —

Poland

Frank J. Kuzminski

ABSTRACT: Poland imports the bulk of its energy from Russia. Russia exploits this dependence through cyberattacks on Polish infrastructure. Poland recognizes the risks posed by Russian interference and has responded by creating a branch of its government specifically to address cyber security. It has also created alliances with its neighbors in the region to prevent and mitigate the Russian cyber threat. The country has taken strong comprehensive steps in legislation, policy, and practice to secure its infrastructure and aid its neighbors who suffer from a similar political situation.

Keywords: Baltic pipe, SCADA, Gazprom, smart grid, Russian cyberattacks, Network of Information Security Directive, Russian disinformation, Poland Ministry of Digital Affairs, NASK, ARAKIS

Introduction

Poland occupies an essential position at the intersection of continental Europe and the so-called near abroad of Russia. It is the bridge through which the Baltic states are connected to the European Union. Since Russia first annexed Crimea and invaded Ukraine in 2014, Poland has grown wary of Russia's coercive political behavior in the region. This wariness has grown exponentially in response to Russia's full invasion of Ukraine in February 2022. Poland's most striking recent trend before the Ukraine invasion was the relative decrease in domestic energy production and relative increase in reliance on energy imports, mainly from Russia.[1] In response to the Russian

1. Rafał Macuk, "Energy Transition in Poland: Edition 2020," Forum Energii (website), 2020, https://forum-energii.eu/public/upload/files/Energy%20transition%20in%20Poland.%202020%20Edition.pdf.

invasion of neighboring Ukraine, the Polish government has pledged to end all imports of Russian energy by the end of 2022, calling Europe's reliance on Russian imports a "tool of blackmail." Poland plans to replace Russian gas with imports from Norway through the Baltic Pipeline, the expansion of its LNG terminal on the Baltic Sea, and the signing new contracts with exporters like Qatar and the United States.[2] Russia stopped gas flow to Poland at the end of April and is now supplying gas to Italy, France, and Germany.[3] With the largest domestic coal sector in Europe, Poland is committed to growing renewable energy sources and upgrading energy distribution infrastructure to 5G networked smart grid. Poland's energy sector nevertheless remains vulnerable to geopolitical threats that can manifest as coercive behavior and hybrid threats that include cyberattacks against Poland's energy sector.

This case study first summarizes Poland's energy sector by outlining energy production and distribution, emphasizing renewable energy sources (RES) and critical infrastructure, which encompasses energy sources of supply and distribution infrastructure.[4] The case study then assesses Poland's energy sector vulnerabilities and surveys the range of threats against Poland's energy sector from both state and non-state actors. A review of Poland's early warning systems follows. Finally, the case study concludes with recommendations to address vulnerabilities and mitigate risks to energy security from technical and geopolitical threats.

Energy Production and Distribution

Poland relies on a range of fuel sources for its domestic energy production requirements, including coal, natural gas, petroleum, and a variety of RES. While Poland generates most of its electricity using coal, renewable energy sources are the fastest-growing segment in Poland's energy production landscape. Renewable energy sources accounted for over 20 percent of installed generating capacity for the first time in 2019. That same year, roughly 15 percent of Poland's domestic energy production came from RES, the most ever.[5] Poland's RES and infrastructure include wind,

2. Zosia Wanat, "Poland to EU: Follow Our Lead on Scrapping Russian Energy," *Politico* (website), March 30, 2022, https://www.politico.eu/article/follow-my-lead-on-scrapping-russian-energy-poland-tells-the-eu/.

3. "Cut Off by Moscow, Poland Gets Russian Gas from Its Allies," Bloomberg (website), May 4, 2022, https://www.bloomberg.com/news/articles/2022-05-04/cut-off-by-moscow-poland-gets-russian-gas-from-its-allies?leadSource=uverify%20wall.

4. "Systemy infrastruktury krytycznej," Rządowe Centrum Bezpieczeństwa, 2021, accessed May 12, 2021, https://www.gov.pl/web/rcb/systemy-infrastruktury-krytycznej.

5. Macuk, "Energy Transition in Poland: Edition 2020."

solar, hydro, and biofuels (biomass and biogas). Wind power is the largest segment of Poland's RES, accounting for 65 percent of installed generating capacity as of 2019.[6] The second-largest RES segment is solar energy. Photovoltaic sources for solar energy amount to nearly 16 percent of installed generating capacity as of 2019, with a mix of government-subsidized solar farms and private end-user installed equipment.[7] Hydroelectric power and biofuels round out Poland's RES and account for 9 percent and 11 percent of installed generating capacity, respectively.[8] Wind power is thus the largest and most promising RES segment in terms of growth and generating capacity.

Despite Warsaw's emphasis on RES, coal-fired power plants supplied approximately 74 percent of Poland's electricity generation demand, while natural gas and renewable sources accounted for 9 percent and 14 percent, respectively, in 2019.[9] In 2020, Poland became the largest coal producer in the EU, after Germany reduced its domestic coal production to meet emissions targets.[10] Coal remains Poland's largest domestic fuel source but is increasingly difficult and expensive to extract. As coal prices drop across the EU, producing electricity from coal-fired plants is increasingly cost-prohibitive under the EU's carbon-swapping scheme and greenhouse gas emissions targets.[11] Despite ample deposits and a large coal industry, Poland had been a net importer of coal, mainly from Russia. As of May 2022, Poland has halted all imports of Russian coal, presenting a time-sensitive challenge to domestic suppliers.[12]

Poland also imports over 80 percent of the natural gas it consumes, most of which came from Russia and its state-owned energy company Gazprom until April 2022.[13] Russian natural gas had been delivered to Poland via the Yamal-Europe pipeline, extending over 4,000 kilometers

6. "Poland – Country Commercial Guide: Energy Sector," U.S. Department of Commerce International Trade Administration, July 2020, https://www.trade.gov/country-commercial-guides/poland-energy.

7. Macuk, "Energy Transition in Poland: Edition 2020."

8. Macuk, "Energy Transition in Poland: Edition 2020."

9. "POLAND," U.S. Energy Information Administration, July 2020, https://www.eia.gov/international/analysis/country/POL.

10. *Statistical Review of World Energy 2020*, 69th ed. (London: British Petroleum, 2020), 6, https://www.bp.com/content/dam/bp/business-sites/en/global/corporate/pdfs/energy-economics/statistical-review/bp-stats-review-2020-full-report.pdf.

11. Paul Hockenos, "As Pressures Mount, Poland's Once-mighty Coal Industry Is in Retreat," Yale Environment 360 (website), October 20, 2020, https://e360.yale.edu/features/as-pressures-mount-polands-once-mighty-coal-industry-is-in-retreat.

12. Zosia Wanat, "Poland to EU: Follow Our Lead on Scrapping Russian Energy."

13. "POLAND," U.S. Energy Information Administration.

from the Yamal Peninsula in northern Russia through Belarus, Ukraine, and Poland toward Germany.[14]

Poland imports natural gas via its liquified natural gas (LNG) terminal at Świnoujście, in operation on the Baltic Coast since 2015. Poland also partnered with several European countries on the Baltic Pipe Project. The Baltic Pipe will connect Norway with continental Europe, pass through the North Sea, Denmark, and the Baltic Sea, and terminate in Poland. In addition, the Polish segment will expand the onshore gas transmission network with over 300 kilometers of new pipeline integrating Baltic Pipe with Poland's national gas transmission system. Construction began in the Baltic Sea in May 2021, with initial deliveries of Scandinavian gas to Poland slated for October 2022.[15]

The Polish government adopted a new energy policy in February 2021, the Poland Energy Plan (PEP) 2040. The PEP policy sets ambitious goals to reduce the country's dependence on domestic coal and foreign hydrocarbon imports for energy production and reduce the country's carbon emissions to better align with EU targets and improve air quality. According to the PEP, Poland will accomplish these energy goals in the near term by expanding generating capacity from RES through 2030 and in the long term by building nuclear reactors to incorporate zero-emissions nuclear power into a diversified energy portfolio by 2040.[16] The policy aims to increase RES generation capacity by 65 percent through 2025, primarily from building offshore wind farms in the Baltic Sea and expanding onshore wind farms and photovoltaic sources.[17] Warsaw plans to invest over 130 billion zloty (approximately $34.4 billion) in offshore wind farms that will generate up to 11 gigawatts by 2040, with the first projects coming online in 2025 and generating 5.9 gigawatts by 2030.[18] With these projects and the attendant reduction

---

14. "The End of the Yamal Contract: Poland's Gas Sector to Enter a New Era," Warsaw Institute, December 6, 2019, https://warsawinstitute.org/end-yamal-contract-polands-gas-sector-enter-new-era/.

15. "GAZ SYSTEM Begins Laying the Baltic Pipe Offshore Gas Pipeline," GAZ SYSTEM (website), May 6, 2021, https://www.gaz-system.pl/en/for-media/press-releases/archives/gaz-system-begins-laying-the-baltic-pipe-offshore-gas-pipeline.html.

16. "Poland Adopts 2040 Energy Policy, Plans to Cut Coal Share to 56% by 2030," S&P Global Market Intelligence, February 3, 2021, https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/poland-adopts-2040-energy-policy-plans-to-cut-coal-share-to-56-by-2030-62459745.

17. Will Mathis and Maciej Martewicz, "Europe's Coal Heartland Is the Hottest Market for Green Power," Bloomberg (website), June 24, 2020, https://www.bloomberg.com/news/articles/2020-06-24/coal-heartland-of-europe-is-the-hottest-market-for-green-power.

18. Adam Easton and Stuart Elliott, "Poland's PGNiG Requests Talks with Gazprom on Contracted Gas Price," S&P Global Platts (website), November 2, 2020, https://www.spglobal.com/platts/en/market-insights/latest-news/natural-gas/110220-polands-pgnig-requests-talks-with-gazprom-on-contracted-gas-price.

in coal usage, Poland seeks to generate at least 23 percent of its domestic power requirements from RES by 2030.[19]

In October 2020, Poland announced a strategic 30-year partnership with the United States to develop Poland's civil nuclear program.[20] Poland plans to build up to six nuclear power plants through 2043 with investment and technical assistance from American nuclear firms, including Westinghouse Electric Corporation.[21] Through the civil nuclear program, Poland aims to reduce its reliance on imported hydrocarbons and increase energy security and clean energy targets.

To better integrate with EU transmission networks, Poland will invest over $3 billion through 2027 to modernize and expand the transmission grid, part of the country's critical infrastructure.[22] The modernized grid will also optimize the integration of Poland's growing RES segment into transmission infrastructure. The PEP directs smart meters to be installed at 80 percent of end users in Poland by 2026. As of 2020, approximately 11 percent of end users had smart meters installed.[23] Smart meters are part of Poland's advanced metering infrastructure (AMI), enabling remote digital communications and data transfer to monitor energy demand and consumption by the country's distribution system operators (DSO). Eventually, AMI will be connected over 5G networks and comprise a smart grid that can mitigate the inherently variable nature of electricity generation from wind and solar sources.[24] In addition, to maximize the reliability of energy supply from RES, smart grids integrate information technology (IT) and sensors with traditional energy transmission infrastructure to actively manage energy supply and demand. Energa, the leading Polish DSO in terms of AMI and smart-grid implementation, is leading a pilot smart-grid project to install IT components and sensors throughout the transmission infrastructure in the north of the country. The suite of smart-grid technologies being installed includes grid automation through switch disconnectors, radio supervisory systems,

19. Ministry of Energy, *Draft Energy Policy of Poland until 2040* (Warsaw: Republic of Poland, 2018), 5, http://seo.org.pl/en/zaktualizowany-projekt-polityki-energetycznej-polski-do-2040-r/.

20. "Nuclear Newswire: Westinghouse to Invest in Poland's Nuclear Future," Nuclear Newswire (website), March 17, 2021, https://www.ans.org/news/article-2722/Westinghouse-to-invest-in-polands-nuclear-future/.

21. "Westinghouse to Invest in Poland's Nuclear Future."

22. "Market Intelligence: Poland Power Transmission and Distribution," US Department of Commerce International Trade Administration, December 20, 2019, https://www.trade.gov/market-intelligence/poland-power-transmission-and-distribution.

23. "Poland – Country Commercial Guide: Energy Sector," US Department of Commerce.

24. "Poland – Country Commercial Guide: Energy Sector," US Department of Commerce.

IT control systems networked over wired and wireless data communications, and energy storage systems to stabilize energy distribution during variable power generation scenarios.[25]

Wireless data communications enable DSOs to monitor usage and update firmware, both of which increasingly occur over 5G networks. Poland's nascent smart-grid infrastructure includes a pilot 5G private digital network connecting smart meters at individual end-user locations with supervisory control and data acquisition (SCADA) control systems. In 2020, *Polska Grupa Energetyczna*, Poland's largest distribution system operator, partnered with Finnish telecommunications giant Nokia to develop and install a pilot 5G network to connect over 20,000 customers as a proof of concept.[26] Under PEP 2040, smart grids will enable Poland to integrate future RES projects, including the offshore wind farms in the Baltic Sea, into Poland's modernized electricity transmission networks and ultimately across the EU.

Vulnerabilities

Poland's dependence on natural-gas imports to meet energy demands will remain a persistent vulnerability to Poland's energy security through the mid- to long term. Pipelines, upon which Poland and other EU members rely for natural-gas imports, are especially vulnerable to sabotage, cyberattacks, and criminal hacking. While sabotage in the form of physical destruction by a state or non-state actor is an extreme and unlikely scenario, cyberattacks and criminal hacking that render a pipeline's supervisory control and data acquisition (SCADA) control systems inoperable are far more likely and common.

Gas transmission networks comprise SCADA control systems of software automation, digital communications, field devices, and instrumentation to manage the safe and consistent operation of pipelines. A variety of sensors and instruments physically installed in the pipeline, known as field devices, collect data passed to the control layer consisting of programmable logic controllers (PLC), remote terminal units (RTU), and other control systems.

25. "Poland Rolling Out Smart Grid Infrastructure," European Commission (website), May 29, 2019, https://ec.europa.eu/regional_policy/en/projects/Poland/poland-rolling-out-smart-grid-infrastructure#:~:text=This%20is%20Poland's%20largest%20project,to%20more%20sustainable%20energy%20sources.

26. Nick Westerby, "National Grid Operator PGE Systemy and Nokia Create World's First 5G Private Network," *First News* (website), April 7, 2020, https://www.thefirstnews.com/article/national-grid-operator-pge-systemy-and-nokia-create-worlds-first-5g-private-network-11807.

The control layer then communicates with the SCADA host computer via two-way digital communications, using wired and wireless Internet protocols.[27] As a result, the physical instruments and field control devices, and digital communications networks are vulnerable to cyberattacks and hacking through multiple vectors.

Ransomware attacks reflect a potential cyber vulnerability endemic to SCADA-controlled gas transmission networks. Malicious actors can also manipulate software to override sensors causing the sensors to send false data back to control systems, resulting in critical failures in transmission infrastructure when control systems attempt to compensate for inaccurate readings. SCADA control systems are present throughout Poland's electricity transmission grid, including Poland's growing smart-grid infrastructure, and thus reflect a collective series of vulnerabilities across Poland's critical energy infrastructure.

Poland's push to optimize the electricity transmission smart grid for integration with broader EU standards also raises the prospect of cyber penetration from a wider area network and vice versa. Malicious actors could gain access to Poland's critical infrastructure from within the standardized EU network, or they could penetrate Poland's smart grid and gain access to the broader EU network. Supervisory control and data acquisition control systems, such as those in Poland's smart-grid infrastructure, are notorious for weak security protocols because they rarely encrypt data transmitted between field devices and host control computer systems.[28] As a result, networked SCADA control systems are consistently vulnerable to penetration over TCP/IP networks. In other words, the same vulnerabilities present in Poland's gas transmission networks also exist in Poland's electricity grid.

Proprietary SCADA control systems used in energy transmission networks are typically air-gapped from the wider Internet. Poland's pilot 5G connected smart grid relies on Nokia private networks operating at 450 megahertz, the European smart-grid standard, enabling rapid wireless two-way communications between smart meters, field devices, and control systems.[29] The 5G networks hold great promise for a digitally connected

27. Russell W. Treat, "SCADA and Telemetry in Gas Transmission Systems" (Technical Report, EnerSys Corporation, 2016), 3, https://asgmt.com/wp-content/uploads/pdf-docs/2003/1/30.pdf.

28. Marcin Spychała, "Artificial Intelligence in the Service of Critical Infrastructure: Opportunities and Threats," in *Cybersecurity of the Polish Industry: The Energy Sector* (Kraków: Kosciuszko Institute, 2017), 15, https://ik.org.pl/wp-content/uploads/cybersecurity-of-the-polish-industry-en.pdf.

29. Agnieszka Konkel, "Standardisation of Cybersecurity Solutions in the Energy Sector: An Overview of the EU Policy," in *Cybersecurity of the Polish Industry: The Energy Sector* (Kosciuszko Institute, 2017), 30, http://www.ik.org.pl/wp-content/uploads/sklad-en-online.pdf.

future, especially smart-grid infrastructure, but their software-based characteristics make them vulnerable to hacking and penetration. Decentralized software-based routing, artificial intelligence (AI) data management, and wide-area bandwidth coverage reflect aspects of 5G networks that make them more vulnerable to cyberattacks, despite their inherent benefits and potential.[30]

Poland's emerging smart grid and its total electricity and gas transmission infrastructure are vulnerable to cyberattack through countless vectors. In addition, smart meters and pipeline pressure sensors, and other field devices and control systems are susceptible to attacks. As emerging 5G networks replace existing wired communications networks, the attendant risks to cyber penetration will grow exponentially. Moreover, Poland's goal to further integrate its distribution networks with the EU's will also increase its exposure to cyberattacks and hacking from state and non-state actors alike.

Threats

Poland faces geopolitical threats from Russia and, to a lesser degree, China. Threats can manifest as part of a broader sublethal hybrid campaign to achieve political objectives below the threshold of war using cyberattacks and other coercive measures. Poland's most significant geopolitical threat stems from what the *2020 National Security Strategy of the Republic of Poland* calls "the neo-imperialist policy of the authorities of the Russian Federation," which includes the use of military force to coerce neighboring states in Russia's near abroad, as in Georgia in 2008 and Ukraine in 2014 and 2022.[31]

While Russia continues to use overt military force in Ukraine, it also pursues activities below the threshold of war, often through proxies or unattributable actors, to coerce nearby states such as Poland. Hybrid activities, including cyberattacks and disinformation campaigns, are attractive tools for state and non-state actors to achieve political objectives without military force.[32] Russia views cyberattacks, hacking, and the spread of disinformation as instruments of foreign policy. Russia uses these instruments

30. Tom Wheeler and David Simpson, "Why 5G Requires New Approaches to Cybersecurity: Racing to Protect the Most Important Network of the 21st Century," Brookings Institution (website), September 3, 2019, https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/.

31. *National Security Strategy of the Republic of Poland* (Warsaw: Biuro Bezpieczeństwa Narodowego, 2020), https://www.bbn.gov.pl/ftp/dokumenty/National_Security_Strategy_of_the_Republic_of_Poland_2020.pdf.

32. *National Security Strategy of the Republic of Poland*, 7.

as part of broader hybrid campaigns to undermine NATO and the European Union and provide Russia strategic advantage through the manipulation of cyberspace.[33] Russian behavior poses a threat to Poland's energy security due to Poland's dependence on natural-gas imports, which will continue until the end of 2022. Russia has dominated the gas and oil markets in Eastern Europe for decades and has used reliance on Russian gas and oil to threaten supply manipulation as an instrument of political coercion.[34] Although Poland plans to cease gas imports from Russia in 2022, Poland's dependence on imported gas will remain a long-term vulnerability.

Russia also conducts information operations to spread disinformation and promote narratives aligned with Russian security interests.[35] Such information operations, which include targeted hacking of public websites and social media profiles of prominent officials, are part of broader influence campaigns reflective of hybrid threats. For example, a Russian influence campaign has been targeting Eastern European NATO members, including Poland and the Baltic states, since March 2017. Through compromised websites, such as news sources and official government sites, Russian operatives published fabricated articles, stories, quotes, and other documents criticizing the United States and NATO's presence in Eastern Europe.[36]

Russia's disinformation apparatus is active in Poland's energy sector. In March 2021, after Poland announced its strategic partnership with the United States to develop Poland's civil nuclear program, malicious actors hacked into several Polish government websites. They posted false information about leaking nuclear waste at a nearby Lithuanian nuclear reactor that endangered Polish citizens living near the border.[37] The cyberattack and ensuing disinformation action to spread falsehoods, ostensibly to sow fear and distrust toward Poland's nuclear plans among its

33. Juha Kukkola, "The Russian National Segment of the Internet as a Source of Structural Cyber Asymmetry," *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*, 9, https://ccdcoe.org/uploads/2020/12/1-The-Russian-National-Segment-of-the-Internet-as-a-Source-of-Structural-Cyber-Asymmetry_ebook.pdf.

34. Duda, *National Security Strategy*, 8.

35. Lee Foster et al., "'Ghost Writer' Influence Campaign: Unknown Actors Leverage Website Compromises and Fabricated Content to Push Narratives Aligned with Russian Security Interests," FireEye (website), July 29, 2020, https://www.fireeye.com/blog/threat-research/2020/07/ghostwriter-influence-campaign.html.

36. Foster et al., "'Ghost Writer' Influence Campaign."

37. Givi Gigitashvili, "Cyber-enabled Information Operations Targets Poland with Radiological Leak Hoax," Atlantic Council Digital Forensic Lab (website), April 2, 2021, https://medium.com/dfrlab/cyber-enabled-information-operation-targets-poland-with-radiological-leak-hoax-28a5b1fb6776.

population, have not been officially attributed to Russia. The hack, however, and spread of disinformation resembled a "typical Russian attempt."[38]

Figure 10-1. Cyber and disinformation threat overlay

Russian perceptions of the EU and NATO, and the greater international order, must be considered in the context of Russia's relationship with China. Russia and China share a range of strategic interests, including diminishing the standing and security role of the United States in global affairs.[39] Poland has sought to strengthen relations and military cooperation with the United States ever since the Crimean crisis of 2014, and Beijing's deepening relationship with Russia, even during the Ukraine invasion, suggests China tacitly accepts Russia's revisionist behavior in Eastern Europe.[40] Moreover, a shared Russian and Chinese vision of a weakened American military presence in the world would undermine the effectiveness and credibility of the NATO alliance, which is the foundation of Poland's security policy.[41] China is a notorious cyber actor that flaunts international norms and engages in malicious activity against government organizations and the private sector. China's continued rise, therefore, reflects potential long-term threats to Poland's security environment.

38. "Polish State Websites Hacked and Used to Spread False Info," AP News (website), March 17, 2021, https://apnews.com/article/europe-poland-eastern-europe-lithuania-nuclear-waste-424dd97778b3d2046bc1cb61a175f270.

39. "Natural Gas Weekly Update: Poland Natural Gas Grid," US Energy Information Administration.

40. Paweł Paszak, "Poland-China Relations in 2021: Current State and Prospects," Warsaw Institute (website), January 29, 2021, https://warsawinstitute.org/poland-china-relations-2021-current-state-prospects/.

41. Paszak, "Poland-China Relations in 2021."

Early Warning Systems

Poland implemented the Network and Information Security (NIS) directive, the first EU-wide cybersecurity legislation, in November 2017 through the National Framework of Cybersecurity Policy (NFCP) of the Republic of Poland for 2017–2022. The NFCP seeks to increase Poland's capacity to achieve security of public and private sectors and citizens alike from cyberattacks and disruption of critical infrastructure.[42] As part of this policy, information about increasing cyber threats and vulnerabilities and potential cyberattacks is essential for providing early warning to Poland's Internet users. Therefore, the NFCP calls for national cybersecurity management systems to aggregate information, analyze threat reports, and issue warnings and risk-mitigation measures to relevant stakeholders.[43]

Poland's Ministry of Digital Affairs thus created the department of cybersecurity in 2015, which is responsible for implementing national and EU guidelines for IT systems protection and risk assessment of IT systems across Poland.[44] The ministry supervises a semiautonomous organization knows as the Research and Academic Computer Network (Naukowa Akademicka Sieć Komputerowa, NASK), which focuses on Internet security with operations ranging from providing responses to cyber threats to early warning of cyberattacks against Polish industrial and economic sectors, including Poland's energy sectors.[45] In addition, NASK manages Poland's National Cyberspace Protection System and operates Poland's Computer Emergency Response Team, CERT.pl. As part of the public-private partnership, NASK leverages innovative technological solutions for practical cybersecurity applications. The most extensive commercial collaboration fostered by NASK is with ARAKIS Enterprise, which implemented ARAKIS-GOV in conjunction with the Polish Internal Security Agency.[46]

ARAKIS Enterprise is a commercial cyber early warning system for businesses. It does not replace typical cybersecurity measures but instead

42. "National Framework of Cybersecurity Policy of the Republic of Poland for 2017–2022," Ministry of Digital Affairs, 2017, 7, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Cybersecuritystrategy_PL.pdf.

43. "National Framework of Cybersecurity Policy of the Republic of Poland for 2017–2022," 14.

44. Joanna Świątkowska, Izabela Albrycht, and Dominik Skokowksi, *National Cyber Security Organisation: POLAND* (Tallinn, EE: NATO Cooperative Cyber Defence Centre of Excellence, 2017), 10.

45. Świątkowska, Albrycht, and Skokowksi, *National Cyber Security Organisation: POLAND*, 11.

46. Piotr Kijewski and Adam Kozakiewicz, "Security Research at NASK: Supporting the Operational Needs of a CERT Team and More," in *Proceedings of 2011 First SysSec Workshop* (Amsterdam: IEEE, 2011), 97, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6092775.

works under the auspices of NASK to provide data on emerging cyber threats and attacks, both localized and regional, to stakeholders and government agencies. ARAKIS improves Poland's situational awareness of cyber threats and potential attacks across Poland's Internet address space. ARAKIS works by operating a network of sensors and data collection mechanisms to obtain near real-time data from firewalls and antivirus systems for early detection of malicious activity and discovering potentially new attack vectors against zero-day vulnerabilities.[47] As an early warning system, ARAKIS detects cyber threats that propagate through active means, such as worms and other malware.

In 2016, the NIS directive incorporated data- and information-sharing protocols into regulatory requirements for incident reporting and threat analysis across EU computer security incident response teams (CSIRT). According to the NIS directive, transmission network and distribution system operators in EU-member states must share sensitive information regarding IT vulnerabilities, cyberattacks, and digital network penetrations to facilitate crisis response and mitigate risks due to a *lack of preparedness*.[48] Such an information-sharing mechanism enables interorganizational and inter-state cyber threat assessments and risk analysis to define appropriate mitigation measures.[49] The NIS directive also created a CSIRT network to "contribute to developing confidence and trust between member states and to promote swift and effective operational cooperation."[50] As of 2021, 25 CSIRTs operate in Poland, representing both government and private organizations across various constituencies. In addition, each of the five major DSOs operates a CSIRT as part of the critical information infrastructure protection (CIIP). Only three of Poland's CSIRTs, however, are members of the NIS-directed network.[51]

47. Piotr Kijewski, Mirosław Maj, and Krzysztof Silicki, *Research and Development Projects Launched in Response to the Dynamic Evolution of Internet Security Threats – A Perspective of a CERT Team* (Warsaw: NATO Science & Technology Organization, November 22, 2010), https://apps.dtic.mil/sti/citations/ADA592007.

48. Smart Grid Task Force Expert Group 2, *Recommendations for the European Commission on Implementation of a Network Code on Cybersecurity, Interim 1st Report* (Brussels: European Commission, 2017), 13.

49. Smart Grid Task Force Expert Group 2, *Network Code on Cybersecurity*, 11.

50. European Parliament and Council of the European Union, "Article 12, Directive (EU) 2016/1148 of the European Parliament and the Council of 6 July 2016 Concerning Measures of High Common Level Security of Network and Information Systems across the Union," *Official Journal of the European Union* 194, no. 19 (July 2016), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&rid=1.

51. CSIRTs Network (website), n.d., accessed May 15, 2021, https://csirtsnetwork.eu/.

Recommendations

Poland's ability to ensure energy security and support alliance efforts to deter aggression relies on its critical infrastructure. This case study provides the following recommendations to mitigate risks of cyberattack and ensure Poland's future energy security.

Transparency

Poland's long-term energy security in the cyber era demands transparency between companies, distribution system operators, government cybersecurity organizations, and EU partners. Organizations at all levels, including national and industry sector CSIRTs, must share cyber threats and vulnerabilities using established NIS-directed networks and channels. In addition, cyber professionals must share risk analysis, based on geopolitical trends and events and best practices, and practical steps to protect critical infrastructure.

5G Supply-chain Security

Poland's 5G connected smart grid will introduce new risks and potential attack vectors into Poland's critical infrastructure. Therefore, Poland must approach 5G risk mitigation holistically by partnering with trusted vendors, such as Nokia, and setting 5G equipment supply-chain standards for the EU.

5G Network Security Protocols

Poland should integrate security protocols into 5G network layers (such as firewalls or malware detectors). Operators should also implement end-to-end encryption for all SCADA control systems as they roll out 5G networks near- to mid-term, especially at distributed cloud computing nodes used in 5G network operations.[52] Additionally, Poland should isolate 5G network slices for dedicated critical infrastructure use, especially electricity smart-grid transmission networks.[53]

52. Gregg Knowles, "The Cybersecurity Risks Associated with 5G Networks and How to Manage Them," ITProPortal (website), March 2021, https://www.itproportal.com/features/the-cybersecurity-risks-associated-with-5g-networks-and-how-to-manage-them/.

53. Ericsson, *A Guide to 5G Network Security 2.0: Conceptualizing Security in Mobile Communications Networks – How Does 5G Fit In?* (Stockholm: Ericsson, 2018), 9, https://www.ericsson.com/en/security/a-guide-to-5g-network-security.

Natural-gas Transmission Network Resilience:

Poland must ensure the Baltic Pipe construction is complete ahead of the Yamal contract termination in December 2022. Poland should continue with its plans to fast-track LNG terminal capacity expansion at Świnoujście and increase the number of market partners to diversify its sources of natural gas. Additionally, Poland must develop redundancy in gas distribution capacity to accommodate planned and unexpected disruptions to gas pipeline operations. Distribution capacity must be flexible enough to maintain consistent supply within the country should a critical node or pipeline be disabled due to a cyberattack.

Conclusion

Poland's geostrategic position at NATO's frontier and the nexus between continental Europe and Russia's near abroad makes it a lucrative target for political coercion and hybrid threats, including cyberattacks against critical infrastructure and the energy sector. Poland remains dependent on energy imports, especially natural gas, even as it seeks to diversify its sources of supply completely away from Russian imports and expand domestic generating capacity from renewable energy sources. This dependence exposes Poland to coercive energy supply manipulation and disruption through cyberattacks, especially during potential hybrid threat scenarios. Poland requires access to a stable supply of natural gas in the near term, which means ensuring the Baltic Pipe and LNG capacity expansion proceed as scheduled in 2022. Delays or disruption of the Baltic Pipe may force Poland to restart gas imports from Russia.

Additionally, Poland must ensure the security of its smart-grid infrastructure and 5G connected control systems through encryption and data resilience while increasing transparency and information sharing to thwart would-be attackers and disinformation campaigns. Poland must develop a diverse energy portfolio consisting of redundant supply streams and distribution infrastructure in the mid- to long term. Poland must integrate domestic energy production from nuclear power and renewable energy sources and coal, with stable natural-gas supply streams from within the European Union. A secure and redundant distribution infrastructure, together with stable energy production and supply, transforms Poland into a hard target against cyber and hybrid threats from state and non-state actors and reduces risks to Poland's and NATO's long-term energy security.

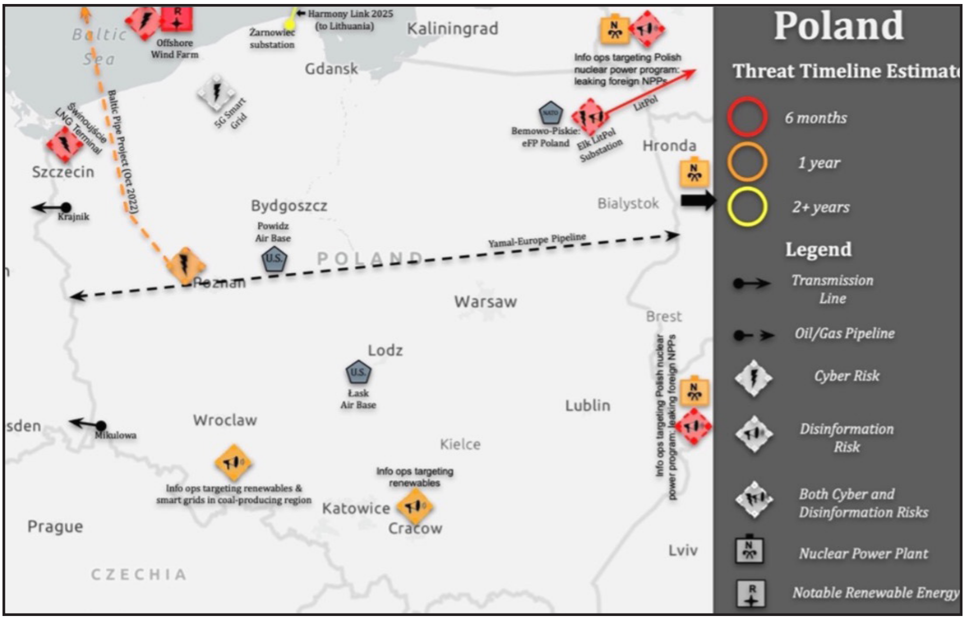

Figure 10-2. Map of Poland's threat timeline estimate (six months indicates likely attack vector in 2022, one year by 2023, two+ years by 2024 or later)
Credit: Frank Kuzminski, Ryan Fisk, and Lucas Cox

Location	Reason for Threat Priority and Timeline
Świnoujście LNG Terminal	Expect the terminal to remain vulnerable for the next six months as it increases energy security in Poland and serves to increase the independence of the Baltics from Russia.
Baltic Pipe	The Baltic Pipe, to be operational October 1, 2022, is the replacement project for the Yamal Pipeline, which supplied LNG from Russia. Since this new connection will be to Norway and is an intentional shift away from Russia, it will remain vulnerable to ICS or disinformation operations within the six months following if tensions continue.
LitPol Link	This electricity link between Poland and Lithuania could remain a target for the next six months because it is an intentional effort to decouple from Russia.
Harmony Link	Harmony Link will increase the reliability of transition from BRELL to the Continental European Synchronous Area once completed in 2025. Intervention to completion could be expected in the year before completion should tensions with Russia increase.
Offshore Wind Farms	Offshore wind farms remain vulnerable for the next six months of the conflict if they do not have adequate cyber protection.
Nuclear Power Program	Nuclear facilities near Belarus and Ukraine likely to be subject to disinformation or cyberattacks within one year due to geostrategic importance during the Ukraine conflict.
Renewable Info Ops and Smart Grids in Coal-producing Region	Disinformation operations will likely occur within the next year as Russia targets renewable energy such as smart grids in its information warfare and cyber operations, especially as Polish coal supplies increase in importance amid the ban on Russian imports.

