NORTH ATLANTIC TREATY
ORGANIZATION

SCIENCE AND TECHNOLOGY
ORGANIZATION

AC/323(SAS-163)TP/1164

www.sto.nato.int

STO TECHNICAL REPORT **TR-SAS-163**

Energy Security in the Era of Hybrid Warfare

(La sécurité énergétique à l’ère de la guerre hybride)

Final technical report.

Published May 2024

Distribution and Availability on Back Cover

NORTH ATLANTIC TREATY
ORGANIZATION

SCIENCE AND TECHNOLOGY
ORGANIZATION

AC/323(SAS-163)TP/1164

www.sto.nato.int

STO TECHNICAL REPORT **TR-SAS-163**

Energy Security in the Era of Hybrid Warfare

(La sécurité énergétique à l'ère de la guerre hybride)

Final technical report.

The NATO Science and Technology Organization

Science & Technology (S&T) in the NATO context is defined as the selective and rigorous generation and application of state-of-the-art, validated knowledge for defence and security purposes. S&T activities embrace scientific research, technology development, transition, application and field-testing, experimentation and a range of related scientific activities that include systems engineering, operational research and analysis, synthesis, integration and validation of knowledge derived through the scientific method.

In NATO, S&T is addressed using different business models, namely a collaborative business model where NATO provides a forum where NATO Nations and partner Nations elect to use their national resources to define, conduct and promote cooperative research and information exchange, and secondly an in-house delivery business model where S&T activities are conducted in a NATO dedicated executive body, having its own personnel, capabilities and infrastructure.

The mission of the NATO Science & Technology Organization (STO) is to help position the Nations' and NATO's S&T investments as a strategic enabler of the knowledge and technology advantage for the defence and security posture of NATO Nations and partner Nations, by conducting and promoting S&T activities that augment and leverage the capabilities and programmes of the Alliance, of the NATO Nations and the partner Nations, in support of NATO's objectives, and contributing to NATO's ability to enable and influence security and defence related capability development and threat mitigation in NATO Nations and partner Nations, in accordance with NATO policies.

The total spectrum of this collaborative effort is addressed by six Technical Panels who manage a wide range of scientific research activities, a Group specialising in modelling and simulation, plus a Committee dedicated to supporting the information management needs of the organization.

•	AVT	Applied Vehicle Technology Panel
•	HFM	Human Factors and Medicine Panel
•	IST	Information Systems Technology Panel
•	NMSG	NATO Modelling and Simulation Group
•	SAS	System Analysis and Studies Panel
•	SCI	Systems Concepts and Integration Panel
•	SET	Sensors and Electronics Technology Panel

These Panels and Group are the power-house of the collaborative model and are made up of national representatives as well as recognised world-class scientists, engineers and information specialists. In addition to providing critical technical oversight, they also provide a communication link to military users and other NATO bodies.

The scientific and technological work is carried out by Technical Teams, created under one or more of these eight bodies, for specific research activities which have a defined duration. These research activities can take a variety of forms, including Task Groups, Workshops, Symposia, Specialists' Meetings, Lecture Series and Technical Courses.

The content of this publication has been reproduced directly from material supplied by STO or the authors.

Published May 2024

ISBN 978-92-837-2476-6

Table of Contents

List of Figures

List of Tables

Foreword

This final report is the culmination of a three-year analysis dedicated to the impact of hybrid warfare on NATO's energy security. This topic proved to be of considerable interest among the member states, and we're pleased to note, generated much discussion and participation. During this period, we benefited from the availability of numerous subject matter experts from the NATO member states, as well as the Partnership for Peace. This panel of experts was instrumental in tackling the immense challenge of gathering and analyzing the body of data surrounding the NATO members' energy infrastructure within the hybrid warfare context. Ultimately, the expertise from our core team of contributors was critical to the project's success.

If the last three years have taught us anything, the threat is persistent and constantly evolving as determined adversaries continue to challenge NATO and its partners via hybrid warfare tactics. In February 2022, we saw first-hand the impact of 21st Century warfare on a NATO partner. Indeed, the Russia-Ukraine War has reinforced many of the notions highlighted in the report; the energy infrastructure is vulnerable and a preferred target of our adversaries. Moreover, hybrid warfare tactics, aligned with kinetic actions, are difficult to detect and defeat, requiring a coordinated, whole-of-Alliance approach.

Russia's invasion of Ukraine in 2022 confronted the United States and its NATO partners with the impact of hybrid warfare far beyond the battlefield. This study examines how hybrid warfare is being used by NATO's adversaries, what vulnerabilities to energy security exist across the Alliance, and what energy critical infrastructure mitigation strategies are available: including a new generation of cyber early warning, microgridding for military installations and a NATO disinformation rapid response force. These mission-actionable mitigations, if implemented, can help NATO face the future with more hardened energy independence and unity.

We would like to acknowledge the SAS-163 team leads and contributing authors. We are also grateful for the enthusiastic support from the SAS-163 members, as well as the following guests and experts:

Ms. Molly ADLER (USA)
Ms. Ratela ASLLANI (ALB)
Ms. Margarita ASSENOVA (USA)
Dr. Andi ATTENBERGER (GER)
Mr. Chuck BENSON (USA)
Mr. Richard BREWIN (GBR)
Dr. Ron BURMAN (CAN)
Ms. Stephanie Hope CLUTE (USA)
Capt. William COMBES (ret.) (USA)
Mr. Alexander DAVIES (GBR)
Ms. Klara DOLOS (GER)
Dr. Dan DUMITRU (ROM)
Mr. Jordan ECCLES (USA)
Ms. Rachel EHRENFELD (USA)