Select Bibliography

Duda, Andrzej. *The National Security Strategy of the Republic of Poland*. Warsaw: Republic of Poland, May 12, 2020.

Easton, Adam, and Stuart Elliott. "Poland's PGNiG Requests Talks with Gazprom on Contracted Gas Price." *S&P Global Platts*. November 2, 2020. https://www.spglobal.com/platts/en/market-insights/latest-news/natural-gas/110220-polands-pgnig-requests-talks-with-gazprom-on-contracted-gas-price.

Świątkowska, Joanna, Izabela Albrycht, and Dominik Skokowski. *National Cyber Security Organisation: POLAND*. Tallinn, EE: NATO Cooperative Cyber Defence Centre of Excellence, 2017.

European Parliament and Council of the European Union. "Article 12, Directive (EU) 2016/1148 of the European Parliament and the Council of 6 July 2016 Concerning Measures of High Common Level Security of Network and Information Systems across the Union." *Official Journal of the European Union* 194, no. 19 (July 2016). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&rid=1.

"Market Intelligence: Poland Power Transmission and Distribution." US Department of Commerce International Trade Administration (website). December 20, 2019. https://www.trade.gov/market-intelligence/poland-power-transmission-and-distribution.

"Natural Gas Weekly Update: Poland Natural Gas Grid." US Energy Information Administration (website). May 21, 2020. https://www.eia.gov/naturalgas/weekly/archivenew_ngwu/2020/05_21/#itn-tabs-1.

Wheeler, Tom, and David Simpson. "Why 5G Requires New Approaches to Cybersecurity: Racing to Protect the Most Important Network of the 21st Century." Brookings Institution (website). September 3, 2019. https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/.

– Case Studies –

Conclusion: West and Central Europe

France, Germany, the Netherlands, Belgium, and Poland have benefited from their energy partnerships in the past. But energy dependencies and the introduction of renewable sources that cannot yet provide sufficient independent energy on a national scale have left the countries vulnerable to hybrid warfare. The transition of these countries to renewables that are not yet cyber-hardened has left their energy landscapes vulnerable to escalating cyberattacks, especially in the context of Russian hybrid warfare during the Ukraine conflict. These major NATO powers will need to focus on ensuring that they diversify their energy sources and speed their development of renewables with appropriate critical infrastructure cybersecurity and that no non-emissions producing independent energy source, such as nuclear, is left off the table.

– Case Studies –

Baltics

The Baltics region consists of three nations: Estonia, Latvia, and Lithuania. All three are former Soviet nations in a unique position of being at high risk from Russian interference. The Baltics are small nations with small populations, but they have a strategic position along the Baltic Sea with several sizable ports allowing access to west Europe, which would be extremely valuable to Russia. The Baltics wish to remain independent from Russia, however, and have expressed no desire to join Russia to recreate the former Soviet Union, instead aligning themselves with NATO and their energy programs with those put forth by NATO member nations.

Of the Baltic states, Lithuania was a net energy exporter prior to joining NATO, at which point it abandoned its nuclear power plant and began to make the shift to renewable energy. The shift from nuclear to renewables took time to implement, however, and the Baltic states became net importers of energy, reliant on Russia for the majority of their energy needs. This reliance on Russian energy has created increased security concerns as Russian belligerence in the region has increased. Russia has taken the stance that certain types of cyberattacks are tools of foreign policy; hence, due to their strategic position and historical ties to the Soviet Union, the Baltics are frequently subject to cyberattacks as a means of strongarming a reliance on Russian energy.

The Russian cyber threat has spurred a great deal of innovation and partnership in the Baltics. This region is generally united in the singular mission of defense, and unlike the western regions, there are no disputes of what policies to adopt. Following several large-scale successful cyberattacks on Baltic infrastructure, the Baltics and Poland have formed their own cyber defense alliances. This region has invested a lot into cyber innovation and cyber-hardening of its energy infrastructures and has moved toward the rapid adoption of smart grids to isolate itself from Russian interference as much as possible.

— 11 —

Estonia

Caitlin Quirk

ABSTRACT: The most significant threats to Estonia's infrastructure security center around Estonia's relationship with Russia. Estonia is in a unique position culturally as a former member nation of the Soviet Union and Russia's geographical neighbor. In addition, Estonia is one of the most energy-dependent countries in Europe, relying on a select few pipelines for its domestic energy supply. Russia exploits this dependency frequently and utilizes cyberattacks on critical infrastructure as a tool to exercise political control over Estonia, and Estonia attempts to mitigate this by creating information- and resource-sharing networks with other nations in the region to resist Russian influence and exploitation.

Keywords: Cooperative Cyber Defence Centre of Excellence/CCDCOE, Russian cyberattack, smart grid, Estlink, Elering, BRELL network, critical infrastructure security, Baltics, cyber mitigation

Introduction

Due to its geopolitical location, cybersecurity infrastructure, and energy systems, Estonia is a uniquely positioned NATO member country when evaluating hybrid warfare threats to critical infrastructure. On a broad scale, Estonia is one of NATO's leading members on cybersecurity, with NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) based in Tallinn. The capital city is also the namesake of the CCDCOE's *Tallinn Manual*, which details international law applicable to cyberwarfare. In addition, the government has adapted a horizontal integration of cybersecurity, including a national cybersecurity strategy and the Cybersecurity Act. At all hours, Estonian cyberspace and cyber incidents are monitored by the Estonian

Information System Authority's (RIA) branch CERT-EE.[1] While Estonia has a robust cybersecurity infrastructure, vulnerabilities to malicious actors remain, especially in the energy sector.

Geopolitically, the threat of cyberwarfare from Russia is particularly pertinent in Estonia. As a country of only 1.3 million positioned on the Baltic Sea, with Russia currently invading Ukraine, hybrid warfare is a reality in Estonia.[2] Furthermore, Estonia is no stranger to Russian cyberattacks. In 2007, Estonia was the victim of a large-scale cyberattack led by Russian hackers after the relocation of a Soviet-era bronze soldier monument. Over 50 websites, including those of government entities, banks, and newspapers, went offline simultaneously. This incident had global repercussions, shedding light on the inevitability of cyber warfare and its ability to create confusion, disruption, and agitation in a nation-state.[3] Following the 2007 attacks, Estonia bolstered its cybersecurity measures to predict vulnerabilities and mitigate risk in the cyber realm. One predicted target of hybrid warfare is the energy sector, due to the critical role energy systems have in the functioning of the state.[4]

In Estonia, oil shale dominates the energy sector. As of 2018, oil shale made up 73 percent of total primary energy supply and 72 percent of domestic energy production. Primary energy supply was then followed by bioenergy and waste at 19.3 percent and natural gas at 7.3 percent. The reliance on oil shale demonstrated by these statistics makes Estonia one of the most energy independent countries in the EU, but also one of the most carbon intensive.[5] Estonia has published goals for decarbonization efforts and is working toward implementing increased renewable energy. Yet, it is not solely decarbonization that marks recent changes in Estonian energy infrastructure; the electric grid is also undergoing an important transition.

To lessen reliance on Russian energy sources, the Baltic States are currently undergoing an electric grid reconfiguration in which Estonia will decouple

1. "CERT-EE," Republic of Estonia Information Security Authority (website), n.d., https://www.ria.ee/en/cyber-security/cert-ee.html.

2. "Estonia Population (2021)," Worldometer (website), n.d., accessed April 28, 2021, https://www.worldometers.info/world-population/estonia-population/.

3. "How Estonia Became a Global Heavyweight in Cyber Security," e-Estonia (website), June 14, 2017, https://e-estonia.com/how-estonia-became-a-global-heavyweight-in-cyber-security/.

4. "Cyber Security in Estonia 2020," Republic of Estonia Information System Authority (website), October 5, 2020, https://www.ria.ee/en/news/cyber-security-estonia-2020.html.

5. "Energy Policies of IEA Countries: Estonia 2019 Review – Analysis," International Energy Agency (IEA) (website), October 2019, https://www.iea.org/reports/energy-policies-of-iea-countries-estonia-2019-review.

from the Moscow-based IPS/UPS power grid and synchronize instead with the EU. Although the synchronization of the Baltic power grid with Europe will make future blackout attempts by Russia more difficult to achieve, the transition phase is accompanied with increased cyber vulnerability.[6] To combat the risks associated with the electric grid transition and enhance the security of electricity supply, Estonia has adopted smart-grid technology.[7] Smart meters and data-sharing efforts are being implemented to optimize energy efficiency and ward off malign actors. Smart-grid technology also is susceptible to vulnerabilities.

In this chapter, the electric grid and use of smart-grid technology in relation to Estonia's energy security will be discussed, including weaknesses and risk mitigation methods. First, the energy landscape of Estonia will be surveyed, with in-depth information on electric and smart grids. Then, the chapter will identify cyber vulnerabilities and demonstrate possible weaknesses in grid technologies. In the third section, risk mitigation methods and early warning systems (by public and private actors) will be discussed to contextualize how Estonia responds to cyber threats in critical infrastructure. Finally, the chapter will conclude with recommendations to enhance the energy security of Estonia and NATO as a whole.

Energy Landscape of Estonia

To provide a survey of the energy landscape of Estonia, this section will briefly overview oil shale and then discuss how the electric grid and smart grid are being used. As previously mentioned, Estonia is highly energy independent due to its domestically produced oil shale, which is the principal fuel input to generate electricity. While energy independence has increased business opportunities and security in Estonia, it has also hindered the diversification of energy sources and created reliance on a few select pipelines.[8] As the recent 2021 ransomware attack against the Colonial Pipeline in the United States demonstrates, energy systems are at growing risks of cyber intrusions in NATO member countries.[9] Although the cyber vulnerabilities of oil and

6. Stephen Jewkes and Oleg Vukmanovic, "Suspected Russia-backed Hackers Target Baltic Energy Networks, Reuters (website), May 11, 2017, https://www.reuters.com/article/us-baltics-cyber-insight-idUSKBN1871W5.

7. "Energy Policies of IEA Countries: Estonia 2019 Review."

8. "Energy Policies of IEA Countries: Estonia 2019 Review."

9. Brad Plumer, "Pipeline Hack Points to Growing Cybersecurity Risk for Energy System," *New York Times* (website), May 13, 2021, https://www.nytimes.com/2021/05/13/climate/pipeline-ransomware-hack-energy-grid.html.

gas pipelines are beyond the scope of this report, it is important to note that Estonia's critical infrastructure is susceptible to threats outside the smart grid and the electric grid, including the extraction and transportation of oil. Pipelines (such as the Baltic Connector, which opened in 2020) should be monitored closely to ensure ongoing energy security.[10] At the same time, Estonia must also monitor the energy grid for potential hybrid warfare attacks.

The Estonian electric grid is managed by Elering, the transmission system operator (TSO). Approximately 5,500 kilometers of transmission lines and 155 substations comprise the electricity transmission network.[11] Currently, Estonia is a part of the BRELL network, which connects the nation to Belarus, Russia, Latvia, and Lithuania via AC power lines. Of particular interest to NATO are the three 330-kilovolt lines that run from Estonia to Russia. The lines present a particular vulnerability, as Russia has physical access to a NATO ally power line. Since 2006, Estonia has also been connected to Scandinavian energy sources with the creation of Estlink 1, which provides direct current interconnection from Estonia to Finland. The creation of Estlink 1 marked a shift in Estonia's electricity systems, as the country diversified its electricity supply and moved away from reliance on Russia. Following Estlink 1, Estonia has continued to move toward linking with Europe's electricity system. In 2014, Estlink 2 was finished and increased the transmission capacity between Finland and Estonia to 1,000 megawatts.[12] By shifting electricity supply toward European countries, Estonia has switched its energy market from the Baltic States and Russia to the Baltic States and Scandinavia.

The Baltic push toward aligning electricity systems with Europe continues to be a key strategy for energy security. In 2018, former President of the European Commission Jean Claude Juncker, and the heads of government of the Baltic States confirmed this energy transition by announcing the full synchronization of the Baltic power grid with continental Europe by 2025.[13] The decision to couple with the European electric grid displays Estonia's allyship with NATO member countries and signals a shift away from Russia. To obtain full integration of the electric grid with continental

10. "Balticconnector Gas Pipeline up and Running since 1 January 2020," European Commission (website), January 8, 2020, https://ec.europa.eu/info/news/balticconnector-gas-pipeline-ready-use-1-january-2020-2020-jan-08_en.

11. "Electricity System," Elering (website), n.d., accessed May 20, 2021, https://elering.ee/en/electricity-system.

12. "Electricity System."

13. "European Solidarity on Energy: Synchronisation of the Baltic States' Electricity Network with the European System Strengthens Security of Supply," European Commission (website), n.d., accessed April 28, 2021, https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4284.

Europe, the Baltic States are in the process of desynchronizing from the IPS/UPS network in Russia and connecting to the LitPol Link (Poland), NordBalt (Sweden), and Estlink 1 and 2 (Finland).[14]

During this time of energy transition and modernization, Estonia has adopted smart-grid technology (such as smart meters, smart city lights, and smart city projects) to become more energy efficient and secure. As the electricity TSO, Elering administers and heads the majority of smart-grid innovation. The main goal of smart-grid technology in Estonia is to provide modern IT solutions in a time of immense change in energy systems. Particularly important to Estonia is Europe's energy retail market integration by means of data sharing and access. To work toward data accessibility, Elering has used X-Road technology to form Estfeed, a smart-grid data-sharing platform. X-Road or X-tee technology is a software-based solution that allows Estonia's public- and private-sector parties to link up through a multilayered data exchange. Utilizing X-Road technology, Estfeed enables data access and sharing, consumer authorization of third-party actors to meter data, and the centralization of electric meter data monitoring.[15] Since 2014, Estonia has provided 100 percent of smart-metering coverage of households and offices, creating a wealth of data to inform energy usage, efficiency, and security.[16] Moreover, Elering, in cooperation with WePower, has tokenized a year's worth of energy grid data.[17]

Cyber Vulnerabilities

After being the target of the first cyberwarfare attack in 2007, Estonia knows the threat of hybrid warfare. Due to a combination of Estonia's geopolitical position and energy systems in transition, critical infrastructure is especially at risk of hybrid threats. With key roles in stabilizing society and the state, the electric grid and smart grid will be susceptible to cyberattacks. According to Baltic scholars Arūnas Molis, Claudia Palazzo, and Kaja Ainsalu, the risk of a blackout scenario "remains highly possible," as "cybersecurity expertise and exercise are lacking

14. "European Solidarity on Energy."

15. Federico Plantera, "Access to Electricity and Gas Smart Meter Data in Estonia, " X-Road (website), n.d., accessed April 15, 2021, https://x-road.global/access-to-electricity-and-gas-smart-meter-data-in-estonia.

16. Plantera, "Electricity and Gas Smart Meter Data."

17. Jason Deign, "WePower Is the First Blockchain Firm to Tokenize an Entire Grid," Greentech Media (website), October 29, 2018, https://www.greentechmedia.com/articles/read/wepower-is-the-first-blockchain-firm-to-tokenize-an-entire-grid.

and integration into European natural gas and electricity systems has not been completed."[18] Furthermore, energy security has been established as a cyber vulnerability in the EU's "Joint Framework for Countering Hybrid Threats."[19] More acutely, electricity has been deemed the Achilles' heel of the Baltics in regard to mitigating hybrid threats.[20] Thus, it is imperative to recognize the cyber vulnerabilities posed by electric-grid and smart-grid technologies in order to respond to the rising challenges of cyberattacks.

On a general level, electric and smart-grid operators struggle with common information technology threats. For instance, Elering noted their energy systems are targeted by "the most common risk factors in the cyber room."[21] These risk factors include incidents like botnet, phishing, and service interruption, which are frequent threats identified by Estonia's annual cybersecurity agenda.[22] While these threats are common among all sectors, they are incredibly dangerous when used against critical infrastructure. An example of the urgency of curbing these threats occurred in 2020, when an Estonian energy company notified the government of "memcached," a temporary information caching service that had been left public online and could be misused in denial-of-service attacks. As a result, the cached information of the energy company was leaked, forcing the company to fix its service. CERT-EE then helped check the company's logs and recommend cybersecurity protocols.[23] Although the damage in this situation was minimal, common cyber risks can cause immense harm when leveraged against companies that provide electrical and smart-grid services.

In terms of specific malign cyber actors, Russia remains the most urgent threat to Estonian energy security. The impact of the Russian power system on the Estonian power system is described by Elering as the "most systemic risk" to critical infrastructure cybersecurity in the past 10 years.[24] Thus, the synchronization of the Estonian power grid to Europe is imperative to energy security. Yet, the electric grid, bolstered

18. Arūnas Molis, Claudia Palazzo, and Kaja Ainsalu, "Mitigating Risks of Hybrid War: Search for an Effective Energy Strategy in the Baltic States," *Journal on Baltic Security* 4, no. 2 (December 2018): 2, https://www.researchgate.net/publication/330928695_Mitigating_Risks_of_Hybrid_War_Search_for_an_Effective_Energy_Strategyin_The_Baltic_States.

19. "FAQ: Joint Framework on Countering Hybrid Threats," European Commission (website), https://ec.europa.eu/commission/presscorner/detail/it/MEMO_16_1250.

20. Molis, Palazzo, and Ainsalu, "Mitigating Risks of Hybrid War."

21. "Electricity System."

22. "Cyber Security in Estonia 2021."

23. "Cyber Security in Estonia 2021."

24. "Electricity System."

by smart-grid technology, is particularly vulnerable during systems transitions. Synchronization of the electric grid creates vulnerabilities because Russia has the power to disconnect Estonia from the IPS/UPS framework before the country has fully joined the European electricity system. On the threat of decoupling the grid, Molis, Palazzo, and Ainsalu have noted that the "key question is not whether this weapon will be used, but how successfully it can work," with Estonia's resilience capabilities being the main determinant of the scenario.[25]

Estonia's preparedness scheme to confront this challenge focuses specifically on decreasing bottlenecks and improving interconnectedness. Thus, market security, regional cooperation, and data sharing are reinforced to avoid a Baltic blackout scenario.[26] Not only did the Lithuanian TSO predict a Baltic blackout would cost the region between 1.3 to 2.1 billion euros, but a blackout would cause critical services to stop functioning, fear in society to spread, and political ramifications of hybrid war.[27] Disruptions of energy supply from Russia during the Ukraine crisis, increased power demand, and the transition away from grid integration with Russia and rising energy prices present significant political and economic challenges for the future of Estonia's energy sector. In 2021 alone, the price of natural gas rose 400 percent.[28]

To curb electrical grid vulnerabilities, Estonia has invested heavily in smart metering and data sharing. These emerging technologies, however, have implications for smart-grid vulnerabilities and are not immune to threats; just "as any other device connected to a network, smart meters become vulnerable to attacks."[29] With 100 percent coverage of households and offices by smart meters in Estonia, the sheer number of networked devices in the electric grid provides increased entry points for cyberattacks. As for data sharing in the smart grid, low involvement in public-private partnerships (PPPs) limits the threat mitigation capabilities of X-Road technology. Recent literature on X-Road technology reveals Estonia has high

25. Molis, Palazzo, and Ainsalu, "Mitigating Risks of Hybrid War," 4.

26. "Estonian National Energy and Climate Plan 2030 (NECP) – Policies," IEA (website), https://www.iea.org/policies/12146-estonian-national-energy-and-climate-plan-2030-necp.

27. Molis, Palazzo, and Ainsalu, "Mitigating Risks of Hybrid War."

28. Kaja Kallas, "Political Statement by Prime Minister Kaja Kallas on the Situation in the Electricity Market, January 18, 2022," Republic of Estonia Government (website), January 18, 2022, https://www.valitsus.ee/en/news/political-statement-prime-minister-kaja-kallas-situation-electricity-market-18-january-2022.

29. Rebeca P. Díaz Redondo, Ana Fernández-Vilas, and Gabriel Fernández dos Reis, "Security Aspects in Smart Meters: Analysis and Prevention," *Sensors* 20, no. 14 (July 17, 2020), https://doi.org/10.3390/s20143977.

PPP potential, yet it struggles to engage private actors due to low awareness and understanding of profitability, among other factors. The data-sharing imperative to X-Road technology is in turn hampered by barriers to PPPs.[30] Part of this barrier is the role of utilities, as the government "must set clear limits in market power of distribution utilities while allowing competition in the generation segment with the establishment of a market for energy."[31]

Current Cyber Mitigation Methods or Early Warning Systems

While the Estonian energy sector is at risk of security vulnerabilities such as the grid transition, energy operators and the Estonian government have worked to ensure risk mitigation through training and early warning systems. Under the scope of government, Estonia has robust pathways to address cyber risks to critical infrastructure. Legislation, government agencies, annual strategies, and national training programs inform threat mitigation. In the private sector, companies have invested in early warning technology, grid stabilization projects, and cybersecurity training. As will be displayed by the overview of mitigation methods, Estonia is aware of the threat posed by cyberattacks on energy systems and is actively trying to counter its technology vulnerabilities.

To begin with, Estonia's Information Systems Authority (RIA) manages the nation's cybersecurity and handles cyber incidents. More specifically to energy security, critical information infrastructure protection (CIIP) under RIA protects "public and private sector networks and information systems that are essential for the functioning of the Estonian state."[32] To ensure this protection, cyber vulnerability reporting and monitoring are key aspects of RIA's cyber mitigation methodology. This is apparent in Estonian cybersecurity legislation, mainly the Cybersecurity Act of 2018. Under the Cybersecurity Act, it is mandatory for critical infrastructure cyber vulnerabilities to be reported to CERT-EE, which monitors Estonian cyberspace 24 hours a day. CERT-EE also sends daily automated notifications

30. Karoline Paide et al., "On the Systematic Exploitation of the Estonian Data Exchange Layer X-Road for Strengthening Public-Private Partnerships," in *Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance* (New York: Association for Computing Machinery, 2018), 34–41, https://doi.org/10.1145/3209415.3209441.

31. "Power," Public-Private Partnership Knowledge Lab (website), May 6, 2015, https://pppknowledgelab.org/sectors/power.

32. "Critical Information Infrastructure Protection CIIP," Republic of Estonia Information System Authority (website), n.d., https://www.ria.ee/en/cyber-security/critical-information-infrastructure-protection-ciip.html.

to companies about the misuse and vulnerability of their networks. Yet, the information is not often forwarded to end users, shedding light on a weakness of mitigation methods. Furthermore, actors that are part of the energy sector must follow the regulation titled "Requirements for Risk Analysis of Network and Information Systems and Description of Security Measures," which outlines the service provider's obligation to assess and secure cyber vulnerabilities. Moreover, Estonia utilizes Suricata-4-All (S4A), a freeware-based network traffic analysis system to detect cyberattacks and threats to critical infrastructure automatically.[33] With legislation such as the Cybersecurity Act, agencies like RIA, the 24-hour monitoring of cyberspace by CERT-EE, and the implementation of anomaly detection systems, Estonia has rigorously worked to protect against hybrid threats.

Another crucial aspect to preventing cyber intrusions in Estonia is an emphasis on cybersecurity training. Through cybersecurity events and education, Estonia works to improve the cyber hygiene of individuals and companies. In Tallinn, the CCDCOE hosts the annual Locked Shields event, an international crisis exercise that tests the skills of cybersecurity professionals to defend critical infrastructure and IT against real-time attacks.[34] After identifying the energy sector as vulnerable to cyberthreats in 2019, Estonia practiced how to solve a ransomware attack on an energy company. Earlier in 2016, under the Baltic Ghost training program, cybersecurity training included how to ensure electricity supply in the case of cyberattacks.[35] Strengths of cybersecurity training practices include preparedness for crisis scenarios and the development of management techniques. Yet, these scenarios are solely helpful in a reactionary capacity and fail to provide preventative measures. To predict threats instead of responding to them, early warning systems are imperative.

To track anomalies in the electric grid and monitor grid stability, Elering uses Guardtime's Keyless Signature Infrastructure (KSI), which uses blockchain technology to detect anomalies autonomously in the electric grid.[36] Elering has also initiated other efforts to ensure electric and smart-grid security. In 2020, the first grid stabilization project

33. "Critical Information Infrastructure Protection CIIP."

34. "Locked Shields," NATO Cooperative Cyber Defence Centre of Excellence (website), n.d., accessed May 19, 2021, https://ccdcoe.org/exercises/locked-shields/.

35. "Cyber Security Training Baltic Ghost Practises Ensuring Electricity Supply in the Case of Cyber-Attacks," Elering (website), September 21, 2016, https://elering.ee/en/cyber-security-training-baltic-ghost-practises-ensuring-electricity-supply-case-cyber-attacks.

36. KSI Blockchain," e-Estonia (website), November 15, 2021, https://e-estonia.com/solutions/cyber-security/ksi-blockchain/.

in the Baltics was contracted. Elering partnered with Siemens Energy to build three synchronous condenser plants to increase the resilience of grid infrastructure.[37] Looking toward the future, Datel (an Estonian ICT company) is developing a large infrastructure early warning system called Sille. This system will rely on open satellite data from the European Space Agency.[38] The private and public sector are both working to automate early warning systems and protect electricity and smart grids.

Recommendations

Hybrid threats remain, and the constantly changing nature of cyberspace requires nations to adapt to new challenges. By continuing to bolster its security, Estonia will in turn aid the cybersecurity of NATO as a whole. To do so, Estonia can proactively adapt tools, plans, and early warning systems that mitigate the threats posed by malicious cyber actors. Recommendations for Estonia and NATO include:

1. **European grid adoption.** Ensure the smooth transition to the European synchronized electric grid by expanding X-Road technology and Estfeed as a multi-stakeholder information-sharing platform for the Baltic region. This action would provide a space to report regional cyber threats to critical infrastructure. It is important that both public and private actors report risks to prevent attacks.

2. **Increase regional cooperation and trust.** The Baltic region has been especially hard hit by hybrid threats from Russia in the lead-up to, and during, the Ukraine invasion, and the region would benefit from NATO cooperation to counter Russian cyberattacks. To face the hybrid threats posed by Russia, a "strong regional cooperation with regional priorities" is needed.[39] Furthermore, the protection of critical infrastructure is "not merely a national issue" because the "disruption of energy supply and the destruction of a part

37. "Siemens Energy Wins Grid Stabilization Project in Baltic States," T&D World (website), December 16, 2020, https://www.tdworld.com/grid-innovations/article/21150570/siemens-energy-inc-siemens-energy-wins-grid-stabilization-project-in-baltic-states.

38. "Estonian ICT Company Is Developing a New Early Warning System Based on European Satellite Open Data," PreventionWeb (website), March 9, 2018, https://www.preventionweb.net/news/estonian-ict-company-developing-new-early-warning-system-based-european-satellite-open-data.

39. Molis, Palazzo, and Ainsalu, "Mitigating Risks of Hybrid War."

of energy infrastructure may affect not only the state where they occur but also other states."[40]

3. Public-private partnerships. Develop incentives for Private-Public Partnerships to fully harness X-Road technology and layered data sharing. As previously mentioned, the most effective functioning of Elering's data-sharing platform, Estfeed, relies on public and private actors to share information. By creating incentives for PPPs, Estonian companies will contribute more to Estfeed and provide more data to build security decisions. This is essential, as "PPPs are of utmost importance in the protection of critical energy infrastructure because they are mostly owned by the private sector."[41]

4. Information sharing. Stakeholders in critical energy infrastructure should share best practices on early warning systems and anomaly detection services to ensure their effective and efficient usage. This action would increase the resilience of energy infrastructure.[42]

5. Integrated best practices. Share best practices surrounding critical infrastructure within Estonia and internationally. Estonia is at the forefront of cybersecurity and ensures national cybersecurity through the implementation of events, legislation, training, education, and more. Estonia has already taken steps toward this recommendation through cyber diplomacy efforts with the United States, the Dominican Republic, and other nations around the globe.[43] Best practices should continue to be shared, especially with NATO member countries.

40. Tiziana Melchiorre, *Recommendations on the Importance of Critical Energy Infrastructure* (*CEI*) *Stakeholder Engagement, Coordination and Understanding of Responsibilities in Order to Improve Security* (Vilnius, LT: NATO Energy Security Centre of Excellence, 2018), https://enseccoe.org/data/public/uploads/2018/04/d1_2018.04.23-recommendations-on-the-importance-of-critical-energy.pdf.

41. Melchiorre, *Recommendations*.

42. Melchiorre, *Recommendations*.

43. "Cyber Security in Estonia 2021."

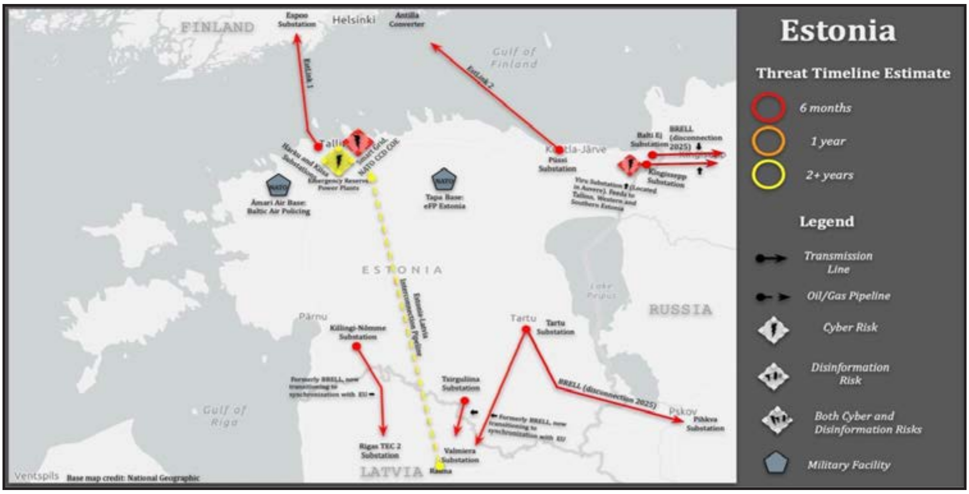

Figure 11-1. Map of Estonia's threat timeline estimate (6 months indicates likely attack vector in 2022, 1 year by 2023, 2+ years by 2024 or later)
Credit: Ryan Fisk and Lucas Cox

Location	Reason for Threat Priority and Timeline
Estlink 1 and 2 to Finland, and Baltic Synchronization (EU Coupling) to Latvia	ICS of Estlink primary transmission lines to remain vulnerable within six months due to Russia's retaliation to Estonia's decoupling from Russian energy
Tallinn Smart Grid	Smart Grid in the Estonian capital remains vulnerable for next two years due to geostrategic importance of the Baltic capital during NATO-Russia tensions.
Viru Substation	The Viru substation, located in Auvere, is a critical juncture that helps to supply Tallinn, western Estonia, and southern Estonia all at once. A cyberattack on the associated SCADA, or a kinetic attack on the physical station, could disrupt a major portion of Estonia's electricity supply.
CCD COE Smart Grid	The CCD COE Smart Grid and ICS could remain a target for the next six months, though Estonia has strong cyber defenses on the grid, and attacks are unlikely to be successful
BRELL	Russia will continue targeting the BRELL interconnection for the next six months to three years due to Russia's last-ditch effort to maintain the Baltics' reliance on Russian energy before another interconnection is complete in 2025.
Estonia-Latvia Interconnection Pipeline	The pipeline infrastructure may be vulnerable to cyber intervention within two years because of its increasing importance as the Baltics seek to diversify away from Russian gas supplies.

Select Bibliography

"Cyber Security Training Baltic Ghost Practises Ensuring Electricity Supply in the Case of Cyber-Attacks." Elering (website). September 21, 2016. https://elering.ee/en/cyber-security-training-baltic-ghost-practises-ensuring-electricity-supply-case-cyber-attacks.

Díaz Redondo, Rebeca P., Ana Fernández-Vilas, and Gabriel Fernández dos Reis. "Security Aspects in Smart Meters: Analysis and Prevention." *Sensors* 20, no. 14 (July 17, 2020). https://doi.org/10.3390/s20143977.

"Estonian ICT Company Is Developing a New Early Warning System Based on European Satellite Open Data." PreventionWeb (website). March 9, 2018. https://www.preventionweb.net/news/estonian-ict-company-developing-new-early-warning-system-based-european-satellite-open-data.

"European Solidarity on Energy: Synchronisation of the Baltic States' Electricity Network with the European System Strengthens Security of Supply." European Commission (website). n.d. Accessed April 28, 2021. https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4284.

Kallas, Kaja. "Political Statement by Prime Minister Kaja Kallas on the Situation in the Electricity Market, 18 January 2022." Republic of Estonia Government (website). January 18, 2022. https://www.valitsus.ee/en/news/political-statement-prime-minister-kaja-kallas-situation-electricity-market-18-january-2022.

"Locked Shields." NATO Cooperative Cyber Defence Centre of Excellence (website). n.d. Accessed May 19, 2021. https://ccdcoe.org/exercises/locked-shields/.

Melchiorre, Tiziana. *Recommendations on the Importance of Critical Energy Infrastructure (CEI) Stakeholder Engagement, Coordination and Understanding of Responsibilities in Order to Improve Security*. Vilnius, LT: NATO Energy Security Centre of Excellence, 2018. https://enseccoe.org/data/public/uploads/2018/04/d1_2018.04.23-recommendations-on-the-importance-of-critical-energy.pdf.

Molis, Arūnas, Claudia Palazzo, and Kaja Ainsalu. "Mitigating Risks of Hybrid War: Search for an Effective Energy Strategy in the Baltic States." *Journal on Baltic Security* 4, no. 2 (December 2018). https://www.researchgate.net/publication/330928695_Mitigating_Risks_of_Hybrid_War_Search_for_an_Effective_Energy_Strategyin_The_Baltic_States.

— 12 —

Latvia

Michael Bervell

ABSTRACT: Like the rest of its Baltic counterparts, Latvia is attempting to move away from Russian power sources into renewable energy independence and has been plagued by Russian cyberattacks for more than a decade which have only increased in the lead up to and during the Ukraine crisis. Latvia is transitioning to a smart-grid energy infrastructure connected through a 5G Internet of Things network, which has increased opportunities for outside exploitation. It has prioritized public-private-international partnerships in combating Russian influence and developing cyber defense strategies, bringing in specialists from different sectors from across Europe to advise on infrastructure security. Furthermore, Latvia has engaged in a unique large-scale education program in order to inform all of its citizens on cyber security.

Keywords: BRELL Network, ENTSO-E, Baltic Energy Market Interconnection Plan/BEMIP, CERT.LV, Russian cyberattacks, Baltic energy security, National Information Technology Security Council

Introduction

"Let the devil into church and he will climb into the pulpit." So goes one of the best-known Latvian proverbs. Originally coined to emphasize piety in the twelfth and thirteenth centuries, today this quip can best be used as an analogy for the state of cybersecurity in Latvia. Located on the cusp of the Baltic Sea, Latvia is a small country the size of Nebraska with 1.9 million citizens.[1] To its North and South are friendly neighbors Estonia and Lithuania; to the East, however, is the devil in the pulpit, Russia.

Time and time again, Russia (a cybersecurity *D'yavol* or devil) has been the culprit of "Easter Egg hacks" in the Baltic region, sowing chaos and discontent in networks through malware hidden on computers that exploits systems at the click of a button. Hiding in a digital pulpit, anti-Baltic actors (often Russian actors) masquerade as natural parts of computer systems before strategically unleashing digital unrest to destabilize countries from within by crippling critical infrastructure. As described in a 2019 report by the Constitutional Protection Bureau of the Republic of Latvia, "Russian cyber-attacks in Latvia have mostly been carried out for espionage purposes and directed against government institutions, mainly in the fields of defence, interior and foreign affairs. The number of cyber-attacks by foreign special services detected in Latvia has not changed significantly over the last 4 to 5 years, reaching a few dozen cases each year."[2]

One of the first examples of the devil in the Baltics occurred in 2008. The subject? Estonia. This attack revealed the power of coordinating physical attacks and cyberattacks.[3] In the midst of one of Estonia's largest public protests about the movement of a historic Estonian statue, the Estonian cyberspace was subject to a distributed denial-of-service (DDoS) attack. Online, thousands of computers around the world repeatedly accessed Estonian websites at Russia's command while planted Russian dissenters sowed unrest in the physical crowds. The result? Internet-connected news organizations, government services, and banking resources in Estonia lost connectivity. While websites in Estonia were only down for a few hours, those who attempted to access Estonian websites from outside the country were unable to for several days.[4] The timing was impeccable. In the midst of riots, a poke of cyber penetration tested the core of Estonian security through a uniquely twenty-first-century battlefield. This was a wakeup call for the Baltic region.

1. "Quick Facts United States," US Census Bureau (website), n.d., accessed May 19, 2021, https://www.census.gov/quickfacts/fact/table/US/PST045221.

2. Constitution Protection Bureau of the Republic of Latvia, *2019 Annual Report* (Riga, LV: Constitution Protection Bureau of the Republic of Latvia, 2019), 26, https://www.sab.gov.lv/files/Public_report_2019.pdf.

3. Luukas Kristjan Ilves, "Cyber Security Trends and Challenges: Latvian and Estonian Experience," February 29, 2012, YouTube video, 2:30, https://www.youtube.com/watch?v=Jg8IADVeNis&list=PL194DD043B0884979.

4. Ilves, "Cyber Security Trend."

Since then, Latvia, Estonia, and Lithuania have banded together with other NATO countries to unify cybersecurity and combat the Russian threat. For instance, the three countries have worked to relieve themselves of Russia's influence by investing in joint infrastructure projects with Sweden, Poland, and Lithuania to reduce Russian dependence by 2025.[5] Latvia has arrested Russian spies and banned Russian TV and the Russian language in schools in an effort to promote national pride on and offline.[6]

Specifically in the cyber context, Latvia hopes to expel the devil from the church by investing in public-private partnerships, international cooperation, and state-wide education. While each Baltic nation has its vulnerability challenges, weaknesses, and successes, this report will focus specifically on Latvian 5G, IoT, and electrical grid challenges. Additionally, it will offer tools and techniques for mitigating future intrusions in cyberspace given the unique makeup of the Latvian cyber defense sector.

Latvia's Cyber Vulnerabilities

Latvian Cyber Structure

The year 2018 was not the best for Latvian cybersecurity. The Republic of Latvia discovered spyware within its Ministry of Interior, and the Latvian social networking site Draugiem.lv was the target of hacktivist attacks.[7] The former of the two attacks was a continuation of targeted 2016 campaigns that threatened the Latvian Defense and Foreign ministries.[8] The latter,

5. Juris Kaža, "Baltics to Cut Electric Links to Russia, Disagree on Power Trading until Then," Medium (website), July 9, 2020, https://juriskaza.medium.com/baltics-to-cut-electric-links-to-russia-disagree-on-power-trading-until-then-b7f7f546c983.

6. AFP, "Latvia Arrests Spy Working for Russia," *Moscow Times* (website), March 2, 2020, https://www.themoscowtimes.com/2020/03/02/latvia-arrests-spy-working-for-russia-a69489; Lauren Chadwick, "Lithuania Follows Latvia in Banning Russian Broadcaster RT," *Euronews* (website), September 7, 2020, https://www.euronews.com/my-europe/2020/07/09/lithuania-follows-latvia-in-banning-russian-broadcaster-rt; and Lucian Kim, "A New Law in Latvia Aims to Preserve National Language by Limiting Russian in Schools," NPR (website), October 28, 2018, https://www.npr.org/2018/10/28/654142363/a-new-law-in-latvia-aims-to-preserve-national-language-by-limiting-russian-in-sc.

7. Inga Šņore, "Iekšlietu IT tīklā atrod spiegu vīrusu, izcelsme liecina par Krieviju," Latvijas Sabiedriskie mediji, November 25, 2018; and "Vēlēšanu dienā uzlauž draugiem.lv un lapā izvieto Krievijas simbolus," Latvijas Sabiedriskie mediji, October 6, 2018.

8. "SAB: Krievijas specdienests pēdējos gados uzbrucis Latvijas kibertelpai," Latvijas Sabiedriskie mediji, October 8, 2018.

timed to take place on election day, posted pro-Russian messages to sway election results.[9]

As described by Krista Viksnins, a Schuman trainee in the European parliament, “hackers replaced the front page of the Facebook-like site with a Russian flag and message saying ‘Fellow Latvians, this concerns you. The Russian border has no limits!’ The page also played the Russian national anthem and included pictures of President Vladimir Putin and the Russian military . . .”

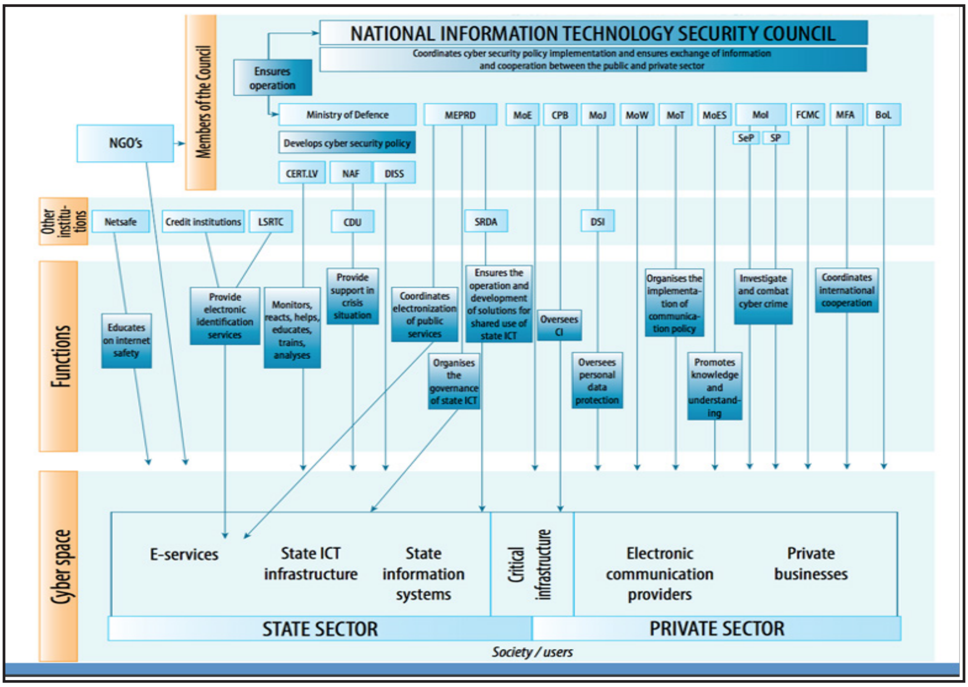

Figure 12-1. Visualization of Latvia’s national cybersecurity policy coordination
Source: Latvian Ministry of Defence, “Cyber Security Strategy of Latvia,” European Union Agency for Cybersecurity (website), n.d., https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss, 21.

In all these cases of Latvian cyberattack, the Latvian Computer Emergency Response Team (CERT.LV) has been the primary institution responsible for analyzing and preventing these attacks, racing to incidents and coordinating incident prevention.[10] Headquartered in the Institute of Mathematics and Computer Science at the University of Latvia, CERT.LV is one of many components of the Latvian cybersecurity arsenal. While the National

9. “Latvia Repulsed Election Day Cyber-attack,” Latvian Public Broadcasting (website), October 18, 2018, https://eng.lsm.lv/article/politics/election/latvia-repulsed-election-day-cyber-attack.a296457/.

10. “Improving Cyber Security Capacities in Latvia,” CERT.LV, accessed May 18, 2021.

Information Technology Security Council develops cybersecurity policy at a national level, the implementation of this cyber policy is left to specific institutions in the public and private sector, including CERT.LV. Figure 12-1 describes the entire Latvian cybersecurity organization, from the National Information Technology Security Council (that functions as a strategy organization) to functional units like Netsafe, SRDA, DSI, and more.[11]

Cyber Challenges Generalized

As a small country, Latvia has always strategically relied on partnerships to thrive. Even after 1991 when Latvia regained independence from the USSR through the Latvian independence and democracy poll, much of Latvia's infrastructure was still tied to Russia. Their former country was still a partner. Demographically, even in 2000, ethnic Russians still made up nearly 30 percent of the country's population of 2.4 million, according to Latvia's census.[12] A core component of the Latvian cybersecurity strategy, however, has been to unwind these relationships with Russia and lean into more global NATO partnerships. While a logically sound goal, its implementation has been far more difficult.

The current Latvian cybersecurity strategy has three major components: building relationships (public, private, and international partnerships), educating the public, and institutionalizing knowledge.

Building Relationships through Partnership

To date, Latvia has relied on public, private, and international partnerships to build and supplement its cybersecurity capabilities. As described by Elina Viksne (a senior expert of the National Cybersecurity Policy Coordination Section at the Latvian Ministry of Defence), cybersecurity is a horizontal issue: the sheer number of actors involved means they all must cooperate in making cyberspace safe.[13] The typical Latvian citizen may interact with government health care, private financial institutions, public Internet networks, websites around the world, and private WiFi routers—all from

11. Latvian Ministry of Defence, *Cyber Security Strategy of Latvia: 2014–2018* (Riga, LV: European Union Agency for Cybersecurity, 2018), https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss.

12. Timothy Heleniak, "Latvia Looks West, But Legacy of Soviets Remain," Migration Policy Institute (website), February 1, 2006, https://www.migrationpolicy.org/article/latvia-looks-west-legacy-soviets-remains.

13. Data Security Solutions, "Securing Cyber Space in Latvia through the Public-private Partnership," November 3, 2016, MP4, 21:10. https://www.youtube.com/watch?v=acM5sfpgHSY.

the same device within the same day. Even though the private sector may have various views on how, when, or why to secure a system, there is no escaping how interconnected cyberspace is, especially for a small country like Latvia. Every citizen's IoT device (cell phones, computers, and more) uses a combination of technologies managed by governments, businesses, and international suppliers.

Unfortunately, one challenge is that in isolation, no single institution has all the human and financial resources to attack every threat or risk globally. By pooling resources, conducting joint cybersecurity exercises, and practicing the coordinated prevention of cyberattacks and issues, Viksne makes an argument for a public-private-international approach. Private companies and governments need to share knowledge with one another to create a system of "security by cooperation."

Latvia has deep investments in this cooperative cybersecurity strategy and fulfills the collectively agreed upon NATO commitment to invest 2 percent of its GDP in defense.[14] Moreover, Latvia helped to establish the NATO Cooperative Defense Centre of Excellence (CCDCOE) in Tallinn in 2008. In partnership with Estonia, Lithuania, Germany, Italy, Slovakia, and Spain, the CCDCOE is designed "to support our member nations and NATO with unique interdisciplinary expertise in the field of cyber defense research" and with training and exercises in technology, strategy, and law.[15] This allows Latvia to fight the military and nonmilitary cyberthreats (hybrid threats) with similar hybrid strategies. Often, these strategies are practiced through red teaming exercises that bring together the public sector, private sector, and international partners to ensure the effectiveness of defenses and counter hybrid responses.

Educating and Training the Public

Even with a public-private-international partnership, the root of cybersecurity is related to individual nodes of people. Thus, a core pillar of Latvian cybersecurity involves educating the public regardless of age. In particular, some of the specific education initiatives include:

14. "Latvia's Security Policy," Ministry of Foreign Affairs of the Republic of Latvia, June 19, 2020.

15. Franklin Holcomb, "Countering Russian and Chinese Cyber-Aggression," Center for European Policy Analysis (CEPA) (website), December 4, 2020, https://cepa.org/comprehensive-reports/countering-russian-and-chinese-cyber-aggression/.

- **Cyber defense unit (18+).** Volunteers from academia, the military, and the general public who have specific skills that can be used to defend the country.[16] While it started with just 13 members, Latvia plans to expand the group to more than 100 soldiers. The pipeline for this unit could come directly from the Baltic University study program that combines regional education resources to develop strong and qualified experts.[17]
- **Youth cyber guards (13–18).** In 2014, Janis Sarts, the state secretary of the Ministry of Defence of Latvia, argued for the need to educate and train teenagers on cyber defense. "We have to understand that children are very active users of the cyber world. We even know of cases when a 14-year-old teenager has created an app which has turned him into a millionaire," Sarts said. In theory, this same type of success could be applied to the security of Latvia generally.[18] The Youth Cyber Guard is an initiative to excite young Latvians to use their technology talents to defend their country in cyberspace.
- **Preschool starting education programs (under 13).** Every phone in Latvia is an IoT device with troves of personal and private information that can be hacked and used maliciously. During a 2012 conference with LATO (the Latvian Transatlantic Organisation), panelists described how Latvia had plans to begin educating students from preschool about Internet safety.[19] Such learning could also trickle up to parents and grandparents, eventually spreading cyber hygiene to the Latvian population.

For all age groups, Latvia recognizes its 3 million citizens must be vigilant. A core pillar of their strategy for vigilance is to develop home-grown talent and tap into existing networks of individuals to turn cyber sleepers into cyber soldiers.

16. Data Security Solutions, "Securing Cyber Space."

17. *Cyber Security Strategy of Latvia: 2014–2018.*

18. Gederts Gelzis, "Cyber Defence Unit Launch," DW (website), 2014, https://www.dw.com/en/latvia-launches-cyber-defence-unit-to-beef-up-online-security/a-17471936.

19. LATO Latvian Transatlantic Organisation, "Estonian Attacks Were Wake-up Call for Us," March 12, 2012, YouTube video, 6:14, https://www.youtube.com/watch?v=Jg8IADVeNis&list=PL194DD043B0884979.

Institutionalizing Knowledge

Latvia has instituted the National Information Technology Security Council to institutionalize its cyber strategy by developing cybersecurity policy at a national level. While discussed earlier in a description of CERT.LV, Latvia's policy, while written nationally, is implemented by specific institutions in the public and private sectors.

This implementation strategy of institutionalizing knowledge has four layers. First, to develop and motivate cyberspace security knowledge, researchers, innovators, and opinion leaders to collaborate in academic environments to develop reports, white papers, and educational content at research conferences. These works are then spread to higher education and professional education professors to create specializations and develop deeper expertise at an educator level. Third, students and educational institutions communicate this research into general knowledge that finally can be used to inform all users in society of basic cyber skills. In moving from academics to professors to students to society, Latvia's strategy is focused on targeting relevant and actionable knowledge at each level of the public.

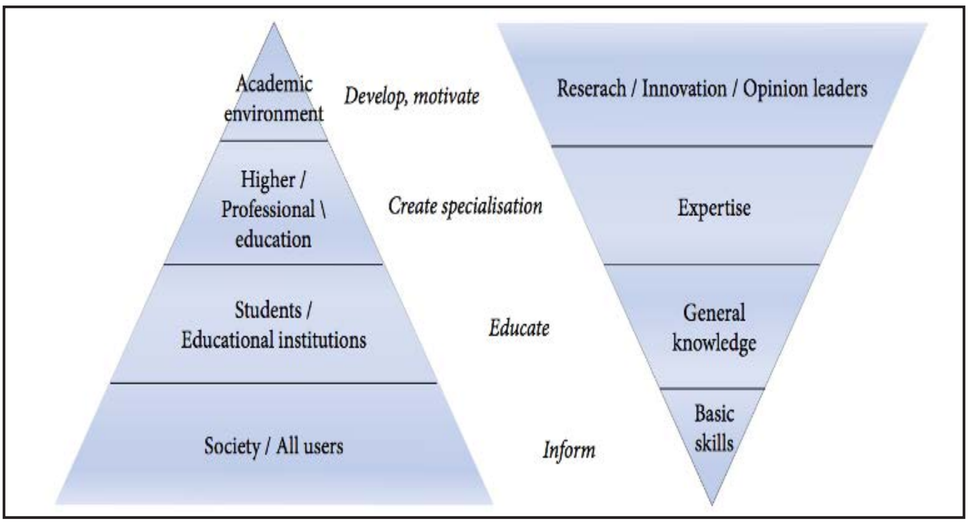

Figure 12-2. Level of cyberspace security knowledge according to the target audience

Ultimately, Latvia's cybersecurity is inherently tied to its neighbors and allies. These three investment areas of partnership, public education, and knowledge creation are particularly Latvian and built into its strategy that is designed to protect Latvia's 5G/IoT infrastructure and electrical grid.

Latvian Electrical Grid

Latvia and Estonia have long been considered the "stars" of the transition from socialism to the market economy. Both countries quickly reached development levels comparable to Central European countries just decades after cutting ties with the USSR. Despite these changes, there are still remnants of the old system. Much of the Latvian electricity grid and rail system is connected to Russian infrastructure. Through legal and technical changes, however, Latvia is on pace to reach independence from Russia by 2025 with systems estimated to offer 700 megawatts of capacity.[20] The process requires completion of a second interconnection between Poland and Lithuania, which is still under construction.[21]

Until 2017, the prevailing technology for the Latvian electrical grid was the BRELL Network, an agreement between Belarus, Russia, Estonia, Latvia, and Lithuania for parallel energy systems in those countries.[22] While a reliable technology, the risk was that all of the Baltic states still had much of their electricity grid connected to Russia. Gazprom (the Russian state-owned energy group) was one of the major players in providing and managing this energy.[23] Intrinsically, it was linked to the Russian government, and there was little confidence from the global markets that Gazprom could maintain a healthy market economy devoid of favoritism or politics. This reexamination revealed a core weakness in the Latvian system—what could the Baltic states do to shift dependence away from Russia to themselves or Western Europe?

Starting as early as 2013, Latvia was moving to leave BRELL and integrate with the EU energy networks to ensure broader energy security. The goal now is to create infrastructure projects with Sweden, Poland, and Lithuania to reduce Russian dependence through investment in and the operation of the ENTSO-E (the Western European counterpart to the BRELL

20. Alissa de Carbonnel and Andrius Sytas, "Baltic States to Decouple Power Grids from Russia, Link to EU by 2025," Reuters (website), June 28, 2018, https://www.reuters.com/article/us-baltics-energy-eu-russia/baltic-states-to-decouple-power-grids-from-russia-link-to-eu-by-2025-idUSKBN1JO15Q.

21. LETA/TBT Staff, "Latvia Would Be Ready to Withdraw from Russian-Belarusian Power Grid Already Today, but There Are Physical Limitations – Karins," *Baltic Times* (website), April 13, 2022, https://www.baltictimes.com/latvia_would_be_ready_to_withdraw_from_russian-belarusian_power_grid_already_today__but_there_are_physical_limitations_-_karins/.

22. Leonid Karabeshkin, "The Baltic Withdrawal from BRELL: An Economic Necessity or a Political Decision?," Energy Collective Group (website), August 21, 2017, https://energycentral.com/c/ec/baltic-withdrawal-brell-economic-necessity-or-political-decision.

23. Rafael Leal-Arcas, Filipa Santos, and Danai Papadea, "Energy, Electricity and Smart Grids in Latvia and Portugal – Developments and Concerns," *Kentucky Journal of Equine, Agriculture, & Natural Resources Law* 12, no. 3 (February 2020), https://uknowledge.uky.edu/kjeanrl/vol12/iss3/2/.

Network). The market at the wholesale level would then be integrated "directly with the markets of Estonia and Lithuania (the Baltic states) as well as with those of Finland, Denmark, Norway, and Sweden (the Scandinavian or Nordic countries)."[24] Another initiative Latvia has invested in is the Baltic Energy Market Interconnection Plan (BEMIP), "an initiative between the European Commission, Denmark, Germany, Estonia, Latvia, Lithuania, Poland, Finland, and Sweden (with Norway as an observer) to synchronize the Baltics' grid with the continental European Network by 2025."[25]

With this model comes strength, as Latvia and the rest of the Baltic states integrate further with NATO. Latvia has already seen the benefits. In October 2019, the country signed an agreement with the United States involving the Baltic energy grid's protection from cyberattacks through strategic and technical support. The weakness comes from the same token. In being an international system, Latvia is always (and for the foreseeable future will be) reliant on other countries. Since Latvia struggles to educate its population on cybersecurity, this dependence on the EU may be detrimental in the long-term.

For Latvia, the modernization and digitization of the electrical grid has been a broader part of Latvia's strategy to become a more renewable energy economy. Moreover, in becoming this electrical economy of the future, the country has invested significant resources in developing IoT and connected smart-city solutions.

Latvian 5G and IoT

With the rise of an independent electrical grid comes the use of more sophisticated electrical technologies like smart metering, utility network monitoring, remotely controlled streetlights, smart waste management, and other city-level services. As described by Kerli Gabrilovica, chief development and marketing officer of Latvia Lattelecom, "The new infrastructure will allow smart devices to be connected to a single network . . . Latvia's capital has many advantages for introducing new technologies." These innovations and others will be protected by Latvia's smart-grid task force that was established in 2017.[26]

24. Leal-Arcas, Santos, and Papadea, "Energy, Electricity, and Smart Grids."

25. Leal-Arcas, Santos, and Papadea, "Energy, Electricity, and Smart Grids."

26. Leal-Arcas, Santos, and Papadea, "Energy, Electricity, and Smart Grids."

The hope is this technology and the proliferation of IoT smart devices generally will open the possibility for consumers to use interconnected devices seamlessly in their daily lives. For consumers concerned about privacy, Latvia has been a leader in data-privacy adoption. In July 2018, Latvia became the first Baltic nation to adopt legislation regarding the EU's General Data Protection Regulation (GDPR) by enacting the Law on Personal Data Processing. Thus, Latvians have confidence knowing that while using IoT devices their data will be gathered, processed, and stored in an ethical manner. If not, the Data State Inspectorate of Latvia (DSI) is the authority responsible for enforcement.

In spite of this well-thought-out system of check, protections, and balances, Latvia still faces weaknesses in the cybersecurity due to the IoT and 5G systems they hope to employ. As described by Rafael Leal-Arcas, Filipa Santos, and Danai Papadea of the University of London: "The proliferation of IoT smart devices has opened many possible routes through which the function of a grid can be compromised: electric vehicles, smart meters, thermostats, and home appliances all could potentially be vulnerable access points of targeted smart grid."[27] In seeing every node as a potential point of entry to the grid, Latvia is exposing itself to an infinite number of attacks as it promotes more connected cities by establishing technology innovations like the LoRaWAN network.[28]

Recommended Systems, Tools, Procedures, and Mitigation Plans

In the last decade, Latvia has recognized the growing importance of anticipating cyber challenges, educating the Latvian public, and anticipating the future development of 5G, IoT, and the electrical grid. Moving forward, however, Latvia's security system will also need to begin developing mitigation plans and strategies for the future.

In the theory of applied deterrence, countries must rely on more than just reactive military power or force. Through a combination of social dimensions, prioritizations, and joint initiatives, countries can develop mitigation strategies to prevent or avoid issues before they arise. In the context of cybersecurity, examples of these mitigation and early warning systems include public-warning systems (for example, tsunami warning

27. Leal-Arcas, Santos, and Papadea, "Energy, Electricity, and Smart Grids."

28. Zenobia Hegde, "Activity Delivers Two New Nationwide LoRaWAN IoT Networks, Partnering Levikom in Estonia and Lattelecon in Latvia," IoTnow, February 16, 2017.

systems), community warning systems (for example, through smart city developments), canary honeypots (for example, digital canaries in the coal mine), and most recently machine-learning systems. [29]

As described by Lukas Milevski, a Baltic Sea fellow at the Eurasia Program at the Foreign Policy Research Institute, Latvia's mitigation plans revolve around "four pillars of national defense: its armed forces, total defense (which comprises the societal dimension of defense), NATO collective defense, international cooperation (including alliance cooperation within NATO or the EU), bilateral military cooperation (especially with the United States), and working with non-NATO partners (such as Georgia and Ukraine)."[30] Generally, this strategy reflects the public-private-international partnership referenced earlier.

As Milevski continues, the aim of these systems is to "prioritize early warning systems to strengthen Latvia's capabilities to detect and resist surprise attack; command and control systems that are resilient against electronic warfare; and overall military readiness, including for the *Zemessardze*, Latvia's National Guard."[31] As a supplement to this existing infrastructure, I propose three additional formulations:

> **1. Investment in proactive cybersecurity.** Latvia should invest more deeply in education and joint-presence priorities with other NATO allies. As described in a September 2019 report for the 100-person Latvian parliament, "Permanent presence of the allied forces strengthens deterrence, closer integration with NATO defence structures and armed forces, facilitates reception of the allied forces and their response if necessary, as well as strengthens NATO defence positions in the Baltic Region at large."[32] Both in and out of cyberspace, it is in the best interest of Latvia to increase the presence and interoperability of more resourced and experienced partners given its underdeveloped mitigation plans. The aims of these programs would be to create a proactive rather than reactive cybersecurity position.

29. Harsha Kalutarage et al., "Early Warning Systems for Cyber Defence," *Lecture Notes in Computer Science* (New York: Springer, May 2016), https://doi.org/10.1007/978-3-319-39028-4_3.

30. Lukas Milevski, "Latvia's New State Defense Concept," Foreign Policy Research Institute (website), June 25, 2020, https://www.fpri.org/article/2020/06/latvias-new-state-defense-concept/.

31. "Valsts Aizsardzibas Koncepcija," Ministru Kabineta, Riga, 2020.

32. "Par Nacionālās drošības koncepcijas apstiprināšanu," Saeima, September 26, 2019.

2. Training the next generation of cyber experts. While Latvia has well-established plans for educating its public from preschool to later life about cyber hygiene, there is no international pipeline to train industry experts. Through partnerships with CERT.EE and CERT.LT (the Estonian and Lithuanian versions of CERT.LV), Latvia can create a regional education ecosystem to train the next generation of cybersecurity thought leaders. Since its establishment, CERT.LV's ability to identify cyberattacks performed by foreign intelligence and security services has improved significantly in isolation. Through collective effort in the Baltic region to "develop the ability to monitor the content created on the Internet by users with the purpose of identifying the targeted activities directed against national security of Latvia and preventing them, as well as actively work on reduction of response time and improvement of proactive ability to prevent threats."[33]

3. Investment in critical infrastructure. Latvia should accelerate its development and independent investment into critical infrastructure. While Latvia contributes 2 percent of its GDP to defense (as recommended by NATO) and has developed partnerships with the regional BRELL network, these steps alone are not sufficient for a mitigation strategy. One core precondition for the resilience of the national information space is the ability of the society and state to be aware of risks and threats to the public space in house and to respond to them in real time.[34] In the context of energy security, Latvia can also begin to build up energy reserves (the Latvian government has already begun exploring the potential of the Inčukalns's underground gas storage facility), promote the use of renewable energy resources (primarily in the agriculture and transport sectors), and develop energy-monitoring systems to flag large deviations from the average.

33. "Par Nacionālās drošības."

34. "Par Nacionālās drošības."

Conclusion: Beyond the D'yavol

As Latvia nears the second quarter of the twenty-first century, it is able to lean in to the West despite historical ties to the east. As institutions like CERT.LV, the Latvian parliament, and BRELL continue to develop skills and technologies, Latvia is evolving its ability to expel the devil in the pulpit. Latvia's population will continue to be prepared for cyber intrusions if the Latvian government continues to focus on public-private-international partnerships, state-wide education, and institutionalized knowledge sharing.

In addition to its armed forces, total defense, NATO collective defense, international cooperation, bilateral military cooperation, and working with non-NATO partners, Latvia must continue to strengthen its 5G, IoT, and electrical grid to address challenges posed by more sophisticated cyber actors. As proposed, such strengthening could come through joint-presence priorities with NATO allies, international education pipelines, and deeper investment into upgrading critical infrastructure. Latvia's cyber defense is unique, but it offers opportunities for growth beyond the *D'yavol*.

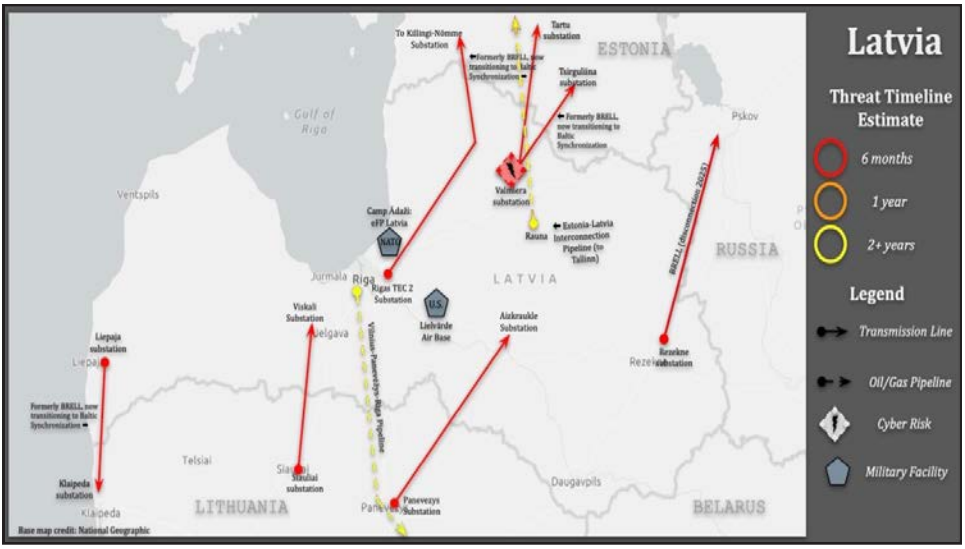

Figure 12-3. Map of Latvia's threat timeline estimate (6 months indicates likely attack vector in 2022, 1 year by 2023, 2+years by 2024 or later)

Credit: Ryan Fisk and Lucas Cox

Location	Reason for Threat Priority and Timeline
Baltic Synchronization Transmission Lines	The transmission lines that are transitioning from BRELL to coupling with the EU are a direct effort to reduce reliance on Russia. It is very likely significant attempts to interfere with the transition will take place over the next two years.
Valmiera Substation	The Valmiera substation is connected to two Baltic Synchronization transmission lines from Estonia. A single attack here, especially in the current transition period, would severely degrade electricity import capabilities.
Estonia-Latvia Interconnection Pipeline	As the Baltics seek to diversify away from Russian gas supplies, the Estonia-Latvia Interconnection Pipeline will be of increasing importance to Latvia's energy security and a likely target for intervention.
Vilnius-Panevežys-Riga Pipeline	The pipeline's importance for Latvia's energy independence from Russia will make it a likely target for the next two years.

Select Bibliography

Hegde, Zenobia. "Activity Delivers Two New Nationwide LoRaWAN IoT Networks, Partnering Levikom in Estonia and Lattelecon in Latvia." IoTnow. February 16, 2017.

Ilves, Luukas Kristjan. "Cyber Security Trends and Challenges: Latvian and Estonian Experience." February 29, 2012. YouTube video. 2:30. https://www.youtube.com/watch?v=Jg8IADVeNis&list=PL194DD043B0884979.

Kalutarage, Harsha, et al. "Early Warning Systems for Cyber Defence." *Lecture Notes in Computer Science*. New York: Springer, May 2016. https://doi.org/10.1007/978-3-319-39028-4_3.

Karabeshkin, Leonid. "The Baltic Withdrawal from BRELL: An Economic Necessity or a Political Decision?" Energy Collective Group (website). August 21, 2017. https://energycentral.com/c/ec/baltic-withdrawal-brell-economic-necessity-or-political-decision.