Prof. Adrian GHEORGHE (USA)
Mr. Alkman GRANITSAS (USA)
Mr. Joel HARDING (USA)
Ms. Afra HERR (GER)
Dr. Saltuk KARAHAN (USA)
Dr. Mehmet KINACI (TUR)
Prof. Krzysztof KSIĘŻOPOLSKI (POL)
Mr. Gerard LAANEN (NLD)
Ms. Kristina LIBBY (USA)
Mr. Dan LITTLE (USA)
Ms. Alberta M. NIKOLAI (USA)
Prof. Marc OZAWA (USA)
Ms. Vishwa PADIGEPATI (USA)
Dr. Joel PETERS (USA)

COL Romas PETKEVICIUS (LIT)

Mr. Richard PRICE (USA)

Prof. Kamila PRONINSKA (POL)

Mr. Derek J. REID (USA)

Ms. Mathilde ROUVILLOIS (FRA)

Ms. Christine SCALES (CAN)

Mr. Paul SCHINDLER (GER)

Mr. Gareth SMITH (GBR)

Mr. Arnis SNORE (LIT)

Mr. John TABLER (USA)

Ms. Darlene THORNTON (USA)

Dr. Alexander TIMMONS (USA)

Mr. Mike WALSH (USA)

Mr. Paul Michael WHIBEY (USA)

Mr. Jon WOODMAN (GBR)

Prof. Marian ZULEAN (ROM)

The SAS-163 leadership team would like to acknowledge the support provided by the Science and Technology Board and give special thanks to the Collaboration Support Office in Neuilly-sur-Seine, France for their tremendous assistance over the course of this study.

Finally, we would like to thank Prof. Stefan Pickl (GER); without his advice and guidance, this project would never have been initiated.

November 2022

Arnold C. DUPUY, PhD (Chair)
Naval Postgraduate School
USA
Email: arnold.dupuy@nps.edu

Daniel NUSSBAUM, PhD (Mentor)
Naval Postgraduate School
USA
Email: danussba@nps.edu

Sarah LOHMANN, PhD (Cyber Team Lead)
Army War College
USA
Email: sarah.lohmann.civ@armywarcollege.edu

SAS-163 Membership List

CHAIR

Dr. Arnold DUPUY
Naval Postgraduate School
UNITED STATES
Email: arnold.dupuy@nps.edu

MEMBERS

Dr. Gisele AMOW
National Research Council Canada
CANADA
Email: Gisele.Amow@forces.gc.ca

Ms. Kyna BOWERS
Department for Business, Energy and Industrial Strategy
UNITED KINGDOM
Email: Kyna.Bowers@beis.gov.uk

Dr. Peter BURGHERR*
Paul Scherrer Institut (PSI)
SWITZERLAND
Email: peter.burgherr@psi.ch

Mr. Vytautas BUTRIMAS*
Energy Security COE (ENSEC)
NATO ENSEC COE
Email: Vytautas.Butrimas@enseccoe.org

Dr. Matthew COTTEE
Department for Business, Energy and Industrial Strategy
UNITED KINGDOM
Email: matthew.cottee@beis.gov.uk

Ms. Isabella CRONIN
University of Amsterdam
NETHERLANDS
Email: isabellacronin23@gmail.com

Mr. Ignacio FONSECA
JALLC – Joint Analysis and Lessons Learned Centre
JALLC
Email: Ignacio.Fonseca@jallc.nato.int

CDR. Georgios GIANNOULIS*
Hybrid COE
NATO HYBRID COE
Email: georgios.giannoulis@hybridcoe.fi

Ambassador Shota GVINERIA
Baldefcol
GEORGIA
Email: Shota.Gvineria@baltdefcol.org

Mr. David HAMON
SAIC Inc.
UNITED STATES
Email: dhamon@umw.edu

Mr. Freddy JÖNSSON HANBERG
Swedish Total Defence Foundation
SWEDEN
Email: freddy@totalforsvar.org

Mr. Rodney HOWES
DRDC
CANADA
Email: rodney.howes@forces.gc.ca

Col Kari JUUTILAINEN
Energy Security COE (ENSEC)\
NATO ENSEC COE
Email: Kari.Juutilainen@enseccoe.org

Dr. Krzysztof KSIEZOPOLSKI
Warsaw School of Economics (SGH)
POLAND
Email: kksiez@sgh.waw.pl

*** Team Leader, Contributing Author**

Mr. Jose PAREJO
CEPSA
SPAIN
Email: jose.parejo@cepsa.com

Prof. Dr. Stefan PICKL
Universität der Bundeswehr München
GERMANY
Email: stefan.pickl@unibw.de

Assoc. Prof. Dr. Gabriel RAICU*
Constanta Maritime University
ROMANIA
Email: gabriel.raicu@cmu-edu.eu

GEN Jukka SAVOLAINEN
Hybrid Threat COE
FINLAND
Email: jukka.savolainen@hybridcoe.fi

Ms. Christine SCALE
DRDC CORA
CANADA
Email: Christine.Scales@forces.gc.ca

Mr. Paul SCHINDLER
University of Amsterdam
NETHERLANDS
Email: schindlerpaul00@gmail.com

Mr. Moritz SCHWAB
University of the Federal Armed Forces
GERMANY
Email: moritz.schwab@unibw.de

Mr. Gareth SMITH
Department of Business
UNITED KINGDOM
Email: Gareth.smith@beis.gov.uk

Mr. Jon WOODMAN
SAJO Ventures
UNITED KINGDOM
jon@sajoventures.com

ADDITIONAL CONTRIBUTORS

Dr. Leigh ARMISTEAD*
Peregrine Technical Solutions
USA
Email: larmistead@gbpts.com

Dr. John DENI*
US Army War College
USA
Email: john.deni@armywarcollege.edu

Prof. David DORONDO*
Western Carolina University
USA
Email: dorondo@email.wcu.edu