Kaža, Juris. "Baltics to Cut Electricity Links to Russia, Disagree on Power Trading until Then." Medium (website). July 9, 2020. https://juriskaza.medium.com/baltics-to-cut-electric-links-to-russia-disagree-on-power-trading-until-then-b7f7f546c983.

LATO Latvian Transatlantic Organisation. "Estonian Attacks Were Wake-up Call for Us." March 12, 2012. YouTube video. 6:14. https://www.youtube.com/watch?v=Jg8IADVeNis&list=PL194DD043B0884979.

Latvian Ministry of Defence. *Cyber Security Strategy of Latvia: 2014–2018*. Riga, LV: European Union Agency for Cybersecurity, 2018. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss.

— 13 —

Lithuania

Thomas A. Elmore

ABSTRACT: Lithuania was one of the few European countries that exported energy instead of importing it from foreign sources while it was part of the Soviet Union. Once it applied for membership in NATO following the fall of the Soviet Union, it was forced to shut down the nuclear power plant supplying most of the nation's energy and import energy from Russia. Lithuania has taken significant steps to reduce Russia's monopoly on energy by forming alignments with other neighboring nations (such as Poland) and announced intentions to withdraw from the BRELL network. Russia has launched cyberattacks on Lithuanian infrastructure regularly to keep the country in the sphere of Russian influence. Lithuania has constructed a comprehensive, coordinated cyber defense strategy to safeguard against predatory Russian interference, though there has been an increase in cyber threats since the Russian invasion of Ukraine. As a country bordering the Russian Kalingrad exclave which houses Russian nuclear weapons, Lithuania is in an especially vulnerable position during the Ukraine conflict.

Keywords: LitPol, NordBalt, BRELL, Russian cyberattacks, energy independence, Baltic Cyber Shield, Kaunas institute of technology, coordinated cybersecurity, Klaipėda

Introduction

Since the dissolution of the Soviet Union, Lithuania has aligned with the North Atlantic Treaty Organization (NATO) and European Union (EU) to improve its security and economy, while reducing dependence on Russia for the same. Energy security during this transition remains a concern for Lithuania's government. The International Energy Agency (IEA) defines *energy security* as "the uninterrupted availability of energy sources at an affordable price."[1] Lithuania currently struggles to achieve both conditions set by the IEA for energy security.

A condition for Lithuanian entry into the EU was the decommissioning of the Ignalina Nuclear Power Plant that provided 77 percent of the country's electricity requirements. The decommissioning of the plant transitioned Lithuania from a net exporter of energy to a net importer.[2] To offset this shortfall, Lithuania had to increase the import of energy from Russia.[3] In 2012, 63 percent of energy imports came from Russia.[4] This dependence was not ideal for Lithuania as they sought to decouple their energy grid from Russia and connect with the EU market.[5] As the country continues this transition, it faces threats from malign cyber actors, most likely from Russia, to the industrial control systems of the electrical grid and renewable energy generation infrastructure as well as disinformation attacks to decrease confidence in these systems and the government. Cyberattacks on either system would require Lithuania to increase, not decrease, dependence on Russian energy supplies.

To lessen Russian influence on the availability of energy, Lithuania undertook two projects. In 2015, Sweden and Lithuania jointly commissioned the NordBalt transmission line from Nybro, Sweden, to Klaipėda, Lithuania. At its peak, this asynchronous line will provide 700 megawatts of electricity.[6] That same year, Poland and Lithuania launched the LitPol Link that can provide up to 500 megawatts of electricity.[7] These two projects reduced dependence on Russian energy imports but failed to provide the 1,830 megawatts needed daily by Lithuania. While significantly reducing the ability of Russia to manipulate the supply of energy for political gain,

1. International Energy Agency (IEA), "Energy Security: Ensuring the Uninterrupted Availability of Energy Sources at an Affordable Price," updated December 2, 2019, https://www.iea.org/areas-of-work/ensuring-energy-security.

2. US Energy Information Administration, "Lithuania," updated March 2013, accessed April 27, 2021, https://www.eia.gov/international/analysis/country/LTU.

3. Rokas Masiulis, "Lithuania's Energy Sector Development Trends" (presentation, Baltic Utilities Forum, Riga, April 9, 2015), 2, http://www.lsta.lt/files/seminarai/2015-04-09_Ryga/03.-ey-bus-2015-rokas-masiulis.pdf.

4. "Lithuania," Organisation for Economic Co-operation and Development (website), n.d., accessed April 29, 2021, https://www.oecd.org/countries/lithuania/.

5. Simon Hoellerbauer, "Lithuania Moves to Bolster Electricity Security," Foreign Policy Research Institute (website), March 23, 2016, https://www.fpri.org/article/2016/03/lithuania-moves-bolster-electricity-security/.

6. "NordBalt: Interconnecting Grids," ABB Group (website), n.d., accessed April 28, 2021, https://library.e.abb.com/public/e97556106e37e7aec1257dcf004f589a/POW0073%20Rev%201.pdf.

7. "LitPol Link," Litgrid (website), n.d., accessed April 21, 2021, https://www.litgrid.eu/index.php?lang=2.

these transmission lines are a security concern.[8] Losing either input significantly exacerbates the energy shortfall Lithuania faces daily.

Another energy sector Russia previously manipulated was the natural-gas market. The monopoly held by state-owned Gazprom over the Russian natural-gas market had been a key bargaining tool used previously between Russia and Europe.[9] To disrupt this monopoly, Lithuania constructed the Klaipėda LNG terminal. This terminal reduces Lithuanian dependence on Russian natural gas by approximately 33 percent. Unfortunately, similar to the NordBalt and LitPol Link transmission lines, this single point of failure presents a great risk to Lithuania's goal of energy security.[10]

Initiatives like NordBalt, LitPol Link, and the Klaipėda LNG terminal decreased dependence on Russia energy sources. In 2016, Lithuania only imported 33 percent of its energy requirements from Russia. Lithuania is still dependent on other nations, however, to meet its energy demands. Current estimates show Lithuania must import approximately 70 percent of its energy requirements.[11]

In 2019, Lithuania energy supplies depended heavily on oil, natural gas, and coal. These nonrenewable sources accounted for 75.8 percent of energy supply. Renewable energy sources like biofuels and waste, hydro, and wind generated the remaining 24.2 percent.[12] The average price for electricity rose by 14.3 percent, second only to the Netherlands in the European Union.[13] Recognizing how the combined dynamics of reliance on external sources and rising prices are problematic to long-term energy security, Lithuania set a goal to produce 70 percent of its electrical demand by 2030 and 100 percent by 2050.[14] Since the nation has relatively few natural resources, Lithuania's focus is on the development of renewable resources.

8. Hollerbauer, "Lithuania Moves."

9. Members of the Ukrainian Parliament, "Putin's Pipeline Is a Strategic Weapon. It Must Be Stopped," *Atlantic Council* (blog), October 13, 2020, https://www.atlanticcouncil.org/blogs/ukrainealert/putins-pipeline-is-a-strategic-weapon-it-must-be-stopped/.

10. Hollerbauer, "Lithuania Moves."

11. "Lithuania 2021: Energy Policy Review," IEA (website), n.d., https://www.iea.org/reports/lithuania-2021.

12. "Lithuania Energy Supply by Total Energy Supply by Sector Chart, 2020," IEA (website), n.d., accessed April 9, 2021, https://www.iea.org/countries/lithuania.

13. Eurostat, "Household Energy Prices in the EU Increased Compared with 2018" (news release), May 7, 2020, https://ec.europa.eu/eurostat/documents/portlet_file_entry/2995521/8-07052020-AP-EN.pdf/2c418ef5-7307-5217-43a6-4bd063bf7f44.

14. "Lithuania 2021," 115.

Lithuania invested in renewable resource production, rising from 3.1 percent of total energy consumption in 1990 to 33.6 percent in 2017. While all subsets of renewable energy sources saw growth over this time, wind-energy generation increased the most. When it began in 2004, it created only 1 gigawatt hour of energy. Most recent figures from 2019 show wind power created 1,499 gigawatt hours of energy.[15]

The deals to export 3.8 terawatts of energy over a 10-year period to Estonia from Lithuanian wind farms, and with Siemens to construct a proof-of-concept storage plant for energy generated by renewable assets, demonstrate Lithuania's commitment to energy security.[16] With its development and expansion of renewable energy sources coupled with other initiatives, Lithuania seeks to establish itself as the new energy hub in the Baltic states and surrounding region.

Consumption by Sector

Since 2000, demand for electricity has consistently risen in the industrial, residential, commercial, and public-service sectors while remaining flat in the agricultural, forestry, and transportation sectors. The industrial sector requires 35.4 percent of Lithuania's electricity, followed by the commercial and public sector at 33 percent and the residential sector at 28.7 percent. The agriculture and transportation sectors make up less than 3 percent of Lithuania's electricity demand. Lithuania uses approximately 60 percent of its natural gas for non-energy-related requirements with the industrial, residential, and commercial sectors accounting for the remaining 40 percent.[17] These figures outline the impact malicious cyber intrusions would have on Lithuania.

Threats

The Baltic nations find themselves on the frontline of a battle for control between Russia and NATO and have done so long before Russia's 2022 invasion of Ukraine. Russia desires to retain control over the region and to prevent increased NATO and EU control. In April 2015, Estonia, Latvia, and Lithuania announced their intent to disconnect from the Belarus,

15. IEA, "Lithuania Energy Supply."

16. Sten Hankewitz, "Estonian Energy Company to Purchase Electricity from a Danish Energy Developer," Estonian World (website), April 14, 2021, https://estonianworld.com/business/estonian-energy-company-to-purchase-electricity-from-a-danish-energy-developer/.

17. IEA, "Lithuania Energy Supply."

Russia, Estonia, Latvia, and Lithuania (BRELL) network and connect to EU energy networks.[18] Russia has three primary concerns with the separation of Lithuania and other nations from the BRELL network.

First, the Baltic states would no longer have to pay Russia to maintain the network, resulting in less revenue for Russia. Second, Russia would lose a tremendous leverage over neighboring states from this loss of control over energy supplies. Russia would have less direct access to alter energy supply to support its end state in the region. Third, a transfer of networks by the Baltic nations would force Russia to either construct a new network to support Kaliningrad where their Baltic fleet is based or make the region energy self-sufficient. Both options are costly, and Russia previously indicated it would attempt to force the EU and Baltic states to fund either.[19]

As a significant importer of energy, Lithuania faces a tremendous amount of risk as it disconnects from BRELL. Russian naval ships harassed construction of the NordBalt undersea transmission line.[20] In addition to physical engagements, Lithuania faces threats from malicious cyber actors to attack in the electrical, natural-gas, and renewable resources sectors. The loss of any component would negatively impact Lithuania's energy security. The tremendous cost required to transition from the BRELL network to synchronous EU networks creates several opportunities for exploitation. Russia understands these vulnerabilities and in 2015, following the announcement of Lithuania's intent to separate from the BRELL network, launched distributed denial-of-service attacks at Baltic electricity grids in an attempt to find vulnerabilities for future exploitation.[21]

Intrusions into Lithuania's infrastructure occurred in 2020 when cybercriminals accessed over 20 public-sector websites, spreading disinformation on the eve of a Lithuanian government transition.[22] Earlier in 2020, NordBalt became inoperable without an explanation, halting 700 megawatts of power (or almost 40 percent of Lithuania's daily

18. Barbara Lewis and Gederts Gelzis, "Baltics May Risk More Russia Tension with Europe Power Grid Plan," Reuters (website), April 14, 2015, https://www.reuters.com/article/baltic-russia-energy/baltics-may-risk-more-russia-tension-with-europe-power-grid-plan-idUSL5N0W75BZ20150414.

19. Hollerbauer, "Lithuania Moves."

20. Hollerbauer, "Lithuania Moves."

21. Stephen Jewkes and Oleg Vukmanovic, "Suspected Russia-Backed Hackers Target Baltic Energy Networks," Reuters (website), May 11, 2017, https://www.reuters.com/article/us-baltics-cyber-insight/suspected-russia-backed-hackers-target-baltic-energy-networks-idUSKBN1871W5.

22. Sarah Coble, "Lithuania Suffers 'Most Complex' Cyber-attack in Years," Infosecurity (website), December 16, 2020, https://www.infosecurity-magazine.com/news/lithuania-cyberattack/.

requirements).[23] The precarious nature of Lithuania's energy system can be exploited through a number of activities by cyber actors. This trend is likely to worsen as Russia increases its hybrid warfare against the Baltic states as part of its expansionist policies in what it considers its near abroad. Figure 13-1 highlights the major locations where Lithuania could face disinformation and attacks on industrial control systems.

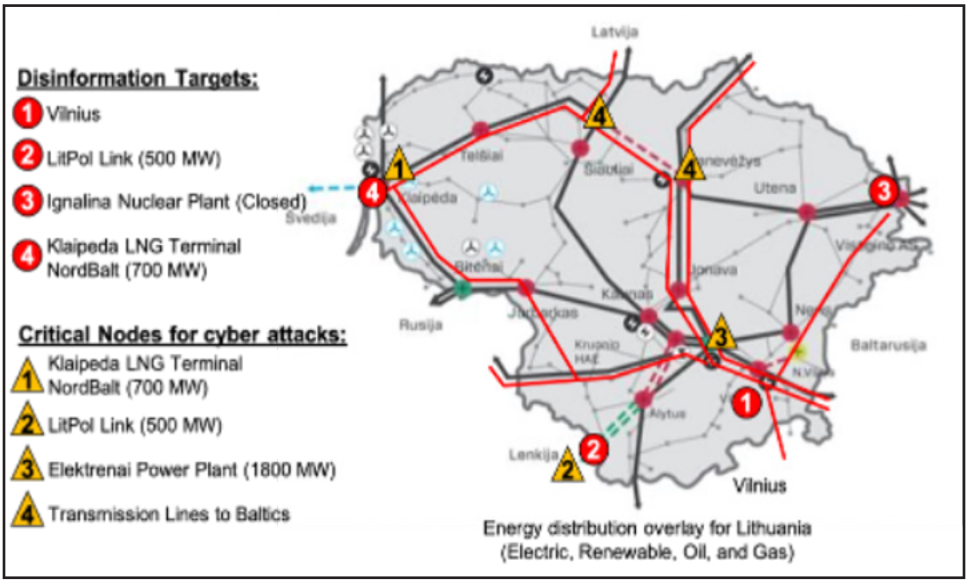

Figure 13-1. Energy distribution overlay for Lithuania

Source: Stasys Backaitis, "Are All Lithuanian Energy Problems Now Resolved?," October 2015, VilNews (website), n.d., accessed May 10, 2021, http://vilnews.com/2015-10-are-all-lithuanian-energy-problems-now-resolved.

Russian cyber actors use disinformation attacks to create confusion and reduce trust in a government. There has been an increase in Russian disinformation efforts surrounding the 2022 Ukraine invasion. In March 2022, the Lithuanian government tightened its national state of emergency, strengthening the state's authority to remove "pro-Russian propaganda" on social media.[24] Once confidence is decreased, any follow-on attacks will have significantly more impact. Highlighted in figure 13-1 are the four most likely targets for disinformation attacks. The first target is the government of Lithuania, against which Russia has allegedly conducted disinformation

23. Government of Lithuania, "Baltic Power Line Disconnects, Triggering Emergency Operations," June 8, 2020, https://www.lrt.lt/en/news-in-english/19/1186395/baltic-power-line-disconnects-triggering-emergency-operations.

24. Lisa Abend, "Meet the Lithuanian 'Elves' Fighting Russian Disinformation," *TIME* (website), March 6, 2022, https://time.com/6155060/lithuania-russia-fighting-disinformation-ukraine/.

attacks. In December 2020, following their elections, cybercriminals conducted a significant disinformation campaign spreading disinformation on multiple government networks on multiple topics, from excessive troop drafting to corrupt Polish officials. In the same attack, cybercriminals alleged corruption at Siauliai airport, the location for NATO's Baltic air policing. Sowing seeds of division between Lithuania and the EU at Klaipėda where the LNG terminal and terminus for NordBalt are or toward the LitPol Link would be another avenue for disinformation attacks.[25] Russia could also conduct disinformation attacks centered on the safety of the closed nuclear power plant at Ignalina. Russian actors already carried out a similar disinformation campaign in Poland centered on a leaking nuclear reactor in Lithuania.[26]

In addition to disinformation attacks, Russian cyber actors could conduct attacks on the industrial control systems of key electrical infrastructure. With minimal redundancy in its system, any successful attack would significantly hinder Lithuania's ability to meet daily energy demands. A shutdown of the Klaipėda terminal would impact LNG and electricity imports. Any shutdown to the LNG terminal leaves only Russia as a potential backfill. LitPol Link provides roughly 30 percent of daily demand and would have a similar impact as when NordBalt was inoperative in December 2020. As Lithuania modernizes the Elektrenai Power Plant to meet EU standards, an attack would double the effect. First, there would be a loss of power generation. Second, the costly improvements to meet EU standards could be damaged, requiring repair or replacement, and increasing the total bill. Last, disabling the transmission lines into Latvia would hinder Lithuania's goal to be the regional energy hub for the Baltic states. Realizing the amount of risk posed by malicious cyber intrusions in the electrical and renewable energy grids, along with their LNG terminal, Lithuania has proactively addressed these risks through multiple avenues.

Lithuanian Cyber Efforts

In 2018, the International Telecommunications Union's Global Cyber Index gave Lithuania its highest score in its legal and organizational

25. Coble, "Lithuania Suffers."

26. Associated Press (AP), "Polish State Websites Hacked and Used to Spread False Info," AP News (website), March 17, 2021, https://apnews.com/article/europe-poland-eastern-europe-lithuania-nuclear-waste-424dd97778b3d2046bc1cb61a175f270.

pillars.[27] Lithuania's efforts on cybersecurity resulted in GCI ranking them the fourth-most committed country, behind the United Kingdom, the United States, and France.[28] This cohesive approach enables Lithuania to enact multiple mitigation measures.

The 2018 cybersecurity strategy for Lithuania clearly identifies the Ministry of National Defence as the lead agency for cybersecurity. The strategy also reinforced the relationship between the National Cybersecurity Centre (NCSC) and the Ministry of National Defence. The strategy specified the roles and functions of each, especially of the National Cybersecurity Centre and its components. The NCSC supports the Ministry of National Defence, and this alignment streamlines Lithuania's cybersecurity enterprise. In addition to the development of plans and policies, the 2018 strategy also mandates the Ministry of National Defence organize national cybersecurity exercises.[29] Lithuania does this with the Baltic Cyber Shield and Amber Mist exercise series.

Baltic Cyber Shield, a proof of concept in 2008 and first executed in 2010, is an annual cyber-defense exercise with the major goal of increasing international, national, and public- and private-industry cooperation. The initial scenario had six teams defend critical power-generation information technology systems against progressively more complicated attacks.[30] The National Cybersecurity Centre and Kaunas University of Technology cohost the exercise, further increasing public and private-sector cooperation. In 2020, the exercise focused on execution of the National Cyber Incident Management Plan and reacting to the myriad different cyber events the National Cybersecurity Centre handles daily.[31] In coordination with this national-level exercise, the Lithuanian Armed Forces hosts Amber Mist.

Amber Mist improves interoperability between Lithuania and other NATO partners in the event of a cyberattack. Amber Mist began in 2014

27. International Telecommunication Union (ITU) Publications, *Global Cybersecurity Index* (*GCI*) *2018*, (Geneva, ITU, 2019), 31, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

28. ITU Publications, *GCI 2018*, 16.

29. Government of the Republic of Lithuania, *Resolution on the Approval of the National Cyber Security Strategy*, no. 818, August 13, 2018, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/LRV+818+National+Cyber+Security+Strategy+%28Lithuania%29.pdf.

30. Cooperative Cyber Defence Centre of Excellence (CCDCOE), *Baltic Cyber Shield Cyber Defence Exercise 2010 After Action Report*, (Tallinn, EE: CCDCOE, 2010), https://ccdcoe.org/uploads/2018/10/BCS2010AAR.pdf.

31. Ministry of National Defence Republic of Lithuania, "Stakeholders of Public and Private Sectors of Lithuania Train to Manage Cyber-incidents" (press statement), October 21, 2020, https://kam.lt/en/news_1098/current_issues/stakeholders_of_public_and_private_sectors_of_lithuania_train_to_manage_cyber-incidents.html.

and runs simultaneously to Cyber Shield to add another layer of realism to Lithuania's exercises by providing real-world scenarios. In 2020, Amber Mist divided participants into friendly, enemy, or neutral teams. The friendly teams actively defended their networks from attacks by the enemy team. The neutral team served as a real-world arbiter of the success of the friendly or enemy teams. If the enemy team's attack succeeded, the neutral team would notice a degradation in operations. If the friendly team succeeded, the neutral team would notice no significant changes.[32] This commitment to realistic training scenarios demonstrates the emphasis Lithuania applies to its cybersecurity. The application of the strategy and lessons learned from these exercises led Lithuania to create a regional cyber center in Kaunas.

Developed in cooperation with the United States and the Kaunas Institute of Technology, the regional cyber center in Kaunas would command the EU Rapid Response Cyber Force, part of the EU's Permanent Structured Cooperation (PESCO). Through the State Partnership Program under the US National Guard, Lithuania has coordinated with the Pennsylvania National Guard to support the center. Support includes US personnel manning positions.[33] This partnership was on display during Lithuania's elections in 2020 when 10 members of the Pennsylvania National Guard's cyber defense team remotely provided support to the Kaunas Center. Because of COVID-19 protocols, the US servicemembers remained in Pennsylvania but integrated their operations with Kaunas to provide cybersecurity for the election.[34]

Another part of this project is the development of an early warning system to notify personnel at the center in the event of an attack. Lithuania allocated 430,000 euros from 2019–21 on this system to use artificial intelligence to identify and analyze incoming attacks. Once analyzed, the system would send reports to the operators for further action.[35] While this is a minor amount of funding compared to other nations' expenditures, it is a necessary step. Lithuania has taken many strides toward cybersecurity and energy security, and there are opportunities for even more improvement.

32. Giedrius Saulenas, "Amber Mist 2020 Cyber Exercise," Saulenas (website), September 29, 2020, https://saulenas.com/Amber-Mist-Cyber-Exercise/.

33. Saulius Jakučionis, "Lithuania to Bolster Cyber Security – Early Warning System, Additional Cybersecurity Center," July 3, 2019, https://www.lrt.lt/en/news-in-english/19/1075107/lithuania-to-bolster-cybersecurity-early warning-system-additional-cybersecurity-center.

34. Keith Hickox, "Pennsylvania National Guard Cyber Branch Supports 2020 Election," November 3, 2020, https://www.dvidshub.net/news/382300/pennsylvania-national-guard-cyber-branch-supports-2020-election.

35. Jakučionis, "Lithuania to Bolster Cybersecurity."

Recommendations

Currently, Lithuania faces numerous threats to its energy security. Adopting the following recommendations would alleviate some of these threats.

1. **Development of sovereign energy production.** Lithuania must continue to develop internal energy production systems. The lack of fossil fuels means they must utilize renewable resources. The growth over the last 10 years in renewable energy production is a positive first step. Developing internal energy production reduces its dependence on external sources. While Lithuania became the first country to eliminate its dependence on Russian energy imports in April 2022—mostly by increasing its reliance on its LNG terminal in Klaipėda—Lithuania still imports more than 75 percent of its energy, mostly from Norway.[36] This action leaves Lithuania vulnerable under the IEA's definition of energy security concerning uninterrupted access.

2. **Improve regional cyber cooperation.** Lithuania has made great strides in cybersecurity through its encompassing strategy, exercises, and regional cyber center. The country should continue these improvements through closer coordination with the other Baltic states. Under a memorandum of understanding signed in 2015, the Baltic nations agreed to work together on common cyber threats. All parties to the MOU agree that "critical infrastructure that forms the foundation upon which modern society functions is also under threat from cyberspace."[37] The requirements for coordination will increase as Belarus looks to complete its nuclear power plant in the future. Connecting to this energy source brings

36. Samanth Subramanian, "Independence Day: How a Baltic Nation Ended Its Reliance on Russian Gas," Quartz (website), April 11, 2022, https://qz.com/2152999/lithuania-became-the-first-eu-nation-to-stop-russian-gas-imports/.

37. Vytautas Butrimas, "Baltic Cyber Cooperation: Estonia, Latvia and Lithuania Sign a Historic Document to Align Their Cyber Defense Policies," *per Concordiam: Journal of European Security and Defense Issues* (website), July 14, 2016, https://perconcordiam.com/baltic-cyber-cooperation/.

increased risk as Belarus has previously aligned closely with Russia.[38]

3. **Decentralization of energy storage**. Lastly, similar to energy production, Lithuania should decentralize its storage of energy generated by renewable sources to prevent grid disruption. The pilot program with Siemens calls for a centralized location to store energy generated. While a pilot program, any improvement would be a proof of concept for distributed storage that can provide energy throughout the grid while also remaining on separate systems. Already facing the pressure on nonredundant energy generation and importation, Lithuania should start its renewable energy storage concepts with a distributed approach.

Conclusion

As Lithuania moves toward its goal of energy security independent of Russian influence, the country faces many vulnerabilities from cyber intrusions into the electrical grids and renewable energy generation. Lithuania understands the issues it faces and has taken several appropriate steps to limit the ability of outside agencies to impact the country negatively. As a necessary first step, the government has a comprehensive strategy that aligns the national ends with appropriate means. The country has coordinated with many external agencies, to include US Cyber Command and the National Guard Bureau, to augment their personnel with subject-matter experts in many areas and dedicated funding to develop early warning systems to detect intrusions from human and artificial intelligence threats. If Lithuania continues to focus on addressing threats, the transition to a synchronous grid with the European Union will succeed.

38. Andrius Sytas, "Lithuania Stops Baltics Power Trade with Belarus, Russia over Nuclear Plant," Reuters (website), November 3, 2020, https://www.reuters.com/article/litgrid-belarus/lithuania-stops-baltics-power-trade-with-belarus-russia-over-nuclear-plant-idUSKBN27J2CA.

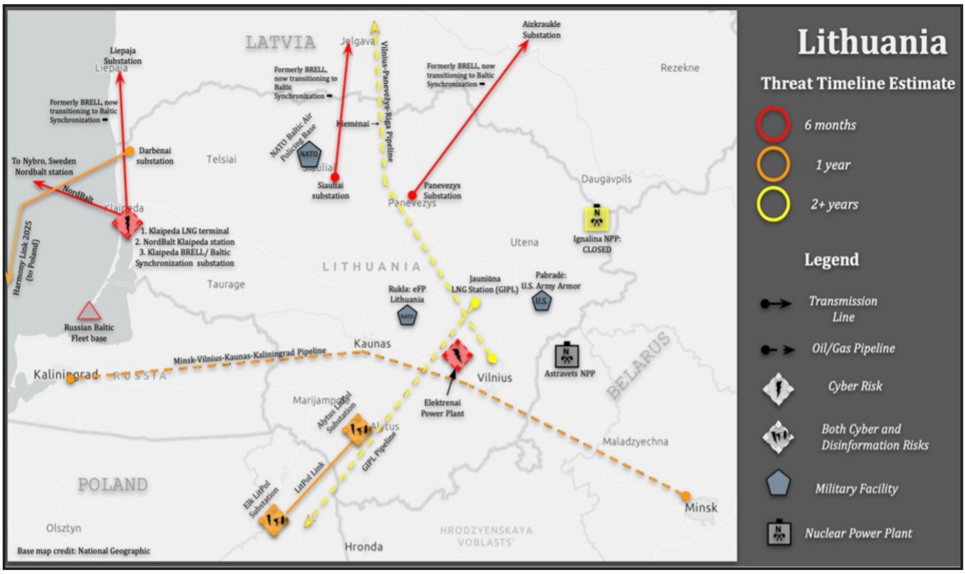

Figure 13-2. Map of Lithuania's threat timeline estimate (6 months indicates likely attack vector in 2022, 1 year by 2023, 2+years by 2024 or later)

Credit: Ryan Fisk and Lucas Cox

Location	Reason for Threat Priority and Timeline
NordBalt, Klaipėda LNG Terminal	Russia already showed its intentions to disrupt NordBalt when its warships harassed NordBalt's construction. The terminal's geographical and geostrategic importance and significance for Lithuanian energy independence could make it a target for the next six months.
Baltic Synchronization Transmission Lines	As the Baltics seek to create an independent power grid before 2025, the transmission lines transitioning to BRELL will remain vulnerable to attack until completion.
LitPol Link	The LitPol Link could be a disinformation operations target as Lithuania reduces electricity dependence on Russia.
Harmony Link	Harmony Link will increase the reliability of the transition from BRELL to the Continental European Synchronous Area once completed in 2025. Intervention to completion could be expected in the year before completion should tensions with Russia increase.
Elektrenai Power Plant	After the closing of the Ignalina nuclear power facility, Elektrenai became one of the main sources of domestic energy production and could remain a target amid tensions for the next six months.
Ignalina Nuclear Power Plant (Closed)	Continue to expect disinformation operations discrediting Lithuania for the next two years following the closure of the nuclear plant.
Vilnius-Panevežys-Riga Pipeline	The pipeline, which is important to Lithuania's energy independence, could be vulnerable to intervention for the next two years.
Jauniūna LNG Station and GIPL Pipeline	An ICS attack on this pipeline within the next two years is possible as Lithuania has turned away from Russian gas supplies.

Select Bibliography

Butrimas, Vytautas. "Baltic Cyber Cooperation: Estonia, Latvia and Lithuania Sign a Historic Document to Align Their Cyber Defense Policies." *per Concordiam: Journal of European Security and Defense Issues* (website). July 14, 2016. https://perconcordiam.com/baltic-cyber-cooperation/.

Cooperative Cyber Defense Centre of Excellence (CCDCOE). Baltic Cyber Shield Cyber Defence Exercise 2010 After Action Report. Tallinn, EE: CCDCOE, 2010. https://ccdcoe.org/uploads/2018/10/BCS2010AAR.pdf.

Government of Lithuania. "Baltic Power Line Disconnects, Triggering Emergency Operations." June 8, 2020. https://www.lrt.lt/en/news-in-english/19/1186395/baltic-power-line-disconnects-triggering-emergency-operations.

Government of the Republic of Lithuania. *Resolution on the Approval of the National Cyber Security Strategy*, no. 818. August 13, 2018. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/LRV+818+National+Cyber+Security+Strategy+%28Lithuania%29.pdf.

Hickox, Keith. "Pennsylvania National Guard Cyber Branch Supports 2020 Election." November 3, 2020. https://www.dvidshub.net/news/382300/pennsylvania-national-guard-cyber-branch-supports-2020-election.

"Lithuania Energy Supply by Total Energy Supply by Sector Chart, 2020." International Energy Agency. (website). n.d. Accessed April 9, 2021. https://www.iea.org/countries/lithuania.

Ministry of National Defence Republic of Lithuania. "Stakeholders of Public and Private Sectors of Lithuania Train to Manage Cyber-incidents." Press statement. October 21, 2020. https://kam.lt/en/news_1098/current_issues/stakeholders_of_public_and_private_sectors_of_lithuania_train_to_manage_cyber-incidents.html.

Members of the Ukrainian Parliament. "Putin's Pipeline Is a Strategic Weapon. It Must Be Stopped." *Atlantic Council* (blog). October 13, 2020. https://www.atlanticcouncil.org/blogs/ukrainealert/putins-pipeline-is-a-strategic-weapon-it-must-be-stopped/.

Saulenas, Giedrius. "Amber Mist 2020 Cyber Exercise." Saulenas (website). September 29, 2020. https://saulenas.com/Amber-Mist-Cyber-Exercise/.

Conclusion: Baltics

The most significant threats to the Baltics stem from their reliance on foreign energy. All three Baltic states have pledged to eliminate their reliance on Russian energy imports completely by the end of 2022, Lithuania being the first to have done so at the time of this publication. All three nations are still connected to Russia and Belarus through the BRELL electric grid. This grid still presents significant security vulnerabilities at a time when the Russian Federation is encroaching dangerously close to NATO's eastern flank, threatening the sovereignty of the Baltic republics. An increase in domestic energy production capabilities and reduction of reliance on foreign power would put the Baltics in a strategic position to defend against Russian intrusions. This goal appears possible as there are already a number of networks in place for the Baltics to receive support from other surrounding NATO nations, which greatly improve their capacity and resilience.

– Case Studies –

Southeastern Europe

Southeastern Europe consists of four nations: Romania, Italy, Greece, and Türkiye. This region faces a more varied threat forecast, with many different types of facilities and energy sources in each nation at risk due to different geographic locations and cyber standards. Each nation has a strategic geographic location, which includes high-value ports to NATO and Russia. In addition, China is making headway in these countries through an increase in foreign direct investment in new technologies, critical infrastructure, and port areas. NATO nation-state territories and mission-critical infrastructure, therefore, are increasingly vulnerable to hybrid attacks.

Italy is unique because Chinese firms have made large investments into the infrastructure to build Italian renewable energy and could be feeding data regarding the use of this infrastructure to the Chinese government. These data could include information regarding infrastructure movements and grid activity, vital elements for Italy's economy, which relies heavily on several strategic ports in the Mediterranean Sea. Much like Italy, Greece has also seen a great deal of Chinese investment in its Ports of Piraeus and Thessaloniki in what appears to be an attempt by the Chinese to carve out an area of influence. This action is seen as very problematic as Greece houses several major joint NATO and US military bases.

Romania and Türkiye have different concerns. Romania is mostly energy independent and has access to the Black Sea via ports on its eastern coastline and is able to exercise autonomy over its power grid and economy. This autonomy has made it a target for Russian cyberattacks as Russia lacks any other method of exercising control over Romania. Türkiye, though in a similar region adjacent to the Black Sea, also has access to the Mediterranean Sea and controls the Bosporus and Dardanelles straits, the only way for ships to move between the Black Sea to the Mediterranean Sea. These routes have long been of interest to Russia, which borders the Black Sea to the northeast and has taken advantage of Türkiye's neutrality to move submarines and warships through this area as it attacks Ukraine. In the southeast, Türkiye borders war-torn Syria. Due to the number of threats Türkiye faces and its geographic location, it is home to several major NATO bases.