Dr. Michael D. EVANS*
Concept Materials Inc.
USA

Dr. Sarah LOHMANN*
US Army War College
USA
Email: slohmann@uw.edu

*** Team Leader, Contributing Author**

PANEL/GROUP MENTOR

Dr. Dan NUSSBAUM
Naval Postgraduate School (NPS)
United States
Email: dnussbaum@nps.edu

Energy Security in the Era of Hybrid Warfare

(STO-TR-SAS-163)

Executive Summary

NATO's military logistics and supply chain systems are now challenged by the tyranny of distance, near peer adversaries, and tight energy in a manner unseen since World War II. Furthermore, the Operational Energy (OE) requirements of the Alliance's war fighters continue to increase sharply due to the greater energy intensity of sophisticated platforms necessary to enhance force mobility, lethality and operational tempo. Compounding this demand for energy is a lack of investment and poorly conceived and executed plans at decarbonization, which have created national security vulnerabilities. These challenges are exacerbated by new strategies, operational constructs, force designs, and new and emerging weapons / platforms that increase the complexity and dynamics of OE management. Closely related, planners do not appreciate the tactical and operational impact of energy, which could limit capabilities, notably in projecting kinetic effects beyond a single mission, particularly in a contested environment. Ultimately, the inability of the Alliance to better integrate OE management could imperil its forces and mission success.

The ability to leverage technology for geo-political gain against an adversary's vulnerabilities, broadly referred to as hybrid warfare, has become increasingly prevalent in the 21st Century. Hybrid warfare has multiple synonyms, such as "grey zone warfare / strategies," "competition short of conflict," "active measures," and "new generation warfare." Despite differences in terminology, these definitions point to the same fundamentals; in its most basic context, hybrid warfare's genesis can be traced to the age-old principle of asymmetrically exploiting an adversary's weaknesses, with clear 21st Century attributes. This is done by using or 'misusing' capabilities meant to serve the public at-large – either through the commodities it consumes or the public goods and services by which everyone carries out their daily affairs.

The project's focus on energy security is rooted in the pretext that it is fundamentally the most vulnerable sector and possesses the largest potential to destabilize a society. Yet, what does this mean in a practical sense? How can NATO and the member states develop actionable policies and countermeasures? Moreover, from an energy security perspective, this study's primary focus, how can we protect the infrastructure and recover from attacks against this most vital of sectors? Although sovereign nations maintain responsibility for the integrity and defence of their energy infrastructure, NATO operations will require a unified response and a resilient international energy supply coordinated with alliance, European Union, and national objectives.

It is acknowledged that NATO has a role at the forefront of the confluence of energy security, cyber security and hybrid warfare. Within the context of NATO energy security, hybrid threats can be identified as actions by state or non-state actors aimed to undermine or harm NATO's assured access to affordable and acceptable supplies of energy and the ability to protect and deliver sufficient energy to meet mission essential requirements by influencing its decision-making at the local, regional, state, or institutional level.

Additionally, we need to keep in mind the two main components of the hybrid warfare and energy security dynamic are cyber defence and malign influence. NATO has maintained a constant though evolving role in addressing cyber as a hybrid threat to the Critical Energy Infrastructure (CEI) of its member states. Over the past two decades, cyber-attacks against Industrial Control Systems (ICS) of NATO member states' energy supply chains have grown exponentially.

The primary objectives of SAS-163 have been to:

1) Raise awareness of the energy-hybrid warfare nexus;
2) Identify its broader impact in the civilian and military realms within NATO; and
3) Define courses of action.

This includes mitigating the impact on civilian and military infrastructure and interests and develop countermeasures. Ultimately, the project's goal has been to provide analytic support to NATO's civilian and military leadership.

The key findings from the study can be categorized as follows:

- Near-term energy insecurity among the NATO Member States.
- Persistent cyber threats to the energy sector.
- Energy sector supply chain vulnerabilities.
- Impact on NATO's operational energy and military capabilities.
- Malign influence in the energy sector can have significant consequences.

The study recommends continued analysis in the topic of hybrid warfare and energy security, particularly with a focus on NATO eastern tier, arguably the most vulnerable sector, and a deeper investigation of cyber advance warning technologies. For this reason, we have submitted a proposal for a three-year study extension.

La sécurité énergétique à l'ère de la guerre hybride

(STO-TR-SAS-163)

Synthèse

Les systèmes logistiques et chaînes d'approvisionnement militaires de l'OTAN sont désormais confrontés à la tyrannie de la distance, à des adversaires aux capacités presque comparables et à une raréfaction de l'énergie, et ce, d'une manière inédite depuis la seconde guerre mondiale. De plus, les besoins en matière d'énergie opérationnelle (OE) des combattants de l'Alliance continuent d'augmenter fortement à cause de l'intensité énergétique accrue des plates-formes sophistiquées qui améliorent la mobilité des forces, la létalité et le rythme opérationnel. Cette demande d'énergie s'accompagne d'un manque d'investissement et de plans de décarbonation mal conçus et mal exécutés, ce qui a créé des vulnérabilités sur le plan de la sécurité nationale des pays. Ces problèmes sont exacerbés par de nouvelles stratégies, de nouveaux concepts opérationnels et de nouvelles conceptions des forces, ainsi que par des armes/plates-formes nouvelles ou émergentes qui accentuent la complexité et la dynamique de gestion de l'OE. Autre aspect étroitement lié, les planificateurs n'apprécient pas les implications tactiques et opérationnelles de l'énergie, susceptibles de limiter les capacités, notamment lors de la projection d'effets cinétiques au-delà d'une seule mission, en particulier dans un environnement contesté. Enfin, l'incapacité de l'Alliance à mieux intégrer la gestion de l'OE pourrait mettre en péril ses forces et compromettre la réussite de ses missions.

L'exploitation de la technologie pour tirer un avantage géopolitique des vulnérabilités d'un adversaire, généralement désignée par l'expression « guerre hybride », est de plus en plus fréquente au 21e siècle. La guerre hybride a plusieurs synonymes, tels que « guerre/stratégies de zone grise », « concurrence sans conflit », « mesures actives » et « guerre de nouvelle génération ». La terminologie diffère, mais s'appuie sur les mêmes fondements ; à la base, la guerre hybride découle d'un principe vieux comme le monde (exploiter de manière asymétrique les faiblesses d'un adversaire), et y applique les caractéristiques du 21e siècle. Elle consiste à utiliser ou « détourner » les capacités destinées à servir le grand public, soit par le biais des marchandises qu'il consomme, soit par le biais des biens et services publics grâce auxquels chacun mène ses affaires quotidiennes.

Le projet se focalise sur la sécurité énergétique parce qu'il s'agit au fond du secteur le plus vulnérable, qui présente le plus grand potentiel de déstabilisation d'une société. Cependant, qu'est-ce que cela signifie concrètement ? Comment l'OTAN et les États membres peuvent-ils élaborer des politiques et contre-mesures applicables ? En outre, du point de vue de la sécurité énergétique, objectif principal de la présente étude, comment protéger l'infrastructure et rétablir le fonctionnement après d'éventuelles attaques contre ce secteur vital ? Bien que les pays souverains conservent la responsabilité de l'intégrité et de la défense de leur infrastructure énergétique, les opérations de l'OTAN nécessiteront une réponse unifiée et un approvisionnement énergétique international résilient, coordonné avec l'alliance, l'Union européenne et les objectifs nationaux.

Il est reconnu que l'OTAN joue un rôle d'avant-garde à la confluence de la sécurité énergétique, de la cybersécurité et de la guerre hybride. Dans le contexte de la sécurité énergétique de l'OTAN, les menaces hybrides peuvent être définies comme des actions menées par des acteurs étatiques ou non étatiques afin de saper ou compromettre 1) l'accès assuré de l'OTAN à des approvisionnements énergétiques abordables et admissibles et 2) la capacité de protéger et fournir suffisamment d'énergie pour répondre aux besoins essentiels de la mission, en influençant son processus décisionnel au niveau local, régional, étatique ou institutionnel.

Nous devons également garder à l'esprit que les deux principales composantes de la guerre hybride et de la dynamique de sécurité énergétique sont la cyberdéfense et l'influence malveillante. Bien que son rôle ait évolué, l'OTAN a toujours traité la dimension cybernétique comme une menace hybride pour les infrastructures énergétiques critiques (CEI) de ses États membres. Ces deux dernières décennies, nous avons constaté une multiplication des cyberattaques contre les systèmes de contrôle industriel (ICS) des chaînes d'approvisionnement énergétique des États membres de l'OTAN.

Les principaux objectifs du SAS-163 étaient de :

1) sensibiliser aux divers aspects de la guerre hybride énergétique ;
2) identifier son impact au sens large dans les domaines civil et militaire au sein de l'OTAN ; et
3) définir des modes d'action.

Cela inclut le fait d'atténuer l'impact sur les infrastructures et intérêts civils et militaires et d'élaborer des contre-mesures. Pour finir, le but du projet était d'apporter un soutien analytique aux dirigeants civils et militaires de l'OTAN.

Les conclusions essentielles de l'étude peuvent être résumées ainsi :

- Insécurité énergétique à court terme parmi les États membres de l'OTAN.
- Cybermenaces persistantes pour le secteur de l'énergie.
- Vulnérabilités de la chaîne d'approvisionnement du secteur énergétique.
- Impact sur l'énergie opérationnelle et les capacités militaires de l'OTAN.
- Une influence malveillante dans le secteur de l'énergie peut avoir des conséquences importantes.

L'étude recommande une analyse continue de la guerre hybride et de la sécurité énergétique, en particulier dans la sphère occidentale de l'OTAN, sans doute la plus vulnérable, et une enquête plus approfondie sur les technologies cybernétiques d'alerte préalable. C'est pourquoi nous avons soumis une proposition pour prolonger l'étude de trois ans.

ENERGY SECURITY IN THE ERA OF HYBRID WARFARE: SUMMARY FINDINGS

1.0 INTRODUCTION

On the day that Ukraine was supposed to start "isolation mode" tests for its new power network, beginning the process of decoupling from the Russian grid, Russia started a full-scale invasion of the country [1]. While this current 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, using cyber-attacks on the grid, disinformation campaigns, and seeking 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% the day of the invasion [2]. Step by step, Russia has used hybrid warfare to challenge energy security, not just in Ukraine, but across NATO member states as Russia seeks to beat back NATO influence and expand its power vortex on the world stage. Now escalating into 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.

Hybrid warfare can be defined as 'grey area' warfare, which exists beneath the threshold of armed conflict. Its goal is to erode confidence in civil society and democracy through cyber-attacks on critical infrastructure, targeted disinformation, and covert military operations. Threats across the Alliance are becoming more frequent, sophisticated, destructive, and coercive. Critical energy infrastructure is an attractive target and can include service disruptions in the civilian infrastructure on which the military depends. It may undermine social cohesion, demonstrating adversaries' destructive capabilities to coerce or intimidate. This poses threats to state sovereignty, as it gives adversaries a low-cost, high yield means to influence the policies of competitor states. Moreover, malicious cyber activity directed at the critical infrastructure of another state is effective, cheap, and deniable.

NATO member states' energy security is also being threatened across the fuel sector by Russia's monopoly of supply and ensuing manipulation of pricing and supply conditions for many European nations. While NATO member states' energy infrastructure encompasses large-scale distribution of fuels and power to its customer base, it was designed and built for efficiency, not for resilience. While it was built to achieve maximum speed of delivery and cost efficiency, the energy infrastructure is also highly networked with countless Industrial Control Systems (ICS) installed to meter and monitor the flow of product across all economic sectors. The critical energy infrastructure is thus an attractive target for adversary cyber-attacks or malign influence. Intersecting hybrid tactics with a vulnerable energy sector creates political, economic, and military risks that cannot be ignored.