— 14 —

Romania

Milagro Castilleja

ABSTRACT: Romania is unique in that it is one of the least foreign energy dependent countries in Europe, relying mostly on its massive investment into renewable energy infrastructure and several nuclear power plants to power most of the nation. There has been a recent growth in cyberattacks on Romania's critical infrastructure by foreign actors seeking to exploit Romania's strategic position along the Black Sea through cyberattacks. For example, a ransomware attack in March 2022 on Romania's largest petroleum pipeline was attributed to the Hive group.[1] Romania has partnered with other NATO and EU nations to tackle these threats and has fostered a robust cyber-defense network.

Keywords: Romanian Economic Exclusion Zone, cyberattacks, cybersecurity, renewable energy, networked energy services, smart grid, nuclear energy, nuclear power plant

Introduction

Romania exists as an important nerve center of the Black Sea region with its strategic location along the crossroads of three major pan-European transport corridors and one of the most significant gateways to the Black Sea.[2] As a prominent gateway to the Black Sea and as a NATO and EU country, the potential for a destabilization campaign targeting Romania is higher than usual. Russia's proximity to Romania after the illegal Russian annexation

1. Emma Vail, "Hive Ransomware Gang Targets Romanian Oil Firm in Its Latest Cyberattack," *Record* (website), March 8, 2022, https://therecord.media/hive-ransomware-gang-targets-romanian-oil-firm-in-its-latest-cyberattack/.

2. "Competitive Advantages," InvestRomania (website), n.d., accessed June 1, 2021, http://investromania.gov.ro/web/doing-business/competitive-advantages/.

of Crimea heightens that potential, considering the identification of Russian-backed disinformation campaigns against Romania in recent years.

Romania is currently in an energy transition period that has diversified the energy sector over the last 10 years. Romania has invested in renewables, with 23.88 percent of Romanian electricity production coming from renewable sources in 2020.[3] While strengthening renewable infrastructure, Romania is also pushing for the modernization of energy infrastructure via numerous smart-grid projects. This push has led to the country ranking third-lowest in energy dependency rate across EU members as of 2020.[4] Much of Romania's renewable electricity potential is generated by hydropower "followed by wind power and then solar power."[5]

A significant portion of Romanian energy comes from older fossil-fuel infrastructure. Romania's eight power plants currently provide an "installed gross capacity of 5315 MW," which should only increase in capacity once Romania's ninth coal power plant is operational. Romania currently operates two nuclear power reactors out of Cernavodă, which are currently generating about 15–20 percent of Romania's electricity.[6] Romania is expected to expand its nuclear-power capacity with two more reactors slated to be constructed in 2021 and 2022 or later. This increase in nuclear power has the potential to further reduce the amount of energy produced from fossil fuels, in accordance with Romania's National Energy and Climate Plan (NECP).

With the goals set by Romania's NECP, the state intends to increase the capacity of hydropower electricity generation and "repower," or install new and/or upgraded technologies to improve the potential of aging systems, across existing solar and wind farms.[7] Romania has also taken on the implementation of smart-grid technology across the existing power grid.

3. Hannah Ritchie and Max Roser, "Romania: Energy Country Profile," Our World in Data (website), 2021, https://ourworldindata.org/energy/country/romania.

4. "The Energy Sector in Romania," CEE Bankwatch Network (website), 2020, https://bankwatch.org/beyond-coal/the-energy-sector-in-romania.

5. Nicolae Marinescu, "Changes in Renewable Energy Policy and Their Implications: The Case of Romanian Producers," *Energies* 13, no. 24 (6493): 24, https://doi.org/10.3390/en13246493.

6. "Energy Sector in Romania"; and "Nuclear Power in Romania," World Nuclear Association (website), updated March 2021, https://world-nuclear.org/information-library/country-profiles/countries-o-s/romania.aspx.

7. Delia Pachiu and Nita Marius, "Electricity Regulation in Romania: Overview," Thomson Reuters Practical Law (website), law stated as of October 1, 2020, https://uk.practicallaw.thomsonreuters.com/4-566-2907?contextData= percent28sc.Default percent29.

Romania's current path forward to modernizing the existing electrical grid and renewable infrastructure will introduce several major risks into the energy sector. Most of Romania's older renewable technology and facilities require upgrades and new technology to bring them up to current energy efficiency and production standards. The installation of emerging technology introduces potential vulnerabilities into strategic energy production facilities. Romania also plans to construct new renewable facilities, including the first offshore wind farm in Romania's exclusive economic zone (EEZ). With Russia close by and the isolated nature of offshore facilities, this project introduces a new dimension of vulnerabilities to the security of Romanian energy production and transportation.

The introduction of smart-grid technology into aging electrical systems creates numerous vulnerabilities along the aging electrical grid. Older electrical grids run the risk of sustaining permanent damage during a cyberattack. Government facilities attached to newly installed smart grids would be vulnerable to data breaches. At an extreme level, the possibility exists that energy production facilities processing or containing hazardous materials (such as nuclear power reactors) are at risk for a cyberattack that could devastate the local region surrounding these facilities and create nuclear disasters like the ones seen at Chernobyl and Fukushima.

Renewable Energy and Smart Grids in Romania

With 13 hydroelectric dams throughout Romania, renewables provide almost half the energy for the country. Hydropower accounted for almost 28 percent of electricity production in 2020 alone, while in 2019, just over 24 percent of energy consumption was provided by renewable energy sources.[8] Renewables account for a large portion of electricity production within the country. As of April 2020, 49.92 percent of electricity production was due to green energy.[9]

Romania is making progress in developing its renewable energy infrastructure in accordance with the European Commission's (EU) goals for the European Green Deal. In 2019, Romania was one of the countries

8. "EY Romania Report: Renewables Can Accelerate the Decarbonisation of the Romanian Energy Sector, But Public Initiatives Must Be Synchronised with Business Intentions," Ernst & Young (website), April 1, 2021, https://www.ey.com/en_ro/news/2021/04/ey-romania-report--renewables-can-accelerate-the-decarbonisation.

9. Varinia Radu, Ramona Dulamea, and Raluca Diaconeasa, "CMS Expert Guide: Renewable Energy Law and Regulation in Romania," CMS (website), n.d., https://cms.law/en/int/expert-guides/cms-expert-guide-to-renewable-energy/romania.

to have met the Green Deal goal of "reaching a share of approximately 27 percent of green energy in 2019" in accordance with said goals.[10] Romania is making strides in achieving the 2030 goal of contributing a 30.7 percent share of renewable energy. Considering ongoing plans of increasing renewable energy capacity, Romania has the potential of meeting and surpassing the 2030 goal in the next 10 years.

Improving Romania's Renewable Energy Infrastructure

Romania's current goal, as mentioned earlier, is to reach a 30.7 percent overall share of renewable energy in gross final energy consumption by 2030.[11] In order to meet this goal, while also strengthening the shift to a larger reliance on internal energy sources, Romania plans to increase renewable energy capacity by almost 35 percent in 2030, with 2.3 gigawatts in wind farms and 3.7 gigawatts in solar-power plants. At an estimate of 1 gigawatt powering 300,000 homes, this increased capacity has the potential of powering 1,800,000 homes in Romania. With repowering alone, Romania plans to add 3 gigawatts of installed capacity in wind power and 1.35 gigawatts in solar power by 2027–30.[12]

Hydroelectric power is the largest contributor to Romania's renewable energy generation, with wind power, solar power, and biomass making the second-, third-, and fourth-largest contributions, respectively.[13] By 2030, projections indicate the capacity of wind power specifically will increase up to 5,255 megawatts.[14] It will also be important for Romania to add new renewable energy facilities to existing energy production infrastructure, install new technology, upgrade existing technology, or "repower" existing renewable facilities.

Doubling Down on Smart Grid

Romania is focusing on implementing smart-grid infrastructure across its general electrical grid. It is taking strong steps to ensure that accepted contracts are with companies within NATO ally countries. With the large-scale introduction of smart meters, Romania looks to turn its current energy market into a "fit-for-RES" (renewable energy

10. Radu, Dulamea, and Diaconeasa, "Renewable Energy Law."

11. "The 2021–2030 Integrated National Energy and Climate Plan," European Commission (website), https://ec.europa.eu/energy/sites/ener/files/documents/ro_final_necp_main_en.pdf.

12. "2021–2030 Integrated National Energy and Climate Plan," 58.

13. "Energy Sector in Romania."

14. "2021–2030 Integrated National Energy and Climate Plan," 57.

source) market.[15] With mass smart-grid implementation, it is possible Romania will see an increase in yearly electricity savings across the board. In 2020, it was estimated that smart metering saved 58.14 gigawatt hours in electricity, a 125 percent increase from 2018.[16]

Romania is also taking strong steps to modernize its electrical grid. As of 2020, 320,000 smart meters were installed by German energy supplier E.ON, one of three NATO ally-based contractors installing Romania's smart-grid infrastructure.[17] This action follows a recent trend of accepting bids from corporations based in NATO countries, as US-based developer, Networked Energy Services (NES), has been awarded another smart-grid project set to introduce approximately 90,000 smart meters into the electrical grid.[18] In 2020, 170,000 meters were also installed by Italy-based Enel Group, an investment of over 11.5 million euros.[19]

An additional note regarding Romania's fossil-fuel landscape: Romania has accepted a bid from China Huadian Engineering Company (CHEC) for the construction and operation of a new coal plant in Rovinari, with the operation of the plant slated to continue until 2063.[20] With electricity generation expected by 2023, and the push for smart-grid technology, this facility would more than likely be connected to the rest of the grid via smart metering. While a Chinese threat of cyberattack on Romania is unlikely, this site does provide an opportunity for a bad actor to utilize known vulnerabilities within Chinese software to attack smart-grid infrastructure. The contact point between Chinese software and technology with Western smart-grid technology also carries the potential to create unique vulnerabilities due to conflicts between technologies.

---

15. "2021–2030 Integrated National Energy and Climate Plan," 72.

16. Lisa Ann Lamont and Ali Sayigh, eds., *Application of Smart Grid Technologies: Case Studies in Saving Electricity in Different Parts of the World* (Cambridge, MA: Academic Press, 2018), 329.

17. Jonathan Spencer Jones, "E.ON – 700,000 Smart Meters in Romania by 2028, 2.5 Million in Germany by 2030," Smart Energy International (website), December 10, 2020, https://www.smart-energy.com/industry-sectors/smart-meters/e-on-700000-smart-meters-in-romania-by-2028-2-5-million-in-germany-by-2030/.

18. "Networked Energy Services Awarded Another Smart Grid Project in Romania," Networked Energy Services (website), 2019, https://www.networkedenergy.com/en/news-events/networked-energy-services-awarded-another-smart-grid-project-in-romania?utm_source=newsletter&utm_medium=email&utm_campaign=newsletter-jan-2020.

19. SEE Energy News, "Romania: Enel Installs Smart Meters Reaching 900,000 Customers by the End of 2020," Serbia Energy (website), October 28, 2020, https://serbia-energy.eu/romania-enel-installs-smart-meters-reaching-900000-customers-by-the-end-of-2020/.

20. Ionut Dulămiță and Michael Bird, "Chinese Coal Power in Romania's Rustbelt," Echowall (website), 2019, https://www.echo-wall.eu/plus-one/chinese-coal-power-romanias-rustbelt.

The development of renewable energy production and smart-grid installation creates a lengthy transitional period for Romania. While Romania continues to improve its energy infrastructure in these areas by accepting bids for new facilities and installations, it will be essential to ensure the security of the technical components being used in these projects. As interconnectivity between every aspect of Romania's energy landscape continues to grow and advance, so do the number of potential vulnerabilities for a cyberattack that could leave every connected component out of commission.

Cyber Challenges of Renewable Energy and Smart-grid Technology

Imagine the following scenario. At 2:34 a.m. local time in Cernavodă, power at the Cernavodă Nuclear Power Plant suddenly shuts down. Backup generators that should activate to shut down the plant in the event of power loss, do not start. The plant is completely without power, and the water pumps designed to keep the power cores at nominal temperatures shut down. The cores begin to heat up, and eventually the nuclear cores melt down, releasing a dangerous amount of radiation into the surrounding area. In what could be hours, days, or even weeks, new backup generators are installed, and the cores are brought back down to safe operating levels. The damage is done, however, as radiation leaks into the surrounding city of Cernavodă and begins to disperse across the landscape on the wind. Elevated radiation levels are detected 43 kilometers away on the coast of Constanța, Romania's major Black Sea port. The meltdown renders the intervening area unsafe, and a mass evacuation is ordered. Several engineers are injured in the chaos, and many more suffer from radiation poisoning as the plant meltdown releases radiation into the air for several days. The exclusion zone around the plant remains unsafe for years after, displacing millions of Romanians and rendering one of Romania's key Black Sea ports inoperable.

In the months afterward, it is discovered the initial power loss at the plant was due to a cyberattack on the power station that supplied electricity to the plant. The backup diesel generators, which could have prevented the meltdown, were physically sabotaged before the power-loss event, rendering the plant inoperative.

While this specific scenario may not occur, the reality is that as Romania introduces new and upgraded smart-grid technology into the existing electrical grid, the potential for a hybrid attack of this nature increases.

The threats of such an attack have become increasingly real with the Russian invasion of Ukraine.

Romania's current infrastructure is in the midst of a large-scale transition that operates at a persistent level of risk out to 2030. With plans for new renewable energy facilities and large-scale expansions of coal and nuclear capabilities, this transition period carries a heightened risk of cyberattack due to vulnerabilities introduced with the installation of emerging technology. As Romania upgrades and strengthens existing energy infrastructure, windows of opportunity for bad actors to access and weaken this infrastructure could multiply.

The number of vulnerabilities will grow exponentially as Romania modernizes older electrical grids and adapts them to smart grids. Romania's Internet-connected smart grids could be subject to phishing operations, denial-of-service attacks, malware propagation, and eavesdropping and traffic analysis efforts.[21] These cyberattacks could expose private data stored on energy facility servers (such as payment records, contractor records, and even government data) if a bad actor attacks the contact point between the smart grid and a government facility.

The aging electrical grid that serves as the foundation for energy transportation throughout Romania will be at a heightened risk of sustaining permanent damage from a cyberattack on integrated smart grids. If a cyberattack were to focus on exploiting and overloading vulnerable systems to cause physical destruction, the attack could cause permanent infrastructural damage that would cost millions to repair and leave millions of citizens without power for an extended period. While Romania is sourcing smart-grid development projects from NATO countries, it is equally important those companies vet the hardware and software being used in the construction of Romania's smart-grid network. If one component or one piece of installed software carries a backdoor or vulnerability for a bad actor to use, the whole network could be compromised.

"Repowering" older renewable facilities and plants features several of the same risks as installing smart grids. If hardware and software components are not properly vetted, systems within solar or wind farms could be compromised, leading to delays in energy production, destruction of valuable renewable technology, or further compromise connected smart-grid networks.

21. Dharmesh Faquir et al., "Cybersecurity in Smart Grids, Challenges and Solutions," *AIMS Electronics and Electrical Engineering* 5, no. 1 (2021): 24–37.

Development in Romania's EEZ

There are several considerations to keep in mind in regard to Romania's plans for the construction of offshore wind farms in the Romanian EEZ. As the sites of these farms will be relatively remote in the Black Sea, there is the potential for a hybrid attack that targets the physical construction elements (for example, undersea cabling and construction equipment) and the digital systems used by contractors to plan, schedule, and store valuable structural data of the projects. The undersea cables that will run generated power from the planned wind farms will take time to lay, and any physical sabotage to them may increase the cost of the project, costing Romania valuable resources. The exact distance of these wind farms is dependent on the type of turbines used in the project, but the further out these turbines are constructed, the greater the possible response time grows. The point of contact between Romania's grid and new offshore wind-farm technology also becomes a sensitive pressure point, at a heightened risk if it is Romania's major port, Constanța. Disruption at this point of contact may affect Romanian operations in the Black Sea and significantly hinder energy transportation from Romania's EEZ.

Furthermore, the risk of hybrid attack on any of Romania's planned offshore wind farms should be considered elevated due to the nature of the current EEZ landscape of the Black Sea. Romania's EEZ shares a boundary with the Bulgarian and Ukrainian EEZs. Ukraine's EEZ surrounding the Crimean Peninsula, however, is currently under Russian control after Russia's illegal annexation of Crimea. This puts Russia within uncomfortable proximity to any development efforts in Romania's EEZ, which presents another avenue for a possible destabilization campaign in the region.

Romania's Cybersecurity Landscape

In 2020, 70 percent of Romanian households had access to data communications networks.[22] This statistic is likely to grow in the next 10 years, as more homes are connected to smart-grid infrastructure. Access to data communications among Romanian households should increase sharply as the Ministry of Transport, Infrastructure, and Communication's (MTIC) RoNET project, aimed at covering areas lacking broadband

22. "Human Development Insights: Romania," United Nations Development Project (website), https://hdr.undp.org/en/countries/profiles/ROU.

infrastructure, continues to connect areas to data communication technology simultaneously with ongoing smart-grid projects.[23]

In 2013, the Supreme Council of National Defense (CSAT) approved the National Cybersecurity Strategy of Romania, which set a necessary organizational and conceptual framework for ensuring cybersecurity and addressed cyber-infrastructure protection in accordance with policies regarding cyber defense illustrated by the EU and NATO.[24] Since its approval, Romania's Cybersecurity Strategy has remained unchanged. Romania's cyber defense will be key in the next 10 years as it transitions from a traditional energy infrastructure to production facilities and technology susceptible to cyberattack.

Romania has prioritized developing its cybersecurity infrastructure and organization to ensure the cybersecurity of the country and the EU. As of 2019, Romania has fully transposed the NIS Directive.[25] In accordance with this directive, Romania has demonstrated its national cybersecurity capabilities to the appropriate level in the EU, prioritized cross-border collaboration with EU allies, and created and implemented supervision of critical sectors, such as energy and transport sectors.[26]

The National Cybersecurity Strategy of Romania created several entities tasked with different aspects of ensuring its cybersecurity across critical sectors. Romania's National Cybersecurity System (SNSC) is the general cooperation framework connecting and tasking both public authorities and institutions with the "responsibilities and capabilities to ensure coordination of actions at the national level for cyberspace."[27] In 2018, the Cyber Defense Command (CApC) of Romania was established, with a mission to "plan, organise, direct and conduct operations in the cyberspace to protect military networks, provide information technology services and support the joint military operations with cyber effects."[28] Currently, the CApC provides day-to-day cyberspace defense as it works toward being fully operational

23. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), *National Cybersecurity Organisation: ROMANIA*, National Cybersecurity Governance Series (Tallinn: EE: NATO CCDCOE, 2020), 6, https://ccdcoe.org/uploads/2020/11/NCS_organisation_ROM-2020_FINAL.pdf.

24. NATO CCDCOE, *National Cybersecurity Organisation: ROMANIA,* 8.

25. "Implementation of the NIS Directive in Romania," European Commission (website), updated November 7, 2020, https://ec.europa.eu/digital-single-market/en/implementation-nis-directive-romania.

26. "NIS Directive," European Union Agency for Cybersecurity (ENISA) (website), n.d., accessed May 24, 2021, https://www.enisa.europa.eu/topics/nis-directive.

27. NATO CCDCOE, *National Cybersecurity Organisation: ROMANIA,* 9.

28. NATO CCDCOE, *National Cybersecurity Organisation: ROMANIA,* 10.

by 2024, and has entered several partnerships with US-based entities to accelerate cyberspace defense excellence.[29]

Romania has also developed several CERT-type (Computer Emergency Response Team) entities to oversee its cyber-defense framework. The Romanian Computer Emergency Response Team (CERT-RO), the main CERT entity of Romania, is the national authority in securing national networks and information technology and communications (IT&C) systems.[30] CERT-RO is tasked with "preventing, analysing, identifying and responding to cyber incidents," and developing and disseminating public policies for preventing and counteracting incidents involving cyber infrastructure.[31] Additionally, Romania has created CERT-MIL that focuses on "cyber risks, specialized assistance, forensics, and the management of cyber incident" for members of the Ministry of Defense, and the National Cyberint Center and serves as the cyber intelligence center of Romania tasked with "counter-espionage, economic security, transnational threats and the protection of classified information."[32]

At present, there is little public information available on the shape of Romania's early warning system in regard to cyber defense. While there is not a clear label or shape to the system, it is safe to assume Romania's early warning system is near completion and should be implemented in 2024 when the CApC is expected to be fully operational. If energy production were to be halted due to a cyberattack, the operational effectiveness of the Romanian Armed Forces (RAF) would be severely impacted. With military preparedness in the Black Sea region growing more and more necessary with Russia's presence on the Crimean Peninsula, ensuring the security of Romania's energy infrastructure on all fronts will be of vital importance to the Ministry of Defense in ensuring the readiness of the RAF.

Recommendations

Whether through direct interference with the installation process of new or upgraded renewable technology or the sabotage of aging electrical systems that will serve as the structure for the smart grid, there is currently a high

29. NATO CCDCOE, *National Cybersecurity Organisation: ROMANIA*, 11.

30. NATO CCDCOE, *National Cybersecurity Organisation: ROMANIA*, 9.

31. "Romania (RO)," Cyberwiser (website), n.d., accessed May 2021, https://www.cyberwiser.eu/romania-ro; and NATO CCDCOE, *National Cybersecurity Organisation: ROMANIA*," 10.

32. "Romania (RO)."

threat of hybrid attack. It is important for Romania to address these security risks in step with developing this rapidly expanding energy infrastructure.

Based on the research presented, the recommendations for addressing these challenges to the cybersecurity of Romania's energy infrastructure are as follows:

1. **Rapid finalization and implementation of cyber-defense early warning systems.** It is of the utmost importance that Romania implement clear cyber early warning systems across its energy landscape as soon as possible. The absence of an early warning system leaves critical facilities and locations at risk of cyberattacks that could have devastating repercussions if the attacks are not detected early enough. The creation of dedicated CERT entities on-site at the Cernavodă Nuclear Power Plant or at any of the 13 hydroelectric dams may be the best short-term solution until the full early warning system is implemented. In this fashion, there can at least be an active defense on standby at these hazardous sites that can respond within seconds of a cyberattack. Constanța will continue to be a major port in the Black Sea that will serve as a transportation hub for energy produced via offshore wind farms in the future. It will be critical to strengthen the cyber defense of the port, as there are numerous systems in operation that may eventually share a network with energy transportation technology. The formation of a CERT tasked with the cybersecurity of the ports would be an excellent way to provide a focused approach at the possible cyberattack vectors present in Constanța.

2. **Introduction of an oversight group tasked with vetting sourced components for repowering and smart-grid projects.** As both renewable-energy projects and smart-grid projects in Romania will rely on the installation of new technology, ensuring the safety and security of this technology should be a major priority. While Romania has focused on working with ally countries, the components sourced by the entities tasked with repowering old renewable-energy facilities or integrating smart meters into the electrical grid are still at high risk of introducing manufactured vulnerabilities and backdoors into the system if they are not properly vetted. To ensure every component involved with these projects

does not create new vulnerabilities, a government group or organization should be created and specifically tasked with both providing oversight to international contractors awarded energy-infrastructure bids and vetting the components used in these projects to ensure they are manufactured at a reliable, trusted facility. The vulnerabilities associated with constructing a new wind farm do not exist primarily at the construction site. While this approach may seem overzealous, it would further shore up the security of these projects while setting an example for other allied countries developing renewable energy or smart-grid infrastructure, which will improve the overall security of the energy landscape across NATO.

3. Installation of upgraded physical components into aging electrical grids targeted for smart-grid integration. Romania's modernization of the existing electrical grid by introducing smart-grid technology is a major step toward increasing energy efficiency. The aging infrastructure, however, should not be overlooked. In regard to addressing the possible permanent damage that could be done to the older electrical grid underneath, it is the recommendation of this paper that as smart-grid networks are installed and integrated with existing electrical grids, the physical grids themselves should also be upgraded, with aging parts replaced completely. This process would potentially further protect the energy-transportation network of the country from any permanent damage in the event of a cyberattack. Upgrading and replacing older electrical grid components in step with smart-grid integration efforts would raise the financial burden immensely. Therefore, this would be a good opportunity for the EU to form a stronger bond with Romania and offer financial support as this modernization could only benefit Romania's goals in supporting the European Green Deal.

4. Increased awareness of EEZ security surrounding offshore facility construction sites. Romania's plan for the first offshore wind farm is a great step in advancing its green-energy goal. As mentioned previously, the proximity of Romania's EEZ to Russia is of concern for the security of any offshore development plans. With the Russian Navy attempting to take Odesa from Ukraine's EEZ, close to Romania's, it is critical Romania is ready. Echoing Romanian President Klaus Iohannis's sentiment, NATO is developing contingencies to support Romania in the event of a Russian-backed hybrid attack on facilities in Romania's EEZ. Increased vigilance of the offshore sites will ensure a rapid response in the event of an attack.[33]

Conclusion

Romania's proximity to Russia and the Russia-Ukraine war creates several concerns for infrastructure security. It is critical now that Romania continue to further its energy independence goals and secure and update its existing energy infrastructure to remain free of foreign interference and exploitation. There is also room for NATO to aid Romania in this mission by assisting in the development of renewable-energy systems and cybersecurity tools to help defend Romanian infrastructure, which is especially critical now that conflict with Russia is raging so close to its borders.

Figure 13-1. Map of Romania's threat timeline estimate (6 months indicates likely attack vector in 2022, 1 year by 2023, 2+ years by 2024 or later)
Credit: Ryan Fisk and Lucas Cox

33. Reuters Staff, "Romanian President Says More NATO Presence Needed in Eastern Europe," Reuters (website), May 10, 2021, https://www.reuters.com/world/europe/biden-join-eastern-european-nato-states-summit-focus-seen-ukraine-2021-05-10/.

Location	Reason for Threat Priority and Timeline
Bucharest	Bucharest's smart grid makes it an attractive cyber target for the next two years, particularly considering the impact it could have on port activities, NATO allies, and military operations in Ukraine.
Port of Constanța	Disrupting the Constanța's port logistics, distribution, and tracking within the next six months would have an impact on NATO capabilities and its posture in the Black Sea.
2026 Offshore Wind Farm	The wind farm's location and connection with strategic assets could make it a target upon completion if cybersecurity is not implemented into the design.
Oil Infrastructure	Oil infrastructure, especially within proximity of the Corbu refinery and Black Sea critical infrastructure, remains a possible target in the wake of the cyberattack on Romania's leading petroleum company in 2021.
Seini Substation and Transmission Line to Mukacheve	Expect an ICS or DDoS attack within six months because this is an important node of Ukraine's power supply and is likely to be targeted by cyber or kinetic attack in the next six months of Russia's offensive operations in Ukraine.
Iasi Smart Grid	The Iasi smart grids could become a target if there is an escalation near or with Moldova.
Corbu Gas Treatment Plant and Pipeline to Midia Gas Development Plant	A DDoS attack on the plant's ICS or other cyberattack within the next six months is likely due to the rising importance of offshore gas and impact on NATO allies.
Cernavoda Nuclear Power Plant	This plant produces 20 percent of Romania's electricity and will be of increasing importance in an energy transition away from Russian imports over the next year. Disinformation or cyberattacks are possible in that time frame.

Select Bibliography

Dulămiță, Ionut, and Michael Bird. "Chinese Coal Power in Romania's Rustbelt." Echowall (website), 2019. https://www.echo-wall.eu/plus-one/chinese-coal-power-romanias-rustbelt.

Faquir, Dharmesh et al. "Cybersecurity in Smart Grids, Challenges and Solutions." *AIMS Electronics and Electrical Engineering* 5, no. 1 (2021): 24–37.

"Implementation of the NIS Directive in Romania." European Commission (website). Updated November 7, 2020. https://ec.europa.eu/digital-single-market/en/implementation-nis-directive-romania.

Marinescu, Nicolae. "Changes in Renewable Energy Policy and Their Implications: The Case of Romanian Producers." *Energies* 13, no. 24 (6493): 24. https://doi.org/10.3390/en13246493.

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). *National Cybersecurity Organisation: ROMANIA*. National Cybersecurity Governance Series. Tallinn: EE: NATO CCDCOE, 2020. https://ccdcoe.org/uploads/2020/11/NCS_organisation_ROM-2020_FINAL.pdf.

Radu, Varinia, Ramona Dulamea, and Raluca Diaconeasa. "CMS Expert Guide: Renewable Energy Law and Regulation in Romania." CMS (website). n.d. https://cms.law/en/int/expert-guides/cms-expert-guide-to-renewable-energy/romania.

"The 2021–2030 Integrated National Energy and Climate Plan." European Commission (website). https://ec.europa.eu/energy/sites/ener/files/documents/ro_final_necp_main_en.pdf.

— 15 —

Italy

Vishwa Padigepati

ABSTRACT: Although Italy is becoming more energy independent, it should prioritize a sustainable strategy in the development of renewable energy sources to minimize risks incurred through the cooperation and sourcing processes. The influx of foreign direct investments in Italy's oil, natural-gas, and electric-grid sectors could introduce cooperation-induced risks if proper vetting processes are not undertaken. A survey of the risks and opportunities provided by cooperation with foreign countries on energy transformation is necessary for effective risk management. Advances in 5G interconnectivity further present vendor-related considerations at the infrastructure level as well as macro-level governance compatibility issues that may pose concerns for Italy's long-term strategic priorities.

Keywords: renewable energy, Italy national energy strategy, Italy renewable energy directive, Huawei, China cyber policy, COPASIR

Introduction

Italy's Energy Landscape

Italy's energy consumption is evolving parallel to its commitment to diversifying its energy landscape and combating the negative effects of climate change. Its investment in sustainable energy sources is driven by its dedication to restructuring the energy program for long-term optimization and moving the country toward a definitive future in energy efficiency. In the 2030 National Energy and Climate Plan, Italy defines its strategy toward achieving the goals set forth by the Energy Union, identifying that energy security and reducing emissions are both necessary in achieving long-term NECP objectives.[1] The country's primary energy consumption is driven by petroleum and natural gas, which account for 70 percent of its total average annual consumption.[2] Supplementary energy shares emerge from coal, hydroelectricity, and other renewable energy sources.

Total energy consumption has been declining since 2017, with Italy's per capita energy consumption at a 20 percent lower average than the EU.[3] While most of Italy's electricity consumption has previously come from fossil fuels, renewable energy sourcing has since been diversified. Italy's current energy mix reflects its energy efficiency directives to have renewables surpass natural gas as the primary fuel for electric power. Currently, renewables account for 21 percent of energy consumption, natural gas for 35 percent, oil for 34.2 percent, and coal for 3.9 percent. Renewable energy sources have seen a considerable increase in Italy's energy consumption mix by more than 1,000 percent since 2005, supporting less than 2 percent of production in 2005 to nearly 10 percent in 2016.[4] Natural gas is predicted to remain the primary source of energy for Italy until 2030, as the consumption of petroleum products falls and that of renewable sources increases.[5]

The evolution of Italy's energy mix is a product of the government's National Energy Strategy and concerted efforts to induce change in industry consumption through policy implementation. The recasting of the Renewable Energy Directive 2018/2001/EU, which moved the legal framework to 2030, set a renewable-energy target of 32 percent and an increased 14 percent target for renewable fuel-share in transport. Italy's final National Integrated Plan for Energy and Climate 2030, released in January 2020, presents core objectives of a target for 30 percent renewable-energy share in gross final consumption of energy, a 22 percent renewable-energy share in the global final consumption of energy in transport, and a reduction in primary energy consumption by 43 percent (compared to Primes 2007 scenario).[6] In September 2020,

---

1. "Italy's Integrated National and Energy Climate Plan," Grantham Research Institute on Climate Change and the Environment (website), 2019, https://www.climate-laws.org/geographies/italy/policies/italy-s-integrated-national-and-energy-climate-plan.

2. Valentina Canalini, Sofia Silveri, and Antonella Guetta, "International Legal Business Solutions – Global Legal Insights," Global Legal Insights (website), 2021, https://www.globallegalinsights.com/practice-areas/energy-laws-and-regulations/italy#chaptercontent1.

3. US Energy Information Administration (EIA).

4. Canalini, Silveri, and Guetta, "International Legal Business Solutions."

5. Canalini, Silveri, and Guetta, "International Legal Business Solutions."

6. Canalini, Silveri, and Guetta, "International Legal Business Solutions."

the European Commission introduced an amendment to the European Climate Law to adjust the target of a 40 percent emission reduction by 2030 from 1990 levels to a 55 percent target, setting forth the Green Deal Communication to prioritize member states' objectives in energy, industry, mobility, and agriculture.[7] Italy has agreed with the larger EU approach and is promoting the Green New Deal objectives by implementing the Clean Energy Package through appropriate domestic legislation.[8]

The prioritization of a sustainable energy transition brings both strategic opportunities and liabilities which can be identified partly in the current incentive policies. The Rilancio Decree in May 2020, for instance, introduced "super bonuses" or a deduction of 110 percent of expenses incurred between mid-2020 and the end of 2021 for interventions in energy efficiency. The Simplification Decree of 2020 is set to accelerate investments and construction of infrastructure by simplifying photovoltaic plant installation and is set to strengthen the public-private alliance for investments by allowing energy performance contracts to be qualified as public partnership contracts.

The COVID-19 pandemic has brought about challenges and changes in Italy's policy approach to its renewable-energy transition. The Italian government is responding to the emergency by identifying important macro areas of intervention, including digitization and innovation, green revolution and ecological transition, and infrastructure for sustainable mobility. Digitization has materialized as an increased emphasis on 5G infrastructure, IoT technology, and smart grids for energy management. Italy's commitment to translating EU environmental policy directives is strong and clearly exemplified in practice. The rapid pace at which the transition toward energy efficiency is occurring, the layered legal landscape on which it is taking place, and its involvement of cyber-connectivity raise cyber vulnerabilities that can be exploited by malign actors. The following case study will consider Italy's future ambitions in renewables and connective technology as they relate to the threats posed by the transition process—namely its supply-chain sourcing for renewable-energy technologies and the risks posed by the connectivity of 5G technology's operational and software infrastructure.