In July 2020, the NATO Science and Technology Board authorized the formation of a Research Task Group on Energy Security in the Era of Hybrid Warfare (reference SAS-163), overseen by STO's System Analysis and Studies (SAS) Panel. The research team is dedicated to the study of confluence of energy security and hybrid warfare. Considering the recent events in Ukraine, a pre-release of key findings was requested. This document is an attempt to consolidate the vast data accumulated in the conduct of the study and to synthesize it into a concise list of vulnerabilities and actionable mitigations.

2.0 THE FINDINGS

This study found that systemic dependencies and vulnerabilities in energy critical infrastructure throughout the European Continent could impact the Alliance's political stability and threaten military effectiveness. Forward mobility and troop readiness directly is affected by energy shortfalls and increasing cyber vulnerabilities across NATO. In addition, ports, rail, aviation, nuclear facilities, and water distribution has been affected, and the impact of compromised energy ICS will continue in the immediate future.

The following preliminary findings of this project, which ends in December of this year, provide a sobering view of the challenges of hybrid warfare on energy security in NATO nations:

1) **Systemic energy insecurities among the European NATO member states will perpetuate long-term political, economic, and military vulnerabilities.**

   The primary insecurity is the procurement of hydrocarbons, which are still the bedrock of economic, political, and military stability on the Continent. More specifically, this primary insecurity can be attributed to both a lack of domestic production and a failure to diversify sources. Perhaps the most critical is the dependence on Russian fossil fuels, which supplies between 30 – 45 % of Europe's energy requirements [3]. Moreover, it is Russian exports of fossil fuels which support the current government. Recent examples of this dependence on Russian fossil fuels are Nord Stream 2 and the internal tensions it has caused within NATO [4].

   This systemic vulnerability in hydrocarbons is further exacerbated with technological challenges with the transitions to renewables, creating general grid instabilities. For example, stability issues have recently emerged in the European Central Power Grid. On January 8, 2021, the European grid, in response to an instability in the system resulting from a faulty crossbar coupler in a Balkan substation, split into two segments [5]. This split was necessary to avoid further instability, which could have led to blackouts on the Continent. While this example was not caused by hostile action, it does demonstrate broader civilian impacts military readiness and operations.

2) **NATO countries are under immediate and persistent cyber threats to critical energy infrastructure in the next 24 months.**

   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.

   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 [6]. Since the invasion of the Ukraine, significant cyber-attacks have impacted NATO member states. A Feb. 24 cyber-attack on a satellite providing services to Ukraine caused a region-wide internet connection outage in the Ukraine, but it also caused 40,000 users in Poland, Germany, Greece, France, Hungary, and Italy to have an internet outage. The same cyber-attack knocked 5,800 wind turbines in Germany and Central Europe offline affecting 11 gigawatts of power [7], [8]. Lithuania, Latvia, Poland and Romania and Central European states such as Germany continue to be targeted. Below are a few examples of threats – actual as well as potential – to NATO members due to hybrid warfare and energy insecurity.

   - **Germany** has been a testing ground for the Russian-based hackers **Berserk Bear's** (https://www.cytomic.ai/alerts/berserk-bear-cyberattacks/) malicious cyber activities, from attacking a number of energy companies and attempting to intrude on **Germany's grid** (https://intelnews.org/2018/06/21/01-2342/) in 2017, to its l**ong-term efforts** (https://www.cyberscoop.com/german-intelligence-memo-berserk-bear-critical-infrastructure/) to compromise the supply chain of critical infrastructure such as energy, water and power sectors up to the present time. Second, as Germany's Interior Ministry's Federal Audit found earlier in 2021, Germany is at heightened risk of grid blackouts through 2025. This is due to the energy shortfall as renewables are not producing enough energy to make up for nuclear plants being taken offline and coal needing to be phased out in line with Germany's energy goals. Hybrid warfare directed at an already unstable grid in the current environment could have devastating effects on Europe's economic powerhouse.

- **Romania's Port of Constanta** could be an immediate hybrid target due to location and technology. In addition to the fact that the port and its surrounding area are home to a NATO airbase, a nuclear plant, and a gas refinery ranking 9th among the 250 refineries in Europe and Africa, Romania's Exclusive Economic Zone shares a boundary with Bulgaria and Ukraine. Any disruption here could affect the Alliance as a whole. Note that since the invasion of the Ukraine on Feb. 24, 2022, Russian military ships in the Black Sea adjoining Romania's EEZ have rerouted or stopped commercial ships headed to Ukraine.
- **Lithuania** imports 70% of its energy requirements. In its **Nord Balt transmission** line, which provides 700 mw of electricity from Sweden to Klaipeda, Lithuania's energy independence has already been tested. In 2020 the line became inexplicably inoperable for a week, halting 4% of Lithuania's energy need for one day, and sending wholesale electricity prices in all three Baltic countries up by 52% [9], [10]. Lithuania has also been subjected to regular disinformation campaigns since 2020 with 20 public sector websites being attacked with disinformation on the Lithuanian government transition [11].

3) **Energy sector supply chain vulnerabilities across the Alliance impact military operations.**

Supply chain vulnerabilities have the potential to significantly impact member state economies and military operations. Moody's Analytics has reported that the greatest risk to the global supply chain is now caused by the Russia-Ukraine military conflict, not the pandemic [12]. With Russia supplying 43% of Europe's natural gas, 40% of the world's palladium, used for semi-conductors, and Ukraine supplying 70% of the world's neon, used to create computer chips, the prolonged uncertainty of the conflict could continue to severely affect the global supply chain [13]. As Russia is the world's number two oil producer, the conflict could continue to destabilize the world's oil and gas prices [14].