7. European Commission, *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: The European Green Deal* (Brussels: European Commission, December 11, 2019), 640, https://ec.europa.eu/info/sites/default/files/european-green-deal-communication_en.pdf.

8. Canalini, Silveri, and Guetta, "International Legal Business Solutions."

Vulnerability: Chinese Foreign Direct Investment in Renewable Energy Technologies

Italy's transition to renewable energy involves extensive international cooperation in supply-chain management that poses cybersecurity challenges. Italy's cooperation with China, for instance, poses substantial risks as China sources a large percentage of Italian photovoltaics, silicon wafers, and other renewable-energy materials.[9] According to Luca Iacoboni, climate and energy campaigner with Greenpeace Italy, China has always played a substantial role in Italy's green-energy market.[10] This assertion is further backed by data, as Chinese foreign direct investment (FDI) increased by 850 percent from 573 million euros in 2015 to 4.9 billion in 2018, per the Italian Parliamentary Committee for the Security of the Republic.[11] Moreover, Chinese multinational company StateGrid has a nearly 35 percent stake in the financing of Italian electricity grids, and companies such as ChemChina hold great influence in energy networks companies.[12] While cooperation with China on the achievement of energy transformation is not a risk itself, the nature and extent of this supply-chain cooperation is not fully known, increasing the potential for liabilities and security vulnerabilities.

Chinese investment in Italian energy and gas infrastructure is characterized by a considerable supply-chain and investment-bound relationship. The Chinese government's motivation is to divest from its previous *minjian xianxing* "non-government (private first)" export-driven growth model and invest efforts in expanding China's international presence and promoting Chinese investments abroad.[13] This aim can be clearly seen in China's current conduct with Italy. Empirical transactions and investments from China in Italy's energy sector substantiate China's increasing influence in sensitive areas. The State Grid Corp. of China's purchase of the Italian state lender company Cassa Depositi e Prestiti (CDP) Reti S.p.A., a holding company with substantial influence and control

---

9. Rudi Bressa, "Italy Welcomes Chinese Investments, but Competition Fears Linger," *Clean Energy Wire* (blog), January 6, 2021, https://www.cleanenergywire.org/blog/italy-welcomes-chinese-investments-competition-fears-linger.

10. Bressa, "Italy Welcomes Chinese Investments."

11. Bressa, "Italy Welcomes Chinese Investments."

12. Parliamentary Committee for Security of the Republic, "RELAZIONE: sulla tutela degli asset strategici nazionali nei settori bancario e assicurativo," XXXIV RELAZIONE: sulla tutela degli asset strategici nazionali nei settori bancario e assicurativo § (2020), 1–40.

13. Pablo Pareja-Alcaraz, "Chinese Investments in Southern Europe's Energy Sectors: Similarities and Divergences in China's Strategies in Greece, Italy, Portugal and Spain," *Energy Policy* 101 (February 2017): 700–10, https://www.sciencedirect.com/science/article/abs/pii/S0301421516305006.

over Italy's electricity grid and gas distribution operations, is a confirmation of China's success in asserting its influence in the Italian energy sector.[14] Gas and electricity distribution are sensitive to foreign investments, allowing China State Grid greater access to Italy's energy technology and networks.

Moreover, in 2014, Shanghai Electric agreed to buy a 40 percent stake in Ansaldo Energia, the Italian power equipment maker, from CDP's Fondo Strategico Italiano, while the People's Bank of China bought stakes topping 2 percent in Italian oil and gas giant ENI (controlled by CDP) and the electricity and natural-gas distributor ENEL (controlled by the Italian Treasury).

The pace of Chinese FDI investment in Italy's energy markets presents security and economic concerns. First, a substantial proportion of Chinese FDI in Italy comes from state-owned enterprises (SOEs). Due to the dependence of SOEs on the state's decisions, financial vehicles, and investment behaviors, it is difficult to reliably differentiate between the investment behaviors of state-owned enterprises and China's state capitalist system. For instance, research has shown that Chinese SOEs' industrial investment aims align with those of the state which aims to control the "most profitable components and nodes of global supply chains."[15] This goal especially pertains to Chinese investments in tech-innovation areas such as renewable-energy generation. The risks emerging from the nature of this partnership present themselves as being driven by the lack of reciprocity between Italy to China's energy engagements, with China placing high restrictions and regulations on non-energy-related FDI despite Italy's high engagement.[16]

First, Chinese investments in Italy present security considerations—the advanced digitization of renewable-energy systems increases vulnerabilities to attacks.[17] China has empirically had a record high number of cyberattacks and, thus, extensive supply-chain and sourcing partnerships between Italy and China can leave Italy's renewable energy technologies vulnerable.[18]

14. Francesca Landini and Luca Trogni, "Italy to Sell Energy Grid Stake to China for 2 Billion Euros," Reuters (website), July 24, 2014, https://www.reuters.com/article/us-italy-china/italy-to-sell-energy-grid-stake-to-china-for-2-billion-euros-idUSKBN0FT1H020140724.

15. Björn Conrad and Genia Kostka, "Chinese Investments in Europe's Energy Sector: Risks and Opportunities?," *Energy Policy* 101 (February 2017): 644–48, https://www.sciencedirect.com/science/article/pii/S0301421516306711.

16. Conrad and Kostka, "Chinese Investments."

17. Conrad and Kostka, "Chinese Investments."

18. Richard Q. Turcsanyi, "Central European Attitudes towards Chinese Energy Investments: The Cases of Poland, Slovakia, and the Czech Republic," *Energy Policy* 101 (February 2017): 711–22, https://www.sciencedirect.com/science/article/pii/S030142151630502X.

Moreover, China's efforts at market dominance are present in several sectors of Italy's renewable energy portfolio, with companies such as China's Three Gorges (CTG) expanding its wind portfolio with a 49 percent stake in EDP's wind projects in Italy.[19]

As Chinese private companies increase their share in Italy's renewable energy market, they are subject to a complex set of Chinese laws that raise cybersecurity concerns for Italy. For instance, new regulations being considered by the Chinese government include those which require companies operating in and out of China to disclose cybersecurity preparations and the security of their networks in other countries.[20] This requirement would entail Chinese distributors having to disclose to the Chinese government their infrastructure in Italy. While this action would certainly augment China's cybersecurity capabilities, it could potentially expose sensitive information about the Italian operations of these Chinese contractors to the Chinese government's scrutiny. Cooperation with Chinese contractors brings about important security considerations.

Moreover, as both Chinese SOEs and private enterprises work with state decisionmakers, extensive cooperation on renewable-energy technology advancements comes with important considerations of security partnerships. This cooperation is especially pertinent to Italy and other EU member states, as China falls outside the European security alliance network. In addition to the security risks, an increase in FDI inflow also enables greater Chinese influence on Italian company boards, with Chinese state-owned and state-supported entities holding influence on Italian companies' management, key strategic decisions, and sensitive information.[21]

The influence of FDI on Italian industry can manifest, for instance, in increased supply-chain sourcing from Chinese manufacturers. In some renewable-industry technologies, the Chinese supply of critical raw materials has indicated long-term risks to Italian wind- and solar-energy industries. Italy has rapidly increased its reliance on Chinese raw materials for its development of renewable-energy technology. To this end, its sourcing of five critical raw materials from China—tellurium, gallium, and indium (used in making solar cells) and neodymium and dysprosium (used in

19. Simon Nicholas, *China Is Investing Heavily in European Wind: Asian Superpower's Renewable Energy Ambitions Go Beyond Its Belt and Road Initiative* (Lakewood, OH: Institute for Energy Economy and Financial Analysis, August 2018), http://ieefa.org/wp-content/uploads/2018/08/China_Research_Brief_August-2018.pdf.

20. Bill Goodwin, "Chinese Law May Require Companies to Disclose Cyber-security Preparations outside China," Computer Weekly (website), July 3, 2020, https://www.computerweekly.com/news/252485674/Chinese-law-may-require-companies-to-disclose-cyber-security-preparations-outside-China.

21. Conrad and Kostka, "Chinese Investments."

manufacturing offshore wind turbines)—is at elevated risk of future supply bottlenecks and price spikes.[22]

As China possesses the only integrated mine-to-magnet value chain in the world, it is currently one of the largest suppliers for Italy's energy transition to solar and wind energy. Italy is the fifth-largest importer of rare-earth metals from China and is extensively sourcing certain critical materials (such as dysprosium, for which China supplies nearly 99 percent of the world supply).[23] The current sourcing relationship with China poses a risk to Italy's supply-chain planning, as the Chinese government augments state control of raw materials and plans to increase prices to factor the environmental and health externalities incurred in processing and exporting.[24] The rate at which Italy and other countries—the United States, South Korea, Japan, and the Netherlands—rely on Chinese raw-material exports for the fulfillment of renewable-energy technologies raises concerns of future supply shortages and anxieties about Italy's engagement in wind and solar energy expansion. As Italy signed the Chinese Belt Initiative in March 2019, which includes deals in the energy and gas sectors, it should employ an understanding of the current Italy-China supply-chain relationship in defining this partnership. Specifically, Italy may consider the degree to which it continues to engage with Chinese suppliers and whether an active diversification strategy should be taken into account as it progresses toward 2030.

5G Technology Vulnerabilities

5G networks enable the transition to machine-to-machine communication, supporting voice and digital conversations, the sharing of data, and a multitude of vertical markets and technology areas such as the Internet of Things, telemedicine, smart cities, and autonomous vehicles. Italy has already held 5G multiband spectrum auctions, a key step for the expansion of 5G networks throughout the country. This is a clear indicator of progress, with 5G carrying great potential to change the economy and directly boost productivity

22. Wiebke Rabe, Genia Kostka, and Karen Smith Stegen, "China's Supply of Critical Raw Materials: Risks for Europe's Solar and Wind Industries?," *Energy Policy* 101 (February 2017): 692–99, https://www.sciencedirect.com/science/article/abs/pii/S0301421516304852#bib37.

23. "Does China Pose a Threat to Global Rare Earth Supply Chains?," ChinaPower Project (website), May 12, 2021, https://chinapower.csis.org/china-rare-earths/.

24. Rabe, Kostka, and Stegen, "China's Supply."

from $3.9 trillion in 2018 to $4.8 trillion in 2023.[25] This rollout should be conducted with caution, however, as the interconnectivity inherent to 5G technology also poses cybersecurity risks and presents high vulnerabilities to compromise. As 5G increases the potential vectors of attack, it raises the risk of a negative impact on the economy. Conversely, Italy tackling the 5G security issue can ensure a trustworthy and secure ecosystem for businesses and reduce the costs to industrial espionage. Building a trustworthy 5G environment in Italy would allow for a better business environment and further encourage international investments.

To this end, cybersecurity risks in the development of the 5G network are two-fold: supply chains and infrastructure and services. 5G supply-chain networks involve the sourcing of critical materials, including processors, memories, chipsets, integrated circuits, capacitors, resistors, and batteries from a wide range of global suppliers.[26] The expansive nature of supply-chain networks for 5G technology invites considerable challenges for the maintenance of cybersecurity in Italy. The physical components of 5G technologies consist of software integration combined with the hardware components to compose the final product curated by original equipment manufacturers. Hardware components are often sourced by international suppliers. Huawei, one of the primary Chinese contractors in Italy, has nearly 150 global suppliers and its component networks have several software and hardware providers.[27]

To this end, the large network of 5G suppliers significantly increases cybersecurity concerns. In 2019, the Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board warned of significant technical issues with Huawei's engineering processes in software development and that these issues would materialize into long-term risks for national security.[28] This acknowledgment came on top of the December 2019 report by Italy's Parliamentary Committee for the Security of the Republic (COPASIR), which expressed similar concerns about Huawei and ZTE's potential security threats at the hardware, software, and installation level of 5G development. The concerns raised by both bodies invite extensive inquiry into future supply-chain and sub-chain networks in software and hardware component vetting. It is critical to remember that the supply chain is the most significant attack surface for a product,

25. European House – Ambrosetti, *5G and Security in Italy: An Overview of Problems and Possible Remedies* (Cernobbio, IT: European House, November 2019), 2, https://www.sipotra.it/wp-content/uploads/2019/11/5G-and-security-in-Italy.-An-overview-of-problems-and-possible-remedies.pdf.

26. European House, *5G and Security in Italy,* 12.

27. European House, *5G and Security in Italy,* 12.

28. European House, *5G and Security in Italy,* 24.

especially as primary suppliers such as Huawei, ZTE, Nokia, Ericsson, and Samsung currently have extensive control over the sourcing process.[29]

A second vulnerability in 5G technology involves the maintenance and configuration of telecom infrastructure. Telecom network equipment enables devices to be installed and maintained, such that network devices' firmware and software are able to be updated periodically. The installation of telecom network equipment is complex and difficult to configure, update, and troubleshoot, often leaving the vendor representatives best equipped to complete the task. Previously in Italy, companies such as Huawei subcontracted their maintenance contracts to service providers. As telecom providers lose network control skills and updates become more specific to hardware infrastructure, the process will again largely depend on subcontracting vendors. Currently, Italian telecom providers use over 100 subvendors.[30]

Firmware updates in telecom may involve patching new releases into networks, which presents risks and transition period access to attackers who can install malicious firmware updates. Italy's contracting of companies that practice maintenance subcontracting increases security risks due to the large number of agents, vendors, and contractors with access to sensitive information on the firmware and network. ASUS, for instance, a Taiwanese original equipment manufacturer with operations in Italy, inadvertently sent malware to hundreds of thousands of customers through an automatic software update tool after the company's server was compromised by attackers, who used the vantage to push malware directly to machines.[31] In this manner, threat groups can take "Trojan" software updates designed for industrial networks and push them onto 5G infrastructure—as Italy's 5G firmware and software are updated over time to account for security patches and efficiency, considerations of vulnerabilities brought by the subcontracting maintenance process and the potential for malicious software entering the update stream should inform the monitoring and vetting of telecom maintenance processes.

A report by Italy's Parliamentary Committee for the Security of the Republic (COPASIR) further identified the most pertinent risks to cybersecurity in Italy, including the use of the TOR network, which allows for illegal

29. European House, *5G and Security in Italy,* 7.

30. European House, *5G and Security in Italy,* 12–15.

31. Kim Zetter, "Hackers Hijacked ASUS Software Updates to Install Backdoors on Thousands of Computers," Vice (website), March 25, 2019, https://www.vice.com/en/article/pan9wn/hackers-hijacked-asus-software-updates-to-install-backdoors-on-thousands-of-computers.

activities and intrusions to be carried out anonymously (this is enabled by mechanisms whereby offensive software is broken down into unidentifiable pieces that take different paths to reach the firmware).[32] Examples of such viruses that could impact Italy include WannaCry, which spread to countries around the world in 2017 and affected computer stations in public administration (such as hospitals and universities). WannaCry virus could have been brought to Italy through the installation of backdoors on Huawei's supply of devices to Vodafone Italia—viruses such as WannaCry encrypt the access keys of the infected system and then follow the request for ransom to recover its data assets.

Viruses such as WannaCry are especially penetrable during the updating and reconfiguration stages. The COPASIR report builds on this vulnerability in its assertion that international suppliers (such as Huawei) pose significant cybersecurity risks to technological infrastructure. Moreover, though Huawei Italia later asserted there is no internal regulation that authorizes the Chinese government entities to induce manufacturers to install hardware or software, there is currently conflicting information on this matter—some evidence suggests the Chinese government and intelligence structures can and have relied on the collaboration of constituent citizens and businesses.[33] This conflict surfaces, again, a recurring concern in partnering with China on the achievement of technological goals. The Chinese government's relationship with private and public enterprises is not fully known, and empirical evidence suggests considerable cooperation between the agents. The unknown nature of Chinese government/supplier cooperation could pose a significant conflict of interest for Italy's vendors from the country.

Public-private sector and EU cooperation in vetting vendors, identifying crime figures, and collecting and implementing threat intelligence will be critical in the future development of 5G technologies. Upon recommendations and findings on Huawei, Telecom Italia (TIM), one of the largest telecom operators in Italy, has excluded Huawei from a public procurement call for 5G network development in July 2020.[34] What the action demonstrates is a willingness of Italian telecom providers

32. COPASIR, "Relazione sulle politiche e gli strumenti per la protezione cibernetica e la sicurezza informatica, a tutela dei cittadini, delle istituzioni, delle infrastrutture critiche e delle imprese di interesse strategico nazionale," December 12, 2019, 17, https://parlamento18.camera.it/228.

33. COPASIR, "Relazione sulle politiche."

34. Elvira Pollina, "Exclusive: TIM Excludes Huawei from 5G Core Equipment Tender," Reuters (website), July 9, 2020, https://www.reuters.com/article/us-huawei-tech-5g-italy-brazil-exclusive/exclusive-tim-excludes-huawei-from-5g-core-equipment-tender-idUSKBN24A2AE.

to receive and implement security intelligence from the national government and the EU. This action reinforces the warrant for state investment in vendor vetting and security intelligence about malicious actors. As the impact of security breaches would affect public operations, the Italian government is best positioned to collect and disperse security advice to 5G developers, providers, and end users of the infrastructure.

Early Warning Systems

The Italian Security Intelligence Department (DIS) has noted in its annual reports that cyber-espionage activities against government entities and industry have grown in scale, volume, and sophistication.[35] Italy's cyber-response system is guided by its administrative and personnel architecture for early detection and alert dispersal. The Inter-Ministerial Committee for the Security of the Republic (CISR) advises the Prime Minister on cybersecurity matters and is supported by the Technical Committee for the Security of the Republic (T-CSIR).[36] T-CSIR enables the implementation of the cybersecurity national plan by collecting and analyzing data from public and private entities, recognizes vulnerabilities in cyber infrastructure, and targets cyber threats. The Security and Intelligence Department oversees and coordinates activities of the External Intelligence and Security Agency (AISE) and the Internal Intelligence and Security Agency (AISI). The Cyber Security Unit (NSC) is an interagency and intergovernmental organization responsible for preventing and preparing for national cyber-crises and coordinating responses in the public and private sectors. Within the NSC, the early warning and cyber incident response unit is responsible for detecting and responding to cyber crises. The NSC collects notifications of cybersecurity concerns internationally and evaluates the severity of incidents and their likelihood of impacting domestic structures and private/public organizations.[37]

These agencies have worked effectively to monitor technologies and coordinate responses across sectors. The Italian Computer Security Incident Response Team (CSIRT- Italia) works in information sharing and coordinating responses in early detection of large-scale compromises. CSIRT-Italia

35. Melissa Hathaway et al., *Italy Cyber Readiness at a Glance* (Arlington, VA: Potomac Institute for Policy Studies, November 2016), 4, https://potomacinstitute.org/images/CRI/PIPS_CRI_Italy.pdf.

36. Hathaway et al., *Italy Cyber Readiness.*

37. Samuele De Tomas Colatin, *National Cybersecurity Organisation: ITALY*, National Cybersecurity Governance Series (Tallinn, EE: NATO Cooperative Cyber Defence Centre of Excellence, 2020), 14, https://ccdcoe.org/uploads/2020/04/NCS_organisation_ITA_2_0_FINAL.pdf.

underwent a transition phase in 2018 as what were formerly the National CERT and Public Administration CERT merged to centralize monitoring, threat detection, prevention, and response systems in one unit. This new joint entity is especially critical in centralizing the detection of malicious intrusion across national and private bodies and information sharing. In October 2019, for instance, the Public Administration CERT section launched an information-sharing platform to encourage automated transmission of indicators of compromise among national public authorities.[38] The National Anti-crime Centre for the Protection of Critical Infrastructure (CNAIPIC) is responsible for overseeing and protecting the national critical infrastructure against cyberattack. CNAIPIC is further effective through its participation in Interpol and Europol collaboration and information-exchange systems and is the Italian representative and point of contact to foreign police departments.

By investing in the entities described above, Italy has moved in the right direction in ensuring a reliable personnel capability and developing response coordination mechanisms among private and public enterprises. CNAIPIC, for instance, is investing in expanding protocol and agreement with private-sector parties to ensure transparency and coordinated response in protecting critical national infrastructure. CNAIPIC and other government entities have solidified public-private cooperation in ensuring cybersecurity of critical national infrastructure and have set a road map for future areas of cooperation in security.

The early warning personnel architecture discussed above is especially important in combating threats to national infrastructure (such as pipelines). In 2016, for instance, the Anonymous hacker collective launched distributed denial of service and cyberattacks on local authorities who participated in the Trans Adriatic Pipeline project and corresponding government portals. The collective specifically targeted the Apulia and Basilicata regions of Southern Italy.[39] Thankfully, response systems detected the attacks at an early stage, allowing the portal's IT administrators to shut down the portal temporarily. Although the attack was not conducted on the pipeline itself, hacktivists (hackers who conduct operations to signal discontent with an issue), admitted to conducting the attack to express frustration

38. Colatin, *National Cybersecurity Organisation: ITALY.*

39. Edward Segal, "7 Crisis Management Lessons from Colonial Pipeline's Response to Cyber Attack," *Forbes* (website), May 10, 2021, https://www.forbes.com/sites/edwardsegal/2021/05/08/colonial-pipeline-cyberattack-is-providing-crisis-management-lessons-in-real-time/?sh=5032154b3d82; and Catalin Cimpanu, "Anonymous Attacks Italian Government Portals Because of Gas Pipeline Project," Softpedia News (website), February 25, 2016, https://news.softpedia.com/news/anonymous-attacks-italian-government-site-because-of-gas-pipeline-project-500977.shtml.

with the negative environmental impact of state pipeline infrastructure, pointing to a deep-seated sentiment that could resurface as further cybersecurity threats for Italy's pipelines and other public infrastructure.[40]

Energy cybersecurity is especially important for Italy since it is a major oil refining contributor to Europe with a total of 13 crude-oil refineries.[41] Current cybersecurity concerns on pipelines are incredibly pertinent and relevant to Italy. The recent Colonial Pipeline attack that took place in May 2021, for instance, could potentially be linked to DarkSide and Adhubllka ransomware, the former of which has already attacked Banca di Credito Cooperativo, a large Italian cooperative credit bank.[42] Thus, the risks of future attacks are imminent, and with Italy's pipelines (TAG, TransMEd, and Transitgas) and extensive public infrastructure, early warning systems are critical in detecting malicious activity at early stages and preventing harm to critical public infrastructure.

Recommendations

Renewable Energy Management

1. **FDI Vetting:** Law Decree No. 23 of April 2020 has already widened the scope of application in FDI screening to protect national security and public order. This decree came after Law Decree No. 105/2019, which had already expanded the scope of the Golden Power Law to extend the Italian government the power to assess companies holding strategic partnerships in sectors in security, defense, energy, transport, communications, or 5G networks, as well as other areas introduced by EU Regulation No. 452/2019. This extension was hampered by shortcomings in identifying "relevant strategic assets in those newly-introduced sectors."[43] Provisions set forth under Article 15 of the new Law Decree should be employed and enforced to monitor investment transactions and impact

40. Cimpanu. "Anonymous Attacks Italian Government."

41. US Energy Information Administration (EIA), "International: Italy," EIA (website), August 2017, https://www.eia.gov/international/overview/country/ITA.

42. Pierluigi Paganini, "An Alleged Ransomware Attack Hit the Italian Banca di Credito Cooperativo Causing Chaos," Security Affairs (website), April 29, 2021, https://securityaffairs.co/wordpress/117360/cyber-crime/banca-di-credito-cooperativo-darkside-ransomware.html.

43. "Newsalert – Foreign Direct Investments Screening: Italy Expands Its 'Golden Powers' to New Key Sectors," Chiomenti (website), April 9, 2020, 3, https://www.chiomenti.net/en/publications/newsalert-foreign-direct-investments-screening-italy-expands-its-golden-powers-to-new-key-sectors.

on strategic sectors. As the article defines critical infrastructure in energy, critical technologies including energy storage (Article 2, No. 1 of Council Regulation), and the security of supply of critical inputs (*fattori produttivi*), including energy and raw materials, must be screened and managed at the national level.[44] While the provision does ensure that companies holding investment relationships or assets in the energy sector are required to disclose the nature and extent of partnerships to the Presidency of the Council of Ministers, it is advisable the Council gather, process, and assess the security implications of specific partnerships proactively and enforce guidelines accordingly. FDI vetting findings and recommendations should further be published and made accessible to both international investors and domestic market agents.

2. Diversification of raw-material sourcing. Diversification in the sourcing of critical raw materials will also aid in the long-term sustainability and security of renewable energy technologies in Italy. EU efforts are already promoting the research consortium "Replacement and Original Magnet Engineering Options" (ROMEO) that consists of 15 research centers and manufacturers with the aim to develop rare-earth-free magnets.[45] Long-term recycling efforts of critical materials that seem promising for minerals (such as indium and gallium) can largely be sourced from CIGS post-industrial scrap.[46]

Wind industries, too, are developing alternate technologies that are less reliant on the use of the neodymium and dysprosium currently extensively sourced from China. Private companies in other EU member states (such as Germany's turbine manufacturer Nordex) have already made strides in reducing their reliance on China by substituting magnet technologies to reduce the usage of Chinese mineral exports.[47] Similar efforts can be promoted and funded at the national level for Italy's renewable energy players as well. In addition to recycling minerals, Australia, Brazil, Canada, South Africa, and

44. Chiomenti, "Newsalert," 5.

45. Rabe, Kostka, and Stegen, "China's Supply."

46. Rabe, Kostka, and Stegen, "China's Supply."

47. Rabe, Kostka, and Stegen, "China's Supply."

the United States also have significant deposits of rare-earth metals, with extraction being the main challenge, as opposed to supply.[48] Alternate deposits exist and can be pursued in the future as international processing and extraction capabilities are augmented.

5G Recommendations

1. Rigorous review process beyond the Golden Power Law. Cybersecurity risks associated with 5G technology involve several vectors of attack and a high negative economic and societal impact potential. A critical item to consider in the development of 5G networks is the Chinese government's relationship with vendors, and the pressures it exerts on the private entities in the 5G development space. Based on the previous risks posed by international vendors, Italy should consider the adoption and enforcement of a rigorous review process beyond the scope of the Golden Power Law. Italy should invest in acting on the design phase of the 5G system in vetting potential vendor contracts and history, auditing vendor processes to reduce the probability of negative occurrences, and testing and simulating critical application systems to achieve a sustainable level of redundancy (this step would involve a joint collaboration between vendors and the CSIRT-Italia with selected vendors).

2. Assessing vendor governance systems. Vendors' governance systems, if they fall outside the EU, should be assessed so the potential influence of the state on their practices is known. Vendors should be assessed on ownership structure and transparency and display the ability to manage state influence by parties of authorities.

3. Assessing technical aspects of vendor competence. Finally, technical aspects of vendor competence should be assessed, including the security of the development life cycle, sustainability, and security of supply chains (including potential malicious third-party components), and the authenticity and integrity of software components. Key recommendations

48. Renee Cho, "Rare Earth Metals: Will We Have Enough?," Columbia Climate School: Climate, Earth, and Society State of the Planet (website), September 19, 2012, https://news.climate.columbia.edu/2012/09/19/rare-earth-metals-will-we-have-enough/.

> by the European House - Ambrosetti, recognized as the best Italian think tank by the University of Pennsylvania in 2021, support the above recommendations by ensuring an assessment of its critical infrastructures for FDI, an audit for the whole supply chain of vendors, and the establishment of a Centre of Expertise for Cyber Threat Intelligence, where threats are detected, contained, and mitigated more quickly.[49]

As suggested in the 5G and renewable management recommendations, a thorough vetting process of vendors and foreign direct investments is critical in ensuring the security of technology development.

Conclusion

Overall, Italy should consider the sustainable development and diversification of its vendors and investors in both the 5G and renewable energy space. In partnerships with countries outside of NATO, rigorous vetting of suppliers and ensuring the integrity of vendors' governance systems and technical capabilities is necessary to avoid falling victim to cybersecurity threats in the future. Both foreign direct investments and supply-chain processes present important considerations for Italy's policymakers, who should work toward strengthening public-private partnerships and information sharing in the cybersecurity space.

49. European House, *5G and Security in Italy*, 32.

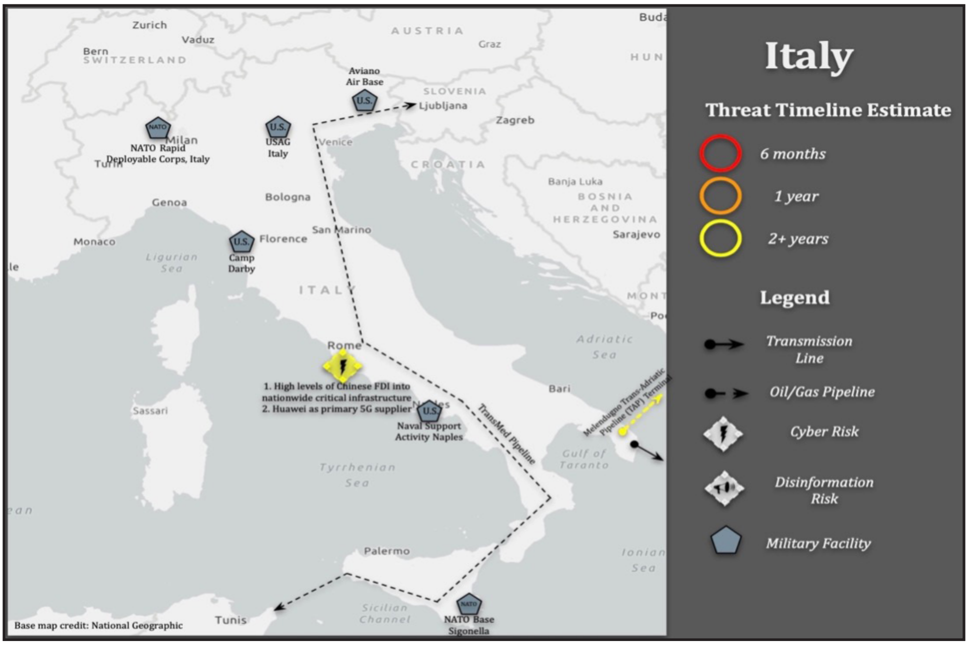

Figure 15-1. Map of Italy's threat timeline estimate (6 months indicates likely attack vector in 2022, 1 year by 2023, 2+ years by 2024 or later)
Credit: Ryan Fisk and Lucas Cox

Location	Reason for Threat Priority and Timeline
Countrywide	Italy, home to several NATO bases, has high levels of Chinese FDI in its infrastructure, and its primary 5G supplier is Huawei. Supply-chain, technical, and communication disruptions over the next two years could be collateral damage in the broader NATO-Russia conflict.
Melendugno Trans Adriatic Pipeline Terminal	As one of the only direct-access points for Southern Europe to gas from Azerbaijan, Russia is likely to intervene to disrupt the energy transition within the next two years.

Select Bibliography

Conrad, Björn, and Genia Kostka. "Chinese Investments in Europe's Energy Sector: Risks and Opportunities?" *Energy Policy* 101 (February 2017). https://www.sciencedirect.com/science/article/pii/S0301421516306711.

De Tomas Colatin, Samuele. "National Cybersecurity Organisation: ITALY." National Cybersecurity Governance Series. Tallinn, EE: NATO Cooperative Cyber Defence Centre of Excellence, 2020. https://ccdcoe.org/uploads/2020/04/NCS_organisation_ITA_2_0_FINAL.pdf.

"Does China Pose a Threat to Global Rare Earth Supply Chains?" ChinaPower Project (website). May 12, 2021. https://chinapower.csis.org/china-rare-earths/.

European House – Ambrosetti. *5G and Security in Italy: An Overview of Problems and Possible Remedies*. Cernobbio, IT: European House, November 2019. https://www.sipotra.it/wp-content/uploads/2019/11/5G-and-security-in-Italy.-An-overview-of-problems-and-possible-remedies.pdf.

Goodwin, Bill. "Chinese Law May Require Companies to Disclose Cybersecurity Preparations Outside China." Computer Weekly (website). July 3, 2020. https://www.computerweekly.com/news/252485674/Chinese-law-may-require-companies-to-disclose-cyber-security-preparations-outside-China.

Parliamentary Committee for Security of the Republic. "RELAZIONE: sulla tutela degli asset strategici nazionali nei settori bancario e assicurativo," XXXIV RELAZIONE: sulla tutela degli asset strategici nazionali nei settori bancario e assicurativo § (2020).

Rabe, Wiebke, Genia Kostka, and Karen Smith Stegen. "China's Supply of Critical Raw Materials: Risks for Europe's Solar and Wind Industries?" *Energy Policy* 101 (February 2017). https://www.sciencedirect.com/science/article/abs/pii/S0301421516304852#bib37.

— 16 —

Greece

Ryan Fisk

ABSTRACT: With huge volumes of international commerce passing through its ports and as the host of several United States and NATO military facilities within its borders, Greece is a strategically significant country in the hybrid threat environment. Greece has an import-heavy economy and has seen an increase in foreign direct investment into critical infrastructure (such as in the case of China's majority stake in the Port of Piraeus). In addition, the country has a heavy reliance on external sources of energy, which could be used against the country and the Alliance. Combined with low apparent effort to secure its critical infrastructure against hostile actors, Greece's energy security, and therefore NATO's, is at an increased risk.

Keywords: Hellenic Electricity Transmission System, China port investing, GRNET, Port of Piraeus, Port of Thessaloniki, PIXEL, Internet of Things, China State Grid Corporation

Introduction and Energy Landscape

Greece is a NATO and an EU member, and the United States and NATO have a military presence in the country. Also known as the Hellenic Republic and located in the southern Balkans, it is a country of strategic value for NATO. It is bordered by Albania, North Macedonia, and Bulgaria to the north, and Turkey to the east. All bordering countries are NATO member states. Historically, Greece's economy has been fragile, and it has had major financial and debt crises in recent history.

There are several military facilities of note to NATO operations. The NATO Deployable Corps Greece in Thessaloniki is rapidly deployable and supports 1,500 troops. Another significant facility is located in Souda Bay on the island of Crete. The United States Navy has a Naval Support Activity base at Souda Bay, which supports maritime and air operations across the region. In addition, a combat wing of the Hellenic Air Force and the NATO Maritime Interdiction Operational Training Centre are located at the same facility.[1] Direct US-Greek defense cooperation has increased in recent years: MQ-9 Reapers began flights out of Larisa Air Force Base in 2018, and bilateral troop exercises happen with increasing frequency.[2]

Currently, Greece relies mostly on natural gas to generate electricity.[3] It also produces electricity from coal and has a significant share of renewable energy production, approaching 20–30 percent of domestic production. The renewable sources are diversified into wind, solar, hydropower, and biofuel. Diversification is an advantageous way to increase redundancy and ensure that cyberattacks must engage more than a single target.

A large share of energy consumed in Greece is from imported sources. The majority of oil, for example, is imported from Iraq, Kazakhstan, Russia, and Iran.[4] Some LNG is imported via cargo ship, while pipelines carry the supply from Azerbaijan and Russia.

The operation of Greek electricity infrastructure (the Hellenic Electricity Transmission System, HETS) is managed by the Independent Power Transmission Company (IPTO). IPTO is responsible for managing the mainland power grid, implementing interconnections to outlying Greek islands and managing international interconnections.[5] In addition, it is responsible for connecting outlying Greek islands (that currently independently rely on fossil fuels) to the main power grid to reduce their emissions and provide better stability.

As part of the international bailout after its financial crisis, Greece was required to privatize ownership of its power grid. To this end, ADMIE Holdings was created to obtain a 51 percent stake in IPTO. Another 25 percent stake was sold directly to the state. China's State

---

1. "Greece," NATO SHAPE (website), n.d., https://shape.nato.int/greece.

2. Nektaria Stamouli, "U.S. Military Finds a Warm Welcome in Once-wary Greece," *Wall Street Journal* (website), February 4, 2019, https://www.wsj.com/articles/u-s-military-finds-a-warm-welcome-in-greece-11549319286.

3. "2020 Fossil Fuel Support Country Notes: Greece," Organisation for Economic Co-operation and Development (website), 2020, https://www.oecd.org/fossil-fuels/data/.

4. "Fossil Fuel Support Country Notes: Greece."

5. "About Us," Independent Power Transmission Operator (website), n.d., https://www.admie.gr/en/company/about-us.

Grid Corporation, the largest utility company in the world and an SOE, bought a 24 percent stake in IPTO in 2016.[6] While that is still a minority stake, China has sought the further acquisition of additional stock at the Port of Piraeus, and it is possible the same could occur in its shares of IPTO. IPTO manages multiple grid interconnections with neighboring countries Italy, Albania, North Macedonia, Bulgaria, and Turkey. Electricity is imported from Turkey, Bulgaria, and North Macedonia. Exports go to Albania.

Port Security and Internet of Things Integration

In recent years, China has taken a major interest in increasing shipping and commerce connections to Greece. In 2016, Cosco, a Chinese shipping SOE, bought a 51 percent stake in the Port of Piraeus, Greece's largest port and one of the largest ports in Europe.[7] Cosco has committed to investment in the port facilities in the years since. In addition, pending delays, Cosco hopes to purchase another 16 percent share. The acquisition of the Port of Piraeus, a capstone of the Belt and Road Initiative, shows the effects of the BRI are not absent from NATO countries.

Internet of Things (IoT) business and integration into infrastructure in Greece is forthcoming. There is no real integration of IoT into critical infrastructure yet, but the Greek government has shown it is willing to fund initiatives that prioritize the integration of digital technologies; IoT would likely be a part of this effort.

Greece's ports have begun to adopt IoT into their infrastructure to improve efficiency, offer better management of cargo logistics, and better manage the impacts a port can have on its surrounding areas. PIXEL, an EU-funded research project intended to study the potential IoT has in making these improvements, has partnered with the Port of Piraeus and the Port of Thessaloniki in testing and adopting IoT.[8] PIXEL is intended to be an upgrade to the existing port community service data exchange facilitation service. The project will connect stakeholders like the port authority, cargo ships, the surrounding community, and other infrastructure

6. Angeliki Koutantou and Mark Potter, "China's State Grid Seals Purchase of Stake in Greek Power Grid," Reuters (website), 2016, https://www.reuters.com/article/us-public-power-m-a-state-grid-corp/chinas-state-grid-seals-purchase-of-stake-in-greek-power-grid-idUSKBN1451SM.

7. Costas Paris, "China's Cosco Pours More Money Into Greek Port," *Wall Street Journal* (website), November 12, 2019, https://www.wsj.com/articles/chinas-cosco-pours-more-money-into-greek-port-11573581625.

8. "PIXEL – Where IoT Meets the Port of the Future," PIXEL (website), n.d., https://pixel-ports.eu.

through IoT sensors. Data collected from the sensors will be used in a centralized dashboard that allows port operators to control and organize logistics for maximum efficiency.

The Port of Piraeus and the Port of Thessaloniki, the two Greek ports involved in PIXEL, are test ports for a PIXEL initiative that focuses on successfully managing the port's impact on the surrounding community.[9] To achieve this goal, there are several target functions IoT will assist in creating a traffic-management software that can predict when a ship or cargo arrival will create bottlenecks and successfully reduce traffic, predicting when emissions will increase due to port activity and successfully managing operations to mitigate them, and the fusion of data from the port as a whole with rail and road activities to create a more cohesive real-time view of holistic management.

While a full deployment of IoT into Greece's ports is not yet a reality, it is entirely possible. That reality, combined with the Chinese stake in Greek commerce, would create the risk that NATO and Greece could lose control of critical assets at opportune times for adversaries.

Vulnerabilities and Trajectories for Hostile Influence

Greece's high reliance on imports is an inherent vulnerability to the security of the energy supply. Energy dependence is an issue that could be exploited to degrade Greece's ability to respond in support of NATO action.

Second, the PIXEL program has the potential to open up an entirely new threat surface that hostile actors could target. Zero-day vulnerabilities in any of the sensors, management dashboard, or anything connected to that system could be exploited to disrupt shipping and commerce. Especially considering the volume of commerce that passes through the Port of Piraeus, a new and potentially vulnerable system could be an attractive way to carry out an attack against Greece or even NATO readiness.

Third, the increasing Chinese foreign direct investment in Greek infrastructure carries risks. The Port of Piraeus and the entire operation of the Greek electricity grid now have a measure of open Chinese influence attached to them. With the majority stake, Piraeus is now effectively controlled by China, and the stake in IPTO gives it increased influence as well.

9. "Port-City Integration: Use Cases," PIXEL (website), n.d., https://pixel-ports.eu/wp-content/uploads/2019/03/PIXEL_UC_PortCity.pdf.

Should NATO or Greece enter into any form of dispute with China, Beijing could use these assets as leverage.

With a location in a volatile region and a large US-NATO military presence, Greece has the potential to be a target for information operations. Concerning Russia, a likely target for disinformation could be the relationship between Greece and the EU. The austerity measures imposed on Greece as a condition for the EU to bail the country out of its debt crisis were unpopular, and Russia has already attempted to use the increased Euroscepticism to gain a better foothold in the country. The previous Greek government, the Syriza-led coalition, had discussions with the Russian government about pivoting away from the EU for bailout support.[10] Russia, however, was not in a financial position to follow through at that time. Combined with an already sympathetic Greek public, information that portrayed the EU as detrimental to Greek interests could find a foothold. Considering Greece's strategic location, vulnerabilities in its infrastructure are vulnerabilities in NATO readiness and troop mobility and should be addressed as such.

Early Warning and Mitigation

The Greek federal government has several organizations tasked with handling cyberspace-related incidents and providing mitigation and recovery services. The first and most prominent organization is the Hellenic CSIRT. It is the most involved CERT in Greek government and infrastructure and would be the most involved response organization in the event of a cyberattack on Greek infrastructure, communications, or anything else that impacts the federal government or daily life.[11]

Second is GRNET-CERT, the CERT for the Greek National Infrastructures for Research and Technology. It focuses on mitigation for Greek research institutes, universities, and educational organizations.[12]

In addition to cybersecurity-specific mitigation, Greece has begun coordinating with countries it exchanges electricity with to ensure a continuous flow. The IPTO recently joined in the creation of a Regional Security Coordinator

10. Paul Stronski, "A Difficult Balancing Act: Russia's Role in the Eastern Mediterranean," Carnegie Endowment for International Peace (website), June 2021, https://carnegieendowment.org/2021/06/28/difficult-balancing-act-russia-s-role-in-eastern-mediterranean-pub-84847.

11. "Large Organizations and Infrastructure," Hellenic CSIRT (website), n.d., https://csirt.cd.mil.gr/large-organizations-infrastructure/.

12. "GRNET-CERT Profile," GRNET CERT (website), 2019, https://cert.grnet.gr/wp-content/uploads/2019/12/rfc.pdf.

center headquartered in Thessaloniki. The Regional Security Coordinator is a joint venture between the TSOs of Bulgaria, Greece, Italy, and Romania.[13] In addition to managing the successful balancing of electricity exchange in the region, it is intended to promote operational security between grids. A center in which TSOs have a real-time view of grid interconnections and energy production from different sources, the RSC can suggest action to the domestic grid operators to minimize the risks of interrupting supply.

While Greece has these organizations in place to reduce the impacts of a cyberattack, it is unclear whether there is a national-level early warning system in place to anticipate and react to a cyberattack on critical infrastructure or other important systems. The National Cyber Security Strategy, created and released as a requirement of the NIS Directive, mentions early warning systems but only in the context of development or that the responsibility to operate such a system would fall on the national CERT.[14]

If there is no national early warning system in place to prevent threats, critical infrastructure is at increased risk.

Policy Recommendations

1. For NATO, Greece is a location of strategic significance. For this reason, a high dependence on external sources of energy increases the chances that dependency could be exploited in a time of conflict or increased agitation between NATO and a hostile actor. The most effective way to address this problem is through accelerating the transition to renewable energy in order to increase energy independence. Without the risk of suddenly losing access to necessary natural gas, for example, Greece would be able to better support NATO operations and deployments. Until that transition is complete, Greece is at risk.

2. The PIXEL program needs to explore the risks of its integration into a geopolitically volatile environment. For example, how could the sensors be exploited to cause a shipping jam and disrupt global commerce? While the potential

13. "Establishment of the Regional Security Coordinator in Thessaloniki, Greece," ENTSO-E: European Network of Transmission System Operators for Electricity (website), 2019, https://www.entsoe.eu/news/2019/12/20/establishment-of-the-regional-security-coordinator-in-thessaloniki-greece/.

14. "ΕΘΝΙΚΗ ΣΤΡΑΤΗΓΙΚΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ 2020–2025," Greek National Cybersecurity Authority, ENISA: European Union for Cyber Security, 2019.

for increased efficiency through PIXEL is large, IoT opens new vulnerabilities. In analyzing the impact that PIXEL will have on a security landscape (if it progresses past trials and eventually enters a more ingrained operational status), the unified interface that brings together IoT sensor data throughout the ports and the city is a system that needs to take security as a first priority. Such a large breadth of data collection should be very closely monitored so large-scale abuse of the system does not occur. In addition, any Greek early warning system would do well to consider a full-scale integration of PIXEL technology a priority.

A similar style of consideration should be adopted for any form of further IoT development as a whole. Greek critical infrastructure is not yet at the point of IoT integration in which a hack could cause a major disruption to daily life or the economy, but IoT that is being developed to manage those areas needs to take security considerations into account.

3. Foreign direct investment into Greek infrastructure needs to be closely monitored to look for signs of exploitation or the potential for exploitation in a conflict or tense situation. Especially when considering the volume of commerce passing through the Port of Piraeus, potential risks should be evaluated. In a situation in which China would need to apply geopolitical pressure to Greece or the EU, it could use its ownership of the port as a stick and a carrot.

4. The development of a cyber early warning system focused on the defense of energy infrastructure should be prioritized. As time passes and the capabilities of hostile actors to interfere with energy security increase, the ability to prevent at least a portion of attacks is crucial to maintaining energy security for NATO and the Greek population. This risk is compounded by the IoT integration into the ports in the country—as IoT develops, the early warning system needs to integrate into places (like the Port of Piraeus) where the risk of a cyberattack has been increased. It is positive an early warning system is on the Greek government's radar; however, concrete action is required soon.

In the case that an early warning system is present but not clearly disclosed, there should be an effort to increase transparency. Increased transparency would increase confidence in Greek cybersecurity and potentially serve as a deterrent to hostile actors in cyberspace.

5. NATO can play a major part in assisting Greece in its development of cybersecurity capability. Lending expertise and resources to the development of an early warning system or ensuring the security of a full deployment of IoT into ports are ways that NATO can support Greece's security and the Alliance as a whole.

Conclusion

Given the level of international commerce passing through Greece's ports and its strategically important geographic position, Greece is at risk of cyberattacks and other activity that is hostile to NATO, the EU, and the country itself. While some steps have been taken to prepare, more detailed and enforceable policies regarding IIoT integration into critical infrastructure are necessary. In addition, foreign direct investment into the country should be vetted more thoroughly to ensure it does not create an unacceptable risk to the country or the Alliance.

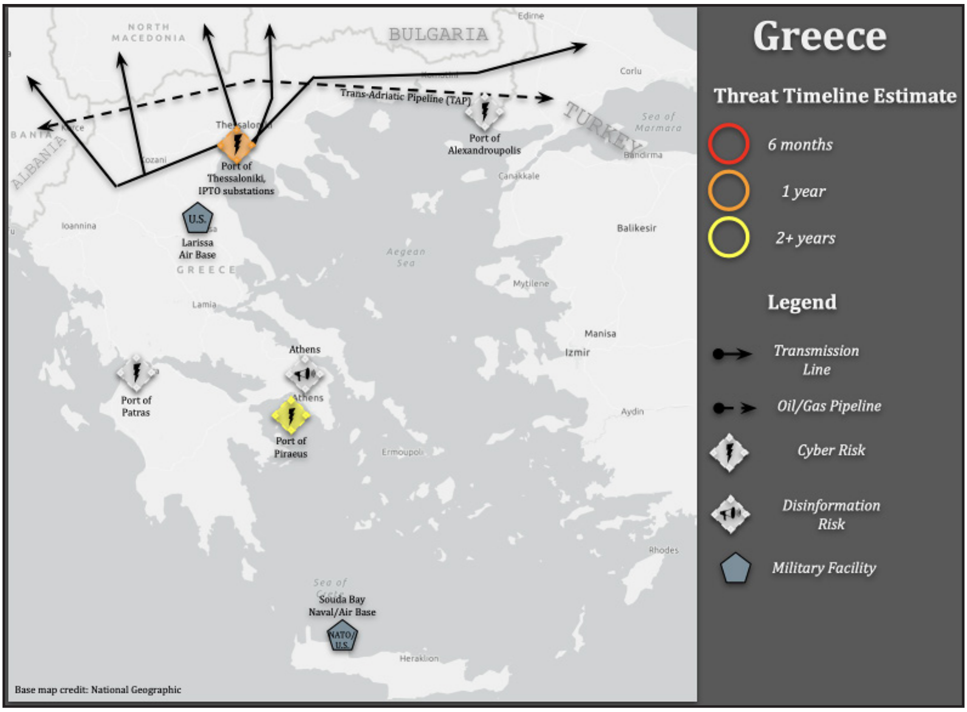

Figure 16-1. Greece threat timeline estimate (six months indicates likely attack vector in 2022, one year by 2023, two+ years by 2024 or later)
Source: Ryan Fisk

Location	Reason for Threat Priority and Timeline
Port of Piraeus	The Port of Piraeus, largely controlled by China, is a test center for large-scale IoT integration into shipping, commerce, and the surrounding community. If a full deployment is implemented after testing, cyber intrusions could disrupt commerce in two years or more.
Port of Thessaloniki, IPTO Substations	Cyber protection of the port's SCADA subsystems will remain vital over the next year. Any attack here could affect the entire port and multiple transmission lines.

Select Bibliography

"ΕΘΝΙΚΗ ΣΤΡΑΤΗΓΙΚΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ 2020–2025." Greek National Cybersecurity Authority. ENISA: European Union for Cyber Security. 2020.

Koutantou, Angeliki. "China's State Grid Seals Purchase of Stake in Greek Power Grid." Reuters (website). June 20, 2017. https://www.reuters.com/article/greece-stategrid-powergrid-idAFL8N1JH32G.

"Greece." NATO SHAPE (website). n.d. https://shape.nato.int/greece.

"2020 Fossil Fuel Support Country Notes – Greece." Organisation for Economic Co-operation and Development (website). n.d. https://www.oecd.org/fossil-fuels/data/.

Paris, Costas. "China's Cosco Pours More Money into Greek Port." *Wall Street Journal* (website). November 12, 2019. https://www.wsj.com/articles/chinas-cosco-pours-more-money-into-greek-port-11573581625.

"Where IoT Meets the Port of the Future." PIXEL (website). n.d. https://pixel-ports.eu.

Stamouli, Nektaria. "U.S. Military Finds a Warm Welcome in Once-wary Greece." *Wall Street Journal* (website). February 4, 2019. https://www.wsj.com/articles/u-s-military-finds-a-warm-welcome-in-greece-11549319286.

Stronski, Paul. "A Difficult Balancing Act: Russia's Role in the Eastern Mediterranean." Carnegie Endowment for International Peace (website). June 2021. https://carnegieendowment.org/2021/06/28/difficult-balancing-act-russia-s-role-in-eastern-mediterranean-pub-84847.

— 17 —

Türkiye

Christopher J. Eaton

ABSTRACT: A NATO member who has provided Ukraine with drones yet has allowed its waters to be used by Russian warships, Türkiye is trying to remain neutral and act as a mediator in the current Ukraine-NATO crisis. A wrong move could compromise Türkiye's energy landscape. Türkiye invested approximately $7 billion into renewable-energy sources, but despite this sizable investment, Türkiye still must import energy primarily from Russia, Iran, and Azerbaijan to meet its domestic energy needs.[1] Türkiye seeks to mitigate the dangers of dependency on these nations by investing in extensive AI-powered early warning systems to govern its smart grids and communications networks. These systems are already bearing the brunt of hundreds of thousands of cyberattacks annually for the purpose of exploiting Türkiye's strategic geographic location. These threats are compounded by the fact that Türkiye does not have very strong cybersecurity legislation, relying mostly on private partnerships to set standards and respond to attacks, leaving significant gaps in security.

Keywords: Turkstream, TANAP, Digital Transformation Office, Turkish Artificial Intelligence Initiative, HackIstanbul, Cyber Star, Southern Energy Corridor, Russian cyberattack, artificial intelligence, AI early warning

Introduction

In the aftermath of World War II, the Republic of Türkiye made the historic choice of siding with the Western Bloc. This move led to Türkiye joining the North Atlantic Treaty Organization on February 18, 1952. Since that date, NATO has been an integral part of the Republic's security

1. Nuran Erkul, "Turkey's Renewable Energy Investments Reach $7B in 2020," AA Energy (website), https://www.aa.com.tr/en/energy/renewable/turkeys-renewable-energy-investments-reach-7b-in-2020/31659.

and defense policy. With the end of the Cold War, the geopolitical landscape radically changed. In this new world, Türkiye found itself in a strategic role as the bridge between Europe and Eurasia, including the Middle East. A key component of this new reality is the mass movement of energy resources from East to West. More importantly, the twenty-first century ushered in vast developments in energy production, security, and alternative/renewable energy sources.

The case study presented here investigates and advises on the cybersecurity situation in Türkiye, with a strong eye toward cybersecurity challenges in the energy sector. More specifically, this case study investigates Türkiye's advancements in artificial intelligence (AI) and its renewable-energy prospects. We analyze the current energy landscape, advancements in artificial intelligence, and renewable energy sources. Next, we investigate vulnerabilities in Türkiye's energy security realm, followed by the many mitigation methods Türkiye employs. Finally, we provide recommendations for improvement.

Current Energy Landscape

Türkiye lacks domestic hydrocarbon reserves and relies very heavily on energy imports. Close to 72 percent of Türkiye's primary energy supplies—oil, natural gas, and coal—are imported.[2] Approximately 29 percent of the country's energy supply comes from oil, 28 percent from coal, and 25 percent from natural gas. Furthermore, the country obtains 17 percent of its total energy from renewable resources, primarily geothermal, with an increasing reliance on hydroelectric.[3] Despite a positive trend toward renewables, the country remains highly reliant on hydrocarbon imports.

2. Riaz Uddin et al., "Energy Storage for Energy Security and Reliability through Renewable Energy Technologies: A New Paradigm for Energy Policies in Turkey and Pakistan," *Sustainability* 13, no. 5 (February 2021): 19, https://doi.org/10.3390/su13052823.

3. Uddin et al., "Energy Storage"; and International Energy Agency (IEA), *Turkey 2021: Energy Policy Review* (Paris: IEA, 2020), 17, https://iea.blob.core.windows.net/assets/cc499a7b-b72a-466c-88de-d792a9daff44/Turkey_2021_Energy_Policy_Review.pdf.

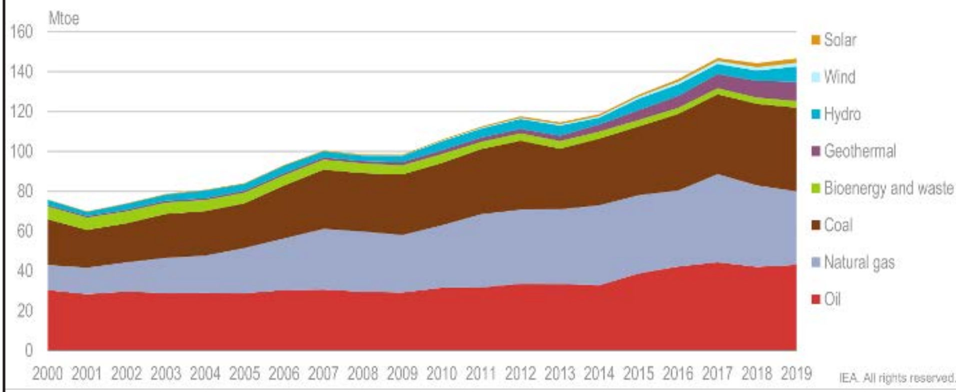

Figure 17-1. Total primary energy supply by source, Türkiye 2000–19
Source: International Energy Agency, "Türkiye 2021: Energy Policy Review," 2020, 20.

Türkiye's primary source of natural gas is the Russian Federation; approximately 63 percent of energy imports come from Russia. Türkiye began importing from Iran in 2001 and Azerbaijan in 2007.[4] Despite diversification, imports from Russia have steadily increased, especially after the completion and activation of the TurkStream pipeline in early 2020. Along with the TANAP pipeline route from Azerbaijan, the two pipelines aid in the diversification of imports (see figure 2). As for oil, Türkiye imports from Iran, Iraq, Russia, and Saudi Arabia. Overall, Türkiye imports 93 percent of its oil and 99 percent of its natural-gas supply.[5]

Naturally, this lack of a domestically controllable energy supply has prompted Türkiye to invest heavily in renewable-energy sources. Electricity production from renewable sources has tripled in the last decade, with close to 44 percent of electricity being produced by solar, wind, and geothermal means.[6] This diversification bodes well for the future in that Türkiye has already exceeded its 2023 goal of 38.8 percent of electricity generation from renewable sources.

At present, the greatest threats to Türkiye's energy security come from its high reliance on foreign energy and from strategically distributed denial-of-service (DDoS) attacks. These attacks can impact local infrastructure,

4. IEA, *Turkey 2021*, 12.

5. IEA, *Turkey 2021*, 11.

6. IEA, *Turkey 2021*, 1; and "Turkey's Cyber Shield: Octopus," TÜBİTAK ULAKBİM Turkish Academic Network and Information Center (website), January 1, 2019, https://ulakbim.tubitak.gov.tr/en/haber/turkeys-cyber-shield-octopus-0.

as well as critical locations abroad, meaning Türkiye can suffer detrimental effects from an attack that occurs well outside its jurisdiction.

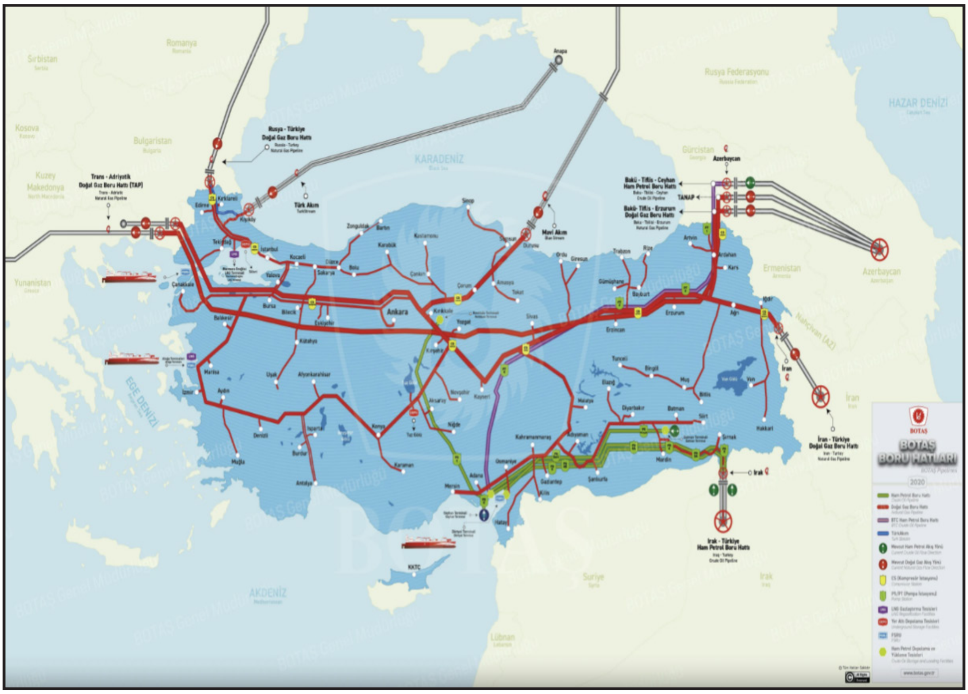

Figure 17-2. Natural gas and crude oil pipeline map
Source: BOTAS (2020)

Alternate/Renewable Energy Sources

Renewables

The Republic of Türkiye has already initiated massive renewable energy development projects. Rightly recognizing the security and energy independence risks associated with relying on energy imports, Türkiye began implementing changes in the early 2000s. Having already attained its 2023 goal of 38.8 percent of electricity from renewables, Türkiye has set a new goal of increasing solar and wind energy capacity to 10 gigawatts by 2027.[7] To achieve this goal, offshore wind projects are already being developed with Finland. Moreover, Türkiye is in a global band that receives an ideal amount of solar radiation for effective photovoltaic generation. The government has demonstrated a desire to repurpose existing land for renewable energy through the Renewable Energy Resource Areas (YKEA). This action

7. IEA, *Turkey 2021*, 13.

allows land that is currently earmarked for other uses, namely, agriculture, to be repurposed—or jointly purposed—for energy production. Moreover, the YKEA grants Türkiye the opportunity to continue its agricultural and industrial production, which is ultimately the cause of increased energy consumption in the country.

Nuclear Energy

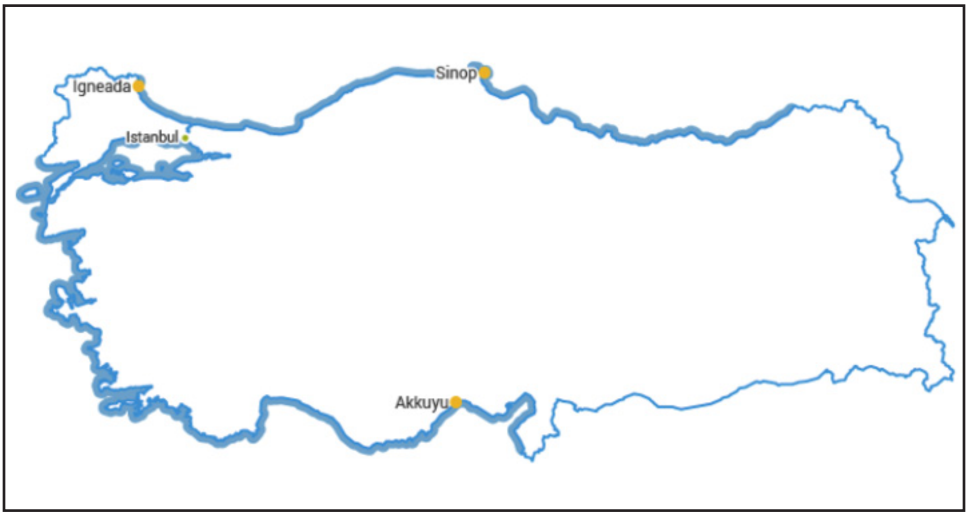

Figure 17-3. Map of potential nuclear energy facilities
Source: World Nuclear Association, "Nuclear Power in Turkey," June 2022, https://world-nuclear.org/information-library/country-profiles/countries-t-z/Türkiye.aspx.

The most immediate major advancement in energy production within Türkiye is the construction of the first nuclear power plant in Akkuyu.[8] Slated to open in 2023, the plant will allow the country to begin producing electricity at a low cost without continual dependence on foreign actors. It is being built with financial aid from Rosatom, Russia's state nuclear power firm. Despite Russia's invasion of Ukraine, Türkiye will continue to build the plant with Russian assistance, as officially condemning Russia would cause too great a strain on the supply chain and broader financial stability. Whether the financial assistance to build the plant will last in light of current sanctions against Russia remains to be seen.

8. IEA, *Turkey 2021*; and George Koukoudakis, "EU Energy Security and Turkey's Contribution to the Southern Energy Corridor," *Mediterranean Quarterly* 28, no. 2 (2017): 106–24, https://doi.org/10.1215/10474552-4164292.

This attempt at nuclear power is not Türkiye's first. Nuclear energy ambitions began as early as 1970.[9] Beyond the Akkuyu plant, a Franco-Japanese consortium is pursuing construction of a second facility in Sinop, while work on a reactor in Igneada, constructed by the Chinese state nuclear corporation and the American firm Westinghouse, has stalled.[10] While Türkiye has few deposits of uranium, it does have very large deposits of thorium—an alternative nuclear fuel source—estimated at 380,000 tons.[11] Thorium reactors are likely one of the main avenues Türkiye will take to move toward future energy independence.

Artificial Intelligence

Türkiye is in the nascent stages of artificial intelligence (AI) development—at least publicly. As in many countries, AI research in the security sector in Türkiye is highly competitive and guarded. This report has already noted the risks of DDoS attacks and vulnerable local infrastructure on the larger Turkish network. Artificial intelligence could be a major boon in terms of rapid response and reaction to cyber intrusions. That said, the government of Türkiye has engaged extensively in AI research, while also investing in other early warning systems to combat cyberattacks.

Launched in mid-2018, the Digital Transformation Office of the Presidency of the Turkish Republic (DTO) was created to coordinate technological and security projects that have potentially great benefits for the entire country.[12] The AI work being monitored by the DTO focuses on energy cybersecurity and economic cyberattacks. Through the DTO, local industry has been encouraged to develop domestic AI programs, advocating for an advanced-technology sector independent of foreign business. Furthermore, the Turkish Artificial Intelligence Initiative (TRAI) has encouraged university and public research into this burgeoning technology field. The initiative finds and promotes AI entrepreneurs, establishes best practices and advisory boards, and provides adequate public knowledge about AI systems. From a content-development

9. "Nuclear Power in Turkey," World Nuclear Association (website), updated July 2022, https://www.world-nuclear.org/information-library/country-profiles/countries-t-z/turkey.aspx.

10. "Nuclear Power in Turkey."

11. Mustafa Balat, "Security of Energy Supply in Turkey: Challenges and Solutions," *Energy Conversion and Management* 51, no. 10 (October 2010): 1998–2011, https://doi.org/10.1016/j.enconman.2010.02.033.

12. "Turkish Cyber Security Cluster," Presidency of the Republic of Türkiye Digital Transformation Office (website), 2021, https://cbddo.gov.tr/en/projects/#4801; and "Turkey's Cyber Shield: Octopus."

side, the TRAI creates webinars, seminars, and training sessions to integrate AI information across the economy through multiple verticals.[13]

Lastly, events such as HackInstanbul encourage cybersecurity cooperation through nongovernmental organizations and public and private institutions. These operations allow for broader participation in countering cyberattacks and create opportunities to identify young talent that can aid the government in future cyber operations. These events work with the AI initiatives as part of Türkiye's cybersecurity three-year plan announced in December 2020. After facing over 325,000 cyberattacks, the country aims to develop robust means to engage cyber threats.

Weaknesses in the Energy Sector

When looking at Türkiye's energy security from the perspective of the North Atlantic Alliance, the clear and present threat is the reliance on Russian energy sources. Due to its proximity and its abundance of resources, Russia is the most competitive and cost-effective energy source for the Turkish state. This reliance is coupled with the extensive pipeline system the Russian Federation has cultivated over the last 30 years. With the completion of TurkStream, Türkiye gained access to low-cost natural gas and the regional power of being an energy hub. Because of the strategic geographic position of the country, directing gas to Türkiye allows it to become the entry point for the Southern Gas Corridor. Relying so heavily on one country's natural gas, however, can create a pressure point that countries can exploit.

The direct threat to Turkish energy security needs to be considered. Indeed, with Russia maneuvering in Turkish waters during the current Ukraine conflict, one wrong move could bring profound consequences for Türkiye.

Türkiye further relies on Russian oil and gas imports, the stability of which are in question in the context of European attempts to ban Russian energy. Türkiye is a growing country, and modern economic growth requires a rapid increase in energy consumption. This need can force the government's hand as public and private demand necessitate the quick facilitation of energy. With pipelines already in place and foreign energy sources readily available—and encouraged by Turkish economic incentives—increased imports are likely.[14]

13. "Working Groups," Turkish Artificial Intelligence Initiative (website), 2021, https://turkiye.ai/en/working-groups/.