NATO forces are reliant on host nation energy systems, such as local grids and hydrocarbon delivery to fuel their military transport and aviation needs. Another layer of complexity is added when private contractors provide these critical services and have different cyber security standards.

Going forward, supply chain components will continue to be subject to major threats from different sub-chains that interact directly with low security scrutiny. These threats include the mining, oil and gas industries, petrochemicals, power, and utilities. Cyber security vulnerabilities in these industries are pervasive, increasing the threats due to the interactions within each sub-chain.

4) **Operational energy and NATO's military capabilities**

The Operation Energy (OE) requirements of the Alliance's warfighters continue to increase sharply due to the greater energy intensity of sophisticated platforms necessary to enhance force mobility, lethality, and operational tempo. As evidenced by the Russia-Ukraine war of 2022, NATO can no longer assume guaranteed and sustained energy in a conflict distinguished by a vast battlespace against an adversary with advanced anti-access/area denial (A2/AD) capabilities.

A specific operational challenge includes the 'fuel desert' between the Central European Pipeline System's (CEPS) eastern edge and NATO's forward-deployed assets in Eastern Europe. Supplying NATO assets in the wider Black Sea region will continue to be a logistical challenge during the current conflict. The result is the potential for diminished Alliance military operational capabilities in a potential resource constrained battlespace.

5) **Malign influence is directly impacting energy critical infrastructure.**

Digital democracies, which respect individual freedoms and openness, have been targets for malign influence campaigns. Hybrid activities, including cyber-attacks and disinformation campaigns, are attractive tools for state and non-state actors to achieve political objectives without military force [15]. Russia views cyber-attacks, hacking, and the spread of disinformation as instruments of foreign policy and security interests.

Russia also conducts information operations to spread disinformation and promote narratives aligned with Russian security interests [16]. 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 targeted 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 [17].

Russia's disinformation apparatus is active in Poland's energy sector. In March 2021, after Poland announced its strategic partnership with the US 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 [18].

Another recent example is the fate of Chevron's shale exploration in Romania, which received strong and unexpected local opposition, ostensibly based on environmental concerns. It was later determined that this opposition was funded by the Kremlin [19]. Finally, there is the question of ownership of European energy assets by Kremlin-affiliated companies. This lack of visibility into these actions presents questions of Russian influence and possible interference on critical energy assets within NATO member states. An example of this lack of visibility is the Kremlin-controlled Rosneft's partial ownership of Germany's Schwedt refinery [20].

3.0 MITIGATION OPTIONS

What solutions are there for militaries of NATO nations facing energy insecurities and hybrid warfare? The five security vulnerabilities identified here are interrelated, requiring a highly coordinated series of responses from the European Union, NATO, and Partnership for Peace members. This list of mitigations is not exclusive.

1) **Increased energy source diversity and resilience among the NATO member states**

   Energy source diversification can be subject to vested interests from commercial and environmental sectors. However, national security ramifications persist by continuing to rely on a single, and hostile source of energy, to include crude oil, natural gas, coal, and refined products [21]. Despite the ongoing war in Ukraine, as of this date, many NATO member states are still buying Russian sourced hydrocarbons. This continuation of sourcing Russian hydrocarbons indicates the difficulties in reshaping long-standing national energy policy. Nevertheless, a divestment plan to remove this source of Kremlin revenue is recommended. Solutions to the hydrocarbons deficit should consider expanded use of nuclear energy, as well as unconventional energy production, notably hydraulic fracturing, on the Continent. Additionally, as demonstrated by the January 2021 Central European Power Grid split, higher levels of resilience are needed, requiring a coordinated response across borders and economic sectors.

2) **Malicious cyber mitigation strategies for critical energy infrastructure**

   The SAS-163 cyber team identified three potential solutions to mitigate cyber-attacks and increase energy independence for militaries of NATO member states and to prevent cyber vulnerabilities to energy critical infrastructure. These options include new Cyber Early Warning Systems (CEWS) that include virtual modeling, small modular reactors, and microgridding.

   Cyber early warning systems that include virtual modeling of energy critical infrastructure for early mitigation of malicious intrusions is 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 cyber-attacks. By using the virtual model of a natural gas pipeline and combining it with machine learning, cyber-attacks 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 implementation of successful prototypes, grids, gas pipelines and other energy sources can be more adequately protected from cyber-attacks. Any CEWS development must be in addition to anomaly detection monitoring in critical energy infrastructure.

Small Modular Reactors (SMRs) are advanced nuclear reactors that have a power capacity of up to 300 MW(e) per unit, which is about one-third of the generating capacity of traditional nuclear power reactors. Given their smaller footprint, SMRs can be used on locations not suitable for larger nuclear power plants. SMRs offer savings in cost and construction time, and they can be deployed by NATO states incrementally to match increasing energy demand.

In areas lacking sufficient lines of transmission and grid capacity, SMRs can be installed by militaries into an existing grid or remotely off-grid, as a function of its smaller electrical output, providing necessary energy for military, industry, and the population. SMRs 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 for 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 SMR between NATO nations is the recent intergovernmental agreement between Romania and the United States signed December 2020 for the US 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 be deployed in the Baltics, Poland, Bulgaria, Turkey, and Greece as well [22].

Microgrids are another alternative source of energy 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. However, they often need a lead time of several years to model, install and to produce enough independent energy in the case that it must be decoupled from a grid as they must be suited to each installations' unique infrastructures and energy needs.

Microgrids have had success on US bases such as the Marine Corps Air Station Miramar in San Diego, the Otis Air National Guard Base, and the Parris Island microgrid at the US Marine Corps Recruit Depot [23]. Before these success stories can be transferred to other US military installations in Europe or North America, however, a few considerations must be made. 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. At the same time, European militaries are actively developing prototype systems for mobile military camps, however, these often lack cybersecurity considerations in the design [24].

3) Supply chain resilience

Proactive risk mitigation begins at the very foundation of global supply chain network with a cyber-physical secured design. In 2021, NATO members heads of state reiterated in the Strengthened Resilience Commitment that there is an urgent need to "step up efforts to secure and diversify supply chains, as well as to ensure the resilience of critical infrastructure (on land, at sea, in space and in cyberspace) and key industries" [25]. Most aspects of resilience are inextricably linked to the interdependencies between supply chain components. Military forces, especially those deployed during crises and war, heavily depend on the civilian and commercial sectors for transport, communications, and even basic supplies such as food and water, to fulfill their missions [26].

NATO also updated its baseline requirements in 2020 to reflect the challenges presented to the supply chain by emerging communications technologies and COVID-19 pandemic, but further actions must be taken in the light of the analysis of the evolution of the war in Ukraine.

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;
4) Increasing stocks;
5) Reshoring;
6) Automation with a careful evaluation of cyber risks;
7) Clearly stated security requirements stated by the buyer and transparent security practices by manufacturer; and
8) Heightened monitoring and control during warehousing and shipment of equipment to ensure integrity of product is not compromised before delivery.

4) Enhanced military capabilities in an Operational Energy (OE) context

The ability of modern militaries to effectively manage OE will help ensure future operational success. OE not only includes liquid fuels, but also power generation and distribution in a networked military force. The war in Ukraine has forced NATO to reconsider its military logistical footprint, particularly as it related to forward-deployed forces in Eastern Europe. Indeed, in the current A2/AD environment, the ability to store large quantities of fuels may be difficult, requiring a more flexible or distributed model.

Two considerations within the Alliance should be NATO Pipeline System (NPS) expansion and improved or hardened storage capacity. Most importantly is the expansion of CEPS, NATO's largest and, arguably, most significant pipeline, though it is recognized there will be environmental challenges to such construction.

What becomes evident is the need for NATO leaders to recognize OE management as a mission enabler, requiring a deeper understanding of its application in the 21st Century battlespace. This can be addressed through doctrinal review and rigorous training exercises, which emphasize interoperability and operational competence in four general areas: fuels, battlespace power generation and distribution, power storage and command and control. Developing such experienced warfighters requires a new generation of leaders who understand the importance of OE as a mission enabler and can effectively leverage this asset. Ultimately, this forces the consideration of NATO capabilities in a contested logistical environment.

The Alliance has numerous options available to it, for instance, leverage existing OE domain work underway and relationships in the US DoD, as well as Allied Command Transformation in Norfolk, VA, and Joint Forces Command, Brunssum, Netherlands. Additionally, the NATO Defence Planning Process (NDPP) and more specifically, the Minimum Capability Requirement (MCR), important tools for deriving posture and mission capabilities, can be leveraged for this effort.

5) Countering malign influence through a disinformation rapid response force

Early detection of disinformation campaigns is crucial to prevent malicious actors from escalating and exploiting this activity. Because of its ubiquity and importance in virtually all sectors of modern society, critical energy infrastructure is a natural target for malign actors [27]. Additionally, the immediacy of this threat, weaponized by modern technology and mass media, requires near-instantaneous response. 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 their nascent stages. This task force could be staffed by local credible actors with a strong presence at the community level. Their focus would be on building a network to ensure that every state is able to evaluate disinformation from different perspectives. This 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.

Malign influence is not limited to communication channels, but to long-term investment by hostile actors as well. There is a need for greater accountability for hostile investors, particularly when this external interest targets NATO member state critical energy infrastructure. Where necessary, stronger parliamentary approval should be considered based on national security assessments. An example of how this process is addressed in the US is The Committee on Foreign Investment in the United States (CFIUS), which is an interagency committee chaired by the Department of the Treasury and is responsible for reviewing foreign investments in, or acquisitions of, US businesses and real estate to determine if the transaction threatens to impair US national security.

4.0 CONCLUSION

As evidenced by the Russia-Ukraine war of 2022, NATO can no longer assume uncontested energy across a vast battlespace against an adversary with advanced anti-access/area denial (A2/AD) capabilities. NATO finds itself just behind the front lines of a war that will provide both kinetic and non-kinetic challenges to its energy security. Russian hybrid warfare methods against NATO energy infrastructure will be a persistent threat, demanding a vigilant NATO response. NATO has taken positive steps to address both energy security and hybrid threats, including through the creation of organizations, such as the Hybrid Challenges and Energy Security Section and the Energy Security Center of Excellence.[1] NATO will need to continue to adapt to emerging and hybrid threats to energy critical infrastructure and energy security. While it prepares to defend against traditional adversaries, Russia, and China, heightened resilience will be needed to counter threats from terrorists and non-state actors who are willing to use disinformation, cyber warfare, and covert operations for their own gain. Investing in and building the educated teams, hardened technologies, and the diverse supply chains it needs to keep its member states' energy supplies secure will help ensure NATO's military readiness in the future.

These challenges are exacerbated by new strategies, operational constructs, force designs, and new and emerging weapons/platforms that compound the complexity and dynamics of OE management. In this fluid battlespace, dictated by greater reliance on technology and ever-increasing energy requirements, NATO planners and operators need greater understanding of OE to ensure sustained operations in contested logistics environments. More specifically, these challenges are manifest by new systems that will not work in combat due to operational energy limitations. Closely related, planners do not appreciate the tactical and operational impact of energy, which could limit capabilities, notably in projecting kinetic effects beyond a single mission, particularly in a contested environment. Ultimately, the failure to adequately prepare the Alliance to better integrate OE management could imperil its forces and mission accomplishment.