14. IEA, *Turkey 2021*.

Cybersecurity Vulnerabilities

Türkiye faces many threats but has established a solid foundation for the alliance. The government is actively increasing domestic AI initiatives but lacks the high-tech industrial base other NATO allies have. This problem creates deficiencies, as there is already a need for advanced cyber defense while Türkiye is still developing its critical technological capacity.

By 2017, Türkiye accounted for 77 percent of "all targeted malware and ransomware detections in Europe."[15] More recently, government sources state over 325,000 attacks have been detected and stopped within the last three years.[16] While the success rate has been good, a major vulnerability exists since Türkiye does not have comprehensive cybersecurity laws/policies. Directives and initiatives have been set up by ministries and security apparatuses, but formal policy does not yet exist.[17] Prior data have shown the soft underbelly of a nation's cyber network is the private and local entities.[18] National security systems are often well-funded and robust. By not having national policy enforced by a powerful state entity, however, local business, small government offices, and private corporations are not required to have rigorous protections.[19] As many of these entities are, in some capacity linked to the critical infrastructure, a small weakness can lead to a major intrusion.

Mitigation Methods

Energy

Renewable energy sources are at the forefront of Türkiye's plans, with strategic initiatives on track to be implemented within the decade. Construction of the Akkuyu Nuclear Power Plant—and future ones already

15. Salih Biçakci, F. Doruk Ergun, and Mitat Çelikpala, "The Cyber Security Scene in Turkey," in *A Primer on Cyber Security in Turkey and the Case of Nuclear Power*, ed. Sinan Ülgen (Istanbul: Centre for Economics and Foreign Policy Studies, 2015), 77, https://www.edam.org.tr/document/CyberNuclear/edam_cyber_security_report.pdf.

16. "Turkey Reveals Its Three-year Cybersecurity Plan," TRT World (website), December 30, 2020, https://www.trtworld.com/magazine/turkey-reveals-its-three-year-cybersecurity-plan-42820.

17. Efe Düveroğlu, "A Comparative Analysis of Critical Infrastructure Cyber Security Policies: Best Practices from the US, EU and Turkey" (master's thesis, Bilkent University, June 2020), http://repository.bilkent.edu.tr/bitstream/handle/11693/53653/10337584.pdf?sequence=1&isAllowed=y.

18. Faruk Aydin, "Cyber Security in National Protection of Turkey" (master's thesis, Çankaya University, September 2012), 18, http://earsiv.cankaya.edu.tr:8080/xmlui/bitstream/handle/20.500.12416/1151/Ayd%20n,%20Faruk.pdf?sequence=1.

19. Biçakci, Ergun, and Çelikpala, "Cyber Security Scene in Turkey," 22–51.

under consideration—coupled with the large deposits of nuclear fuel should make Türkiye hopeful for increased energy independence. Even with the increased funding for renewable energy sources, Türkiye will remain a fossil-fuel-oriented country for the near future.

When considering the politics of the Eastern Mediterranean, and Türkiye's place in the larger Arab/Muslim world, we must consider the fact that Türkiye seeks to increase its station as a regional energy hub.[20] Türkiye is seeking to expand pipelines through/from their territory and domestic production of natural gas via mining. Natural-gas deposits in the Eastern Mediterranean are a major point of contention for Türkiye, which seeks to gain a foothold in the Levantine.[21] More relevant to Türkiye's energy needs is the August 2020 natural-gas discovery in the Black Sea, the Sakarya gas field, by the Turkish petroleum agency.[22] Beyond finding deposits, the Turkish government has finalized agreements to build an undersea gas pipeline from Turkmenistan to Azerbaijan, through Türkiye, and into Greece and the rest of Europe.[23] This pipeline, along with TANAP, strengthens Türkiye's position as an energy hub for Europe, and reduces reliance on Russian natural gas.

Cybersecurity

As with renewable energy sources, Türkiye has made large investments in creating and building up its domestic cyber sector. Türkiye has already made major advancements in domestic early-warning technologies through the development of four cyber-shield/early-warning software systems: Octopus (which meets NATO standards), Avci, Azad, and Kasirga. Reports state these systems were critical in stopping the 325,000 cyberattacks.[24]

Türkiye's Cyber Star competition created opportunities for rising cybersecurity leaders. Successful entrants in the competition were hired by TRCERT, Türkiye's National CERT unit. This unit went on to participate in NATO's CMX-2017 Crisis Management Exercise in October 2017 and the National Cyber Defense Exercise in November 2017.[25] Altogether, the

20. Ali Tekin and Paul A. Williams, "Turkey and EU Energy Security: The Pipeline Connection," *East European Quarterly* 42, no. 4 (January 2009): 419–35.

21. Vedat Yorucu and Özay Mehmet, *The Southern Energy Corridor: Turkey's Role in European Energy Security*, vol. 60, Lecture Notes in Energy Series (Cham, CH: Springer International Publishing, 2018), 47–49.

22. IEA, *Turkey 2021*, 25.

23. Yorucu and Mehmet, *Southern Energy Corridor*, 48.

24. TRT World, "Turkey Reveals Three-year Cybersecurity Plan"; and "Turkey's Cyber Shield: Octopus."

25. ITU Publications, *Global Cybersecurity Index – 2018* (Geneva, CH: ITU Publications, 2019), https://www.itu.int/pub/D-STR-GCI.01-2018.

advancements made garnered Türkiye a "High Level of Commitment" rating in the Global Cybersecurity Index, the same level as the United States, the United Kingdom, France, and many other NATO allies.[26]

Recommendations

1. **Energy independence.** Türkiye should rapidly increase the production of renewable-energy sources and reduce dependence on Russia. The more integrated Russia and Türkiye become, the harder it will be for them to disengage in the future. Naturally, this reliance embeds foreign interests in Türkiye for years to come.

   Additionally, Türkiye should move away from cooperation with Russian financiers on secondary projects, specifically the nuclear power plant. Future nuclear power plants are already under discussion, and seeking NATO-backed financing would instill confidence with NATO allies and ensure reliable parties are participating in critical infrastructure. More importantly, this action would allow Türkiye to ensure its infrastructure meets Alliance security standards. Continued partnership with Russia erodes Türkiye's sovereignty by creating opportunities for Russia to exercise further control over the Black Sea region through cyberattacks on existing oil fields as well as controlling funding over new nuclear power plants.

2. **Develop domestic cybersecurity laws.** This development is most important in the private sector. As Türkiye is a growing regional and global economic force, its private sector will be increasingly integrated with European and American businesses. If the Turkish private sector has significant lapses in security or inadequate protocols for responding to cyberattacks, vulnerabilities will be created for their business partners, posing a grave threat to their European and American counterparts and the economic growth and security of Türkiye.

26. ITU Publications, *Global Cybersecurity Index – 2018*.

3. **Prioritize NATO objectives in the Middle East.** Türkiye is seeking to increase its power and independence within its geopolitical sphere of influence. Its advantageous position in the Southern Energy Corridor gives Türkiye many new opportunities. Türkiye should use its position to aid greater NATO objectives in the Middle East and Asia. Rapidly expanding its cybersecurity infrastructure and integrating it with NATO allies and industries would bolster Türkiye's position as a frontline nation in a volatile region. This integration, however, is not just the responsibility of Türkiye. Europe and the United States must make overtures to Turkish industry and Turkish geopolitical goals. Sharing technology and integrating Turkish security policy into the grander NATO objective would fortify against threats to the alliance.

Conclusion

Türkiye is maintaining a delicate balancing act between NATO investment and business in the region, Russian interests, and its rapidly expanding domestic infrastructure. Foreign investments have generated a great deal of domestic wealth. Without a strong domestic policy focus on security, these new developments will be difficult to maintain in the future as they may become points of exploitation. Due to NATO exposure through business interests and investment, foreign investments could create an opening to exercise political influence over Türkiye and NATO nations operating in Türkiye.

Figure 17-4. Map of Türkiye's threat timeline estimate (6 months indicates likely attack vector in 2022, 1 year by 2023, 2+ years by 2024 or later)
Credit: Ryan Fisk and Lucas Cox

Location	Reason for Threat Priority and Timeline
Kirkuk-Ceyhan Oil Pipeline	Expect a kinetic or ICS attack within two years as the pipeline has been previously kinetically attacked several times by the PKK. It could also serve as target for Russia if tensions escalate.
Akkuyu Nuclear Power Plant	Expect the Rosatom-funded nuclear plant to serve as target within two years if Türkiye changes its posture toward Russian energy.
Kemer Dam and Power Plant	Expect an ICS attack within six months if tensions escalate with Russia due to the plant's strategic importance to Turkish energy independence, which Moscow seeks to disrupt.
Strait of Bosporus	Expect disinformation or ICS attacks in the infrastructure surrounding the Bosporus due to its strategic location for Russia's war in Ukraine and military needs in the Mediterranean.

Select Bibliography

Balat, Mustafa. "Security of Energy Supply in Turkey: Challenges and Solutions." *Energy Conversion and Management* 51, no. 10 (October 2010). https://doi.org/10.1016/j.enconman.2010.02.033.

Biçakci, Salih, F. Doruk Ergun, and Mitat Çelikpala. "The Cyber Security Scene in Turkey," in *A Primer on Cyber Security in Turkey and the Case of Nuclear Power*. ed. Sinan Ülgen. Istanbul: Centre for Economics and Foreign Policy Studies, 2015. https://www.edam.org.tr/document/CyberNuclear/edam_cyber_security_report.pdf.

Koukoudakis, George. "EU Energy Security and Türkiye's Contribution to the Southern Energy Corridor." *Mediterranean Quarterly* 28, no. 2 (2017). https://doi.org/10.1215/10474552-4164292.

Presidency of the Republic of Türkiye: Digital Transformation Office. "Turkish Cyber Security Cluster." 2021. https://cbddo.gov.tr/en/projects/#4801.

Tekin, Ali, and Paul A. Williams. "Turkey and EU Energy Security: The Pipeline Connection." *East European Quarterly* 42, no. 4 (January 2009).

TRT World. "Turkey Reveals Its Three-year Cybersecurity Plan." TRT World. 2020. https://www.trtworld.com/magazine/Türkiye-reveals-its-three-year-cybersecurity-plan-42820.

Uddin, Riaz et al. "Energy Storage for Energy Security and Reliability through Renewable Energy Technologies: A New Paradigm for Energy Policies in Turkey and Pakistan." *Sustainability* (Switzerland) 13, no. 5 (February 2021). https://doi.org/10.3390/su13052823.

Yorucu, Vedat, and Özay Mehmet. *The Southern Energy Corridor: Turkey's Role in European Energy Security*. vol. 60. Lecture Notes in Energy Series. Cham, CH: Springer International Publishing, 2018.

Conclusion: Southeastern Europe

The nations of Southeastern Europe face a wide variety of threats to their critical energy infrastructure. Romania faces cyberattacks and potential hybrid warfare in the wake of the Ukraine crises in its EEZ, while Greece and Italy face vulnerabilities due to Chinese and Russian financing of critical infrastructure and potentially dangerous hardware. Türkiye is reliant on Russia for its energy needs, making it captive to Russia's geopolitical interests. The current energy landscape leaves Southeastern Europe rich for exploitation by state and non-state actors with the number of cyberattacks in the region rising as Russia, China, and Iran exert their influence. The current Ukraine conflict provides the opportunity for the region to wean itself off its dependencies. While Russia will not be able to continue to support some of the energy critical infrastructure development projects due to its economic isolation, China will try to continue to play a subtle role. Southeastern Europe will need to choose to partner consciously with NATO member states for its renewable, oil and gas, and energy infrastructure needs if the cycle of energy insecurity is to be broken.

Conclusion

"Just as there is a hybrid war, there will be hybrid peace."

—Ukrainian President Volodymyr Zelensky[1]

As of this writing, Russia's hybrid war against Ukraine and its allies in NATO continues. Any lessons Ukraine has taught NATO may be preliminary, but patterns have already started to emerge.

- **The emerging technology environment creates additional vulnerabilities to critical energy infrastructure during hybrid war.** As section one demonstrated, malicious cyber actors, whether nation-states or cybercriminals, are taking advantage of the vulnerabilities created by an Internet of Things environment, where SmartGrids, renewable energy sources, and the IT and OT environment can be compromised remotely. This landscape has been tested and attacked in the early months of the war in both Ukraine and NATO member states by Russian-backed hacker groups who have targeted satellites, wind turbines, and the technological processes of distribution of coal and thermal power plants.[2] In addition, Russian FSB officials have previously carried out cyberattacks against critical energy infrastructure in the United States, including oil and gas, energy, nuclear power plants, and utilities companies, giving Moscow the ability to cause disruption on a massive scale now.[3]

- **Russia is targeting energy security through cyber means in tandem with kinetic attacks.** As the Microsoft Digital Security Unit's report on Russia's cyberattacks on Ukraine mentioned in chapter 2 shows, the current hybrid war

1. "Purpose of Meeting with Putin Depends on When Such Talks to Take Place," Ukrinform (website), May 21, 2022, https://www.ukrinform.net/rubric-polytics/3488659-zelensky-purpose-of-meeting-with-putin-depends-on-when-such-talks-to-take-place.html.

2 Sean Lyngaas, "Russian Hackers Allegedly Target Ukraine's Biggest Private Energy Firm," *CNN* (website), July 1, 2022, https://www.cnn.com/2022/07/01/politics/russia-ukraine-dtek-hack/index.html.

3. Katie Benner and Kate Conger, "U.S. Accuses 4 Russians of Hacking Infrastructure, Including Nuclear Plant," *New York Times* (website), March 24, 2022, https://www.nytimes.com/2022/03/24/us/politics/russians-cyberattacks-infrastructure-nuclear-plant.html.

being waged was planned long in advance. It included cyber espionage on NATO countries (such as Turkey and Germany). Physical attacks on cities are timed with major cyberattacks on critical infrastructure, both in Ukraine and partner NATO member states.

While stating that Ukraine's cybersecurity teams are not afraid of Russian attacks on their power grids and nuclear sites, Viktor Zhora, Ukraine's cyber authority of the State Service of Special Communications, predicted: "This is happening for the first time in history and I believe that cyber-war can only be ended with the end of conventional war, and we will do everything we can to bring this moment closer."[4]

- **Russia has used information operations and malign influence and manipulation to create a global energy crisis in the lead-up to and throughout the Ukraine war.** These operations in turn affected food security, the supply chain, transportation, and logistics, with an impact on NATO's militaries. Whether holding gas and oil supply hostage or using disinformation to try to divide Allies or reframe their war of aggression, Russia has used the West's reliance on its energy for its geopolitical purposes. As demonstrated in the case studies, Russia's hybrid war is being fought with the support of China. China has helped materially to soften the impact of economic sanctions on Russia, assisted Russia with tracking Chinese-made drones being used on the battlefield in Ukraine, and exerted its control over the critical infrastructure and supply chain of NATO member states.

A Look Ahead

It is clear from lessons one and two that today's hybrid warfare will continue to target critical energy infrastructure. This study also found the cybersecurity in place on critical energy infrastructure is not sufficient to protect NATO member states from attacks. This finding was true whether examining traditional infrastructure (such as gas pumps and electric grids) or renewable infrastructure (such as wind turbines and microgrids).

4. Joe Tidy, "Ukraine Says It Is Fighting First 'Hybrid War,'" *BBC News* (website), March 4, 2022, https://www.bbc.com/news/technology-60622977.

It is, therefore, highly recommended that NATO member states prioritize investing in research and development on cyber early warning systems (CEWS) that include virtual modeling of critical energy infrastructure for early mitigation of malicious intrusions. As demonstrated in section two, these new generation CEWS are meeting with success in labs from the United States to Romania and Germany. There, AI and machine-learning technologies have been combined with sensing and controls to locate and neutralize cyberattacks. By using the virtual model of a natural-gas pipeline and combining it with machine learning, cyberattacks can be identified early and mitigated. Threat intelligence modeling and identification systems, based on heterogeneous information networks that use cyber entanglement capabilities, are also helpful in this effort. The modeling helps visualize the strategic, operational, and tactical effects in cyberspace. While these methods are just in nascent phases of development, with increased R & D funding and the implementation of successful prototypes, grids, gas pipelines, and other energy sources can be protected more adequately from cyberattacks. Any CEWS development must be in addition to anomaly detection monitoring in critical energy infrastructure.

Second, NATO and the US military have stated their intentions to ensure installations are energy independent, and mobile combat units are not fuel dependent. Strides are being made to improve mobile microgrids. Field testing and research still need to be done, however, to ensure microgrids can use renewable and fuel sources reliably. In addition, cybersecurity must be built in on the front end of the microgrid design, and islanding should be practiced regularly to ensure military installations can support critical systems if host nation grids fail.

Finally, NATO member states should free themselves from future malign influence and coercion campaigns—whether from Russia, China, or other NATO adversaries—by decreasing their energy and supply-chain dependencies. Tracking and countering information operations through NATO's Joint Intelligence and Security Division is a start, but fostering sustainable, non-hackable energy sources within and across the NATO Alliance will be equally crucial.

Areas for Further Research

Sourcing cyber secure energy independence for militaries in an era of hybrid warfare remain an area requiring more research. While NATO has politically rallied around supporting the expansion of renewable-powered microgrids and is interested in improving its cyber early warning capacities, technologies that may be developed more quickly may be too controversial at NATO Headquarters to be approved for use any time soon. One example is the small modular reactor (SMR). Small modular reactors are advanced nuclear reactors that have a power capacity of up to 300 megawatts of electricity per unit, which is about one-third of the generating capacity of traditional nuclear power reactors. While SMRs will be ready for deployment on US bases by 2026, likely much earlier than renewables-powered microgrids, their use on military installations in Europe remains an area that requires additional testing and political will.[5] A study by the NATO Energy Security Centre of Excellence assessed them not battlefield-ready due to high construction costs and waste and excessive regulatory restrictions.[6] Given their smaller footprint, however, SMRs can be used on locations not suitable for larger nuclear power plants. They offer savings in construction time and can be deployed by NATO states incrementally to match increasing energy demand.[7]

In areas lacking sufficient lines of transmission and grid capacity, militaries can install SMRs into an existing grid or remotely off-grid, as a function of their smaller electrical output, providing necessary energy for military, industry, and the population. They also have reduced fuel requirements. Power plants based on SMRs may require refueling only every three to seven years in comparison to between one and two years for conventional nuclear plants. Some SMRs are designed to operate up to 30 years without refueling. These advantages make them especially useful for the military to ensure independence of energy supply to their bases or forward operating areas.

One example of the future cooperative use of SMRs between NATO nations is the intergovernmental agreement between Romania and the United States signed in December 2020 for the United States to help Romania develop, license, and construct its own SMR. Similar agreements could also assist with deployment in other Three Seas Initiative countries, and the SMRs could also be deployed in the Baltics, Poland, Bulgaria, Turkey, and Greece.[8] Until there is greater political momentum in Brussels, research and

5. Timothy Renahan, "Realizing Energy Independence on U.S. Military Bases," *Joint Forces Quarterly* 103, no. 4 (2021).

6. Lukas Trakimavicius, "Is Small Really Beautiful? The Future Role of Small Modular Nuclear Reactors (SMRs) in the Military," NATO Energy Security Centre of Excellence (website), November 2, 2020, https://www.enseccoe.org/data/public/uploads/2020/11/02.-solo-article-lukas-smr-eh-15-web-version-final.pdf.

7. Renahan, "Realizing Energy Independence."

8. "Teaming Agreement Signed for Romanian SMR Deployment: New Nuclear," World Nuclear News (website), November 5, 2021, https://www.world-nuclear-news.org/Articles/Teaming-agreement-signed-for-Romanian-SMR-deployme.

construction of this energy independent option for military installations will likely need to be done on a bilateral or regional level.

Today's energy is only as secure as the cybersecurity protecting its critical infrastructure and the will of its state users not to be reliant on adversary nations for its supply. Ukraine has taught NATO that hybrid wars are worth fighting to defend freedom. Critical energy infrastructure, cyber resilience, a fierce sense of independence, and support from democratic alliances can aid that process. For the sake of Ukraine and its NATO partners, let us hope hybrid war turns to hybrid peace soon.

Select Bibliography

Benner, Katie, and Kate Conger. "U.S. Accuses 4 Russians of Hacking Infrastructure, Including Nuclear Plant." *New York Times* (website). March 24, 2022. https://www.nytimes.com/2022/03/24/us/politics/russians-cyberattacks-infrastructure-nuclear-plant.html.

Lyngaas, Sean. "Russian Hackers Allegedly Target Ukraine's Biggest Private Energy Firm." *CNN* (website). July 1, 2022. https://www.cnn.com/2022/07/01/politics/russia-ukraine-dtek-hack/index.html.

"Purpose of Meeting with Putin Depends on When Such Talks to Take Place." Ukrinform (website). May 21, 2022. https://www.ukrinform.net/rubric-polytics/3488659-zelensky-purpose-of-meeting-with-putin-depends-on-when-such-talks-to-take-place.html.

Renahan, Timothy. "Realizing Energy Independence on U.S. Military Bases." *Joint Forces Quarterly* 103, no. 4 (2021).

"Teaming Agreement Signed for Romanian SMR Deployment: New Nuclear." World Nuclear News (website). November 5, 2021. https://www.world-nuclear-news.org/Articles/Teaming-agreement-signed-for-Romanian-SMR-deployme.

Tidy, Joe. "Ukraine Says It Is Fighting First 'Hybrid War.'" *BBC News* (website). March 4, 2022. https://www.bbc.com/news/technology-60622977.

Trakimavicius, Lukas. "Is Small Really Beautiful? The Future Role of Small Modular Nuclear Reactors (SMRs) in the Military." NATO Energy Security Centre of Excellence (website). November 2, 2020. https://www.enseccoe.org/data/public/uploads/2020/11/02.-solo-article-lukas-smr-eh-15-web-version-final.pdf.

Glossary

Terms as defined by the Department of Defense and NATO

AI: Artificial Intelligence.

BAD: Behavior Anomaly Detection.

Baltic Cyber Shield: An annual cyber defense exercise.

BRELL Network: A network that connects Belarus, Russia, Latvia, and Lithuania via AC power lines.

CERT: Computer Emergency Response Team.

CEWS: Cyber Early Warning System.

CHEC: China Huadian Engineering Company.

CIA Triad: Confidentiality, Integrity, and Availability of Data.

CIIP: Critical Information Infrastructure Protection.

CNAIPIC: The National Anti-crime Centre for the Protection of Critical Infrastructure.

Critical Energy Infrastructure (CEI): Encompasses the processes of energy generation, transmission, distribution, and consumption.

Critical Infrastructure: Systems and assets, whether physical or virtual, vital to the United States.

Cybercriminals: Criminals who use the computer in the commission of a crime.

DDoS: A Distributed Denial-of-service attacks target websites and servers by disrupting network connectivity and service.

Digital Certificates: A crucial part of public key infrastructure that binds an identity (often a user or device) to the encryption keys associated with them for identification purposes.

Disinformation: Verifiably false or misleading information created, presented, and disseminated for economic gain or to deceive the public intentionally.

DoS: Denial of service is a malicious attack aiming to render a computer or network resources unavailable.

DSO: Distribution System Operator.

Dutch Polder Model: A consensus-based method of economic and social policy making that draws together 100+ stakeholders.

EEZ: Exclusive Economic Zone.

EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances.

Energy Security: Uninterrupted availability of energy sources at an affordable price.

EWS: Early Warning System.

FDI: Foreign Direct Investment.

Fit-for-RES: Fit-for-Renewable Energy Source market economy.

Gazprom: Russian state-owned energy group.

Golden Power Law: An Italian law that provided the Italian government the power to access companies holding strategic partnerships in sectors in security, defense, energy, transport, communications, or 5G networks; other areas were introduced by EU Regulation No. 452/2019.

Honeypot: A computer security mechanism set to detect, deflect, or counteract attempts by unauthorized user.

Hybrid Threats: Threats that combine military and nonmilitary as well as covert and overt means.

Hybrid Warfare: A theory of military strategy that combines conventional and irregular methods.

ICA: Internal Certificate Authority. A serval internal to a network responsible for managing, generating, and issuing digital certificates.

IDS: Intrusion Detection System is a device that monitors a network for malicious activity. When suspicious activity is detected, it is logged and sent to an administrator or stored.

IEA: International Energy Agency.

Insider Threat: The potential of an insider to use his/her access knowledge of an organization's resources to cause damage or disruption.

Internet of Things (IoT): A network computing device that interacts with its environment, sensors, software, and other technologies.

Intrusion Detection System (IDS): A device used to monitor or surveille a network system.

IRES: Intermittent Renewable Energy Resources.

Locked Shields: An international crisis exercise that tests the skills of cybersecurity professionals to defend critical infrastructure and IT against real-time attacks.

Memcached: A temporary information cache system that, if left public online, could be used to conduct a denial-of-service (DoS) attack.

Microgrids: An alternative source of energy. It is a self-contained power system network confined to a small geographic area.

Norms: Aspects of international relations that arise from a community based on certain beliefs and values.

OES: Operations Essential Service.

OVI: Operations Vital of Importance.

Phishing: Using a fraudulent e-mail in order to steal information or gain unauthorized access to a network. Designed to trick a user into executing malicious code or responding with information.

Ransomware: A type of malware which holds a device hostage by locking down key system components, usually at the root level, until the user meets the demands of the attacker.

Renewable: A natural resource or source of energy that is not depleted by use, such as water, wind, or solar power.

RES: Renewable Energy Source.

RIA: Estonia's Information Systems Authority.

ROMEO: Replacement and Original Magnet Engineering Options, consisting of 15 research centers and manufacturers aiming to develop rare-earth-free magnets.

RTOS: Real-time Operating System.

SCADA: Supervisory Control and Data Acquisition is a system of software and hardware elements used for controlling, monitoring, and analyzing industrial devices and processes.

SMR: Small modular reactor.

SOEs: China's State-owned Enterprises.

Spear phishing: Using a targeted, fraudulent e-mail under the guise of legitimate personal circumstances in order to steal information or gain unauthorized access to a network.

TOR Network: A network that allows users to access web browsers anonymously and conduct their illegal and nefarious activities.

TRAI: Turkish Artificial Intelligence Initiative.

TSO: Transmission System Operator.

Wateringhole: A cyberattack where the attacker infects a website often visited by the victim.

WOMBAT: Worldwide Observatory of Malicious Behaviors and Attack Threats.

YKEA: Türkiye's Renewable Energy Resource Areas.

About the Contributors

Editor and Lead Author

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 colead 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, a master of international service degree from American University, and a doctorate in political science from the Universität der Bundeswehr.

Main Contributing Authors

Chuck Benson is the director of IoT risk mitigation strategy at the University of Washington. He is the author of *Managing IoT Systems for Institutions & Cities* and is a contributing author to *Creating, Analysing, and Sustaining Smart Cities – A Systems Perspective*. He is currently writing another book on the implications of IoT and national security and is an investigator on a National Science Foundation research grant on interorganizational aspects of IoT implementations. He has testified before the US-China Economic and Security Review Commission on IoT risk mitigation. Benson has an electrical engineering degree from Vanderbilt University and a master of science degree in computer science from Eastern Washington University. He is a former Marine Corps captain and helicopter pilot.

Vytautas Butrimas has worked in various defense and cybersecurity roles. His recent work has focused on industrial cybersecurity and includes a Cybersecurity Risk Study of the NATO Central Europe Pipeline System, *Guide for Protecting ICS against Cyber Incidents in the NATO Pipeline System and Hybrid Warfare against Critical Energy Infrastructure: Case of Ukraine*. Butrimas has contributed to various studies and reports on cybersecurity and critical infrastructure (for OSCE, EU ENISA, IEA, NATO, and other organizations), published articles, and made presentations at many conferences and courses on cybersecurity and defense policy. He has participated in NATO and national exercises, which included cyberattack scenarios on critical infrastructure. Butrimas is currently serving as a subject-matter expert for the NATO Energy Security Centre of Excellence in Vilnius, Lithuania.

Georgios Giannoulis is a senior analyst in the field of maritime hybrid threats and critical infrastructure of COI vulnerabilities and resilience of European hybrid CoE. Giannoulis is commander engineer of the Hellenic Navy with more than 10 years of experience onboard naval vessels, participating in many allied operations/exercises in the Aegean and Mediterranean Seas. After accomplishing his onboard duties, he served in different positions, including as the department head of the Hellenic Navy General Staff, a surveyor of the Hellenic Navy General Staff General Inspection, and the head of the Technical Department for Operating and Maintenance of Naval Base Salamis critical infrastructure. He graduated from the Hellenic Naval War College and Supreme Joint War College. He also holds master of science degrees in electrical engineering and applied mathematics.

Gabriel Raicu is the director of the Centre of Excellence in Maritime Cyber Security, lead developer for the first cybersecurity simulator under the umbrella of the Black Sea Maritime Cyber Security Training Center at Constanta Maritime University. He is the lead coordinator on cyber and critical infrastructure for a research section of a NATO science and technology organization program. He is also vice rector for innovation and research at Constanta Maritime University.

Case Study Authors

Michael Bervell is a Ghanaian-American angel investor, entrepreneur, and author. He is the author of *Unlocking Unicorns*, a bestselling book about the stories, habits, and lessons of billion-dollar startup founders in Africa, Asia, and the Middle East. For over two years, he blogged daily on his website "Billion Dollar Startup Ideas" and received more than 800,000 impressions from over 150 different countries. Prior to writing, Bervell cofounded "Hugs for" an international, student-run nonprofit organization focused on using grassroots strategies to develop countries around the world. Because of his work, Bervell was awarded the National Caring Award in 2015 alongside Pope Francis and Dikembe Mutombo. He holds a bachelor's degree in philosophy from Harvard University, a master's degree in communications from the University of Washington, and a master of business administration degree from Harvard Business School.

Milagro Castilleja is a master of communication in digital media graduate of the University of Washington's Communication Leadership Program. Castilleja also earned a bachelor of arts degree in film production from Central Washington University. Castilleja's recent studies focused on communication through emergent platforms and utilizing technology to uplift underrepresented voices in digital media. Castilleja has been volunteering with Making Contact Radio as a Project Coordinator working to better understand Making Contact's audiences and create a strategy to further connect with listeners and identify those voices in the Making Contact community.

Colonel Chris Clyde is a former Asia-Pacific US Army War College fellow at the University of Washington. His 23-year Army career includes numerous deployments to Iraq, Kuwait, and Afghanistan. Clyde has also participated in exercises in Thailand, Qatar, Bahrain, and the United Arab Emirates. He is an Aviation officer and most recently served in the US Army Security Assistance Command as an aviation program manager to modernize the Saudi Arabian Ministry of National Guard's aviation fleet. Clyde has served in multiple leadership and staff positions in conventional, special operations, and combined and joint military organizations. He holds a master's degree in international relations from Webster University and a bachelor's degree in resource and environmental studies from Texas State University.

Christopher J. Eaton graduated with a master of arts in international studies from the University of Washington in 2022. His research focused on the role nuclear energy and weapons play in geopolitics, as well as the domestic sociological effects of nuclear production. Eaton conducted original research on the nuclear production towns that arose as part of the Manhattan Project, while examining his family's role in nuclear weapons production.

Alex Elmore is a colonel with the Alaska Army National Guard and has served as the commander of the 297th Regional Support Group at Joint Base Elmendorf-Richardson in Richardson, Alaska, since August 2021.

Ryan Fisk, at the time of this writing, was an undergraduate at the University of Washington in Seattle, Washington. He provided support to SAS-163 as a direct member of the SAS-163 team and through an internship with the US Army War College. He has since graduated and accepted a position at the Public Health Company, an epidemiological risk assessment company, doing geopolitical analysis. Long-term, he intends to continue his education and begin a career in international affairs with the US federal government.

Erin Hodges, at the time of this writing, is an intern at the US Army War College and the National Defense University. She holds a master of arts degree in international relations and affairs from Syracuse University with a certificate of advanced studies in security studies.

Lieutenant Colonel Frank J. Kuzminski is a US Army officer and strategist. A native of Poland, Kuzminski emigrated to the United States in 1990. He graduated from the United States Military Academy at West Point 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, he was assigned to the Army Staff at the Pentagon and later 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.

Vishwa Padigepati is an undergraduate junior at Yale University, class of 2023, where she is pursuing the studies of cognitive science and political science. She is the coeditor in chief of the *Yale Review of International Studies* and the *Yale Human Rights Journal*. She is a cabinet member of Plan International USA. Padigepati previously worked in global technology strategy at Ingram Micro and for the US International Trade Administration, the Department of Commerce, and the US Congress in various intern capacities.

Caitlin Quirk is an international studies student at the University of Washington. She is interested in cybersecurity policy and the ethical use of technology.

Brenton M. Riddle is a dual-degree, triple-major graduate of the University of Washington, from which he received degrees in international diplomacy and security, comparative history of ideas, and environmental science and resource management. Riddle currently lives in the Pacific Northwest where he advocates for innovative, sustainable, and equitable energy and environment policy decision making at all levels of government. Prior to his work with the US Army War College, Riddle led the research on critical energy infrastructure cybersecurity as part of the Henry M. Jackson School of International Studies Rome Task Force, "European Defense: Strategic Choices for 2030." His interests include the sustainability considerations of infrastructure development projects, combating climate change with renewable energy, and improving community resilience.

Shuo Zhang holds a bachelor of arts degree from the University of Washington with a major in international studies and a minor in music. During her time at the Henry M. Jackson School of International Studies, she conducted research for country-specific case studies on France, China, and Singapore, with issues relating to cybersecurity, energy security, trade and AI policies. She is currently pursuing a master of public administration degree from Cornell University.

Interns

Lucas Cox, at the time of this writing, is an intern with the Strategic Studies Institute and a graduate of the University of Washington's Henry M. Jackson School of International Studies with a bachelor of arts degree in international security, political science, and Russian studies. He is also the 2023 University of Washington Trina Deines Rome Center Intern and an intern at NATO's science and technology organization.

Samira Oakes, a West Orange County narcotics task force agent, served as a US Army War College research intern on this book project for three months.

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

U.S. ARMY

ISBN 1-58487-843-6
9 781584 878438
90000

https://press.armywarcollege.edu

THE UNITED STATES ARMY WAR COLLEGE
STRENGTH and WISDOM