What becomes evident is the need for NATO leaders to recognize OE management as a mission enabler, requiring a deeper understanding of its application in the 21st Century battlespace. This can be addressed through doctrinal review and rigorous training exercises, which emphasize interoperability and operational competence in four general areas; fuels, battlespace power generation and distribution, power storage and command and control.

[1] The European Commission's Hybrid Threats Center of Excellence in Helsinki, Finland should also be mentioned.

For these reasons, it is imperative that NATO training and education systems prepare military leaders to address the criticality of OE and the enhanced combat capabilities it provides. With the associated challenges and opportunities, there is the potential that NATO military personnel will miss the larger picture, leading to a myopic view, with little understanding of conditions at echelons above or below.

The SAS-163 team envisions further analysis in the field of hybrid warfare and NATO energy security. This will entail greater emphasis on the Baltic and Black Seas, as well as deeper analysis of advance warning technologies in the cyber security field.

5.0 REFERENCES

[1] Lee, A. "War in Ukraine: Russia attacks nation looking to renewables and EU grid for energy freedom," Recharge, Feb 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

[2] Duffy, K. "Russian gas flows to Europe via Ukraine reportedly jumped nearly 40% on Thursday, underscoring the continent's dependence on Putin's energy," Business Insider, Feb 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

[3] European Commission. "Joint European action for more affordable, secure energy," European Commission, Mar 8, 2022. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1511

[4] Buchholtz, K. "Chart: Which European countries depend on Russian gas?" Statista, Feb 24, 2022. https://www.statista.com/chart/26768/dependence-on-russian-gas-by-european-country/?msclkid=5b742d93b8ea11ec930eb903dda236a4

[5] Starn, J., Parkin, B. and Vilcu, I. "The day Europe's power grid came close to a massive blackout," Bloomberg, Jan 27, 2021. https://www.bloomberg.com/news/articles/2021-01-27/green-shift-brings-blackout-risk-to-world-s-biggest-power-grid?msclkid=ee4238c2b8e911ec97d0d5bea2e24ae5

[6] Associated Press. "Russian officials charged in years-old energy sector hacks," US News, Mar 25, 2022. https://www.usnews.com/news/business/articles/2022-03-24/russian-officials-charged-in-years-old-energy-sector-hacks?msclkid=5fbb7759b8ee11ecb9487d9555eadb7f

[7] Henry, J. "Europe cyberattack results to 'massive' internet outage | About 5,800 wind turbines went offline," Tech Times, Mar 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

[8] Viasat. "KA-SAT Network cyber attack overview," Mar 30, 2022. https://www.viasat.com/about/newsroom/blog/ka-sat-network-cyber-attack-overview/

[9] The Baltic Course. "Lithuania-Sweden power link NordBalt back in service," The Baltic Course, June 16, 2020. http://www.baltic-course.com/eng/energy/?doc=156716&msclkid=112f64ccbcd511ec911bfbe86b742903

[10] 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

[11] Coble, S. “Lithuania suffers ‘most complex’ cyber-attack in years,” Dec 16, 2020. https://www.infosecurity-magazine.com/news/lithuania-cyberattack/

[12] Uy, T. “Russia-Ukraine’s impact on global supply chains,” Moody’s Analytics Economic View, Mar 3, 2022. https://www.economy.com/economicview/analysis/387912

[13] Amaro, S. “Kadri Simson says EU ready if Russia decides to cut off the gas,” CNBC, Mar 3, 2022. https://www.cnbc.com/2022/03/03/kadri-simson-says-eu-ready-if-russia-decides-to-cut-off-the-gas.html

[14] Egan, M. “Russia-Ukraine crisis replaces Covid as top risk to global supply chains, Moody’s says,” CNN, Mar 4, 2022. https://www.cnn.com/2022/03/04/business/russia-ukraine-supply-chain-oil/index.html

[15] Yegorov, O. “Why does Russia have such a low unemployment rate?” Russia Beyond, 2019. https://www.rbth.com/business/330166-russia-low-unemployment

[16] Lavikainen, J., Pynnöniemi, K., and Saari, S. “Russia’s foreign policy”, in Russia of Power, 2019. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161710/Russia%20of%20Power.pdf

[17] Cockrell, C.D. “Russian actions and methods against the United States and NATO,” Army University Press, Sep 22, 2017. https://www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2017-Online-Exclusive-Articles/Russian-Actions-and-Methods/msclkid/e7433684b8ee11eca6d1fc6744e6d1df/

[18] Gigitashvili, G. “Cyber-enabled information operations targets Poland with radiological leak hoax,” Atlantic Council Digital Forensic Lab, Apr 2, 2021. https://medium.com/dfrlab/cyber-enabled-information-operation-targets-poland-with-radiological-leak-hoax-28a5b1fb6776

[19] Higgins, A. “Russian money suspected behind fracking protests,” The New York Times, Feb 1, 2014. https://www.nytimes.com/2014/12/01/world/russian-money-suspected-behind-fracking-protests.html?msclkid=b1917ad7b8e911ec94a82045798b602d

[20] Reuters Staff. “Germany puts Rosneft’s purchase of Schwedt refinery stake under review,” Reuters, Mar 21, 2022. https://www.reuters.com/business/energy/rosnefts-purchase-shells-schwedt-refinery-stake-under-review-econmin-2022-03-21/?msclkid=e64dd11ab8e811eca34b1667754da098

[21] Kowsmann, P. “New Sanctions add pressure on Russia but don’t shut off business,” The Wall Street Journal, Apr 8, 2022. https://www.wsj.com/articles/new-sanctions-add-pressure-on-russia-but-dont-shut-off-business-11649414051?mod=Searchresults_pos9&page=1

[22] World Nuclear News. “Teaming agreement signed for Romanian SMR deployment: New Nuclear,” World Nuclear News, Nov 5, 2021. https://www.world-nuclear-news.org/Articles/Teaming-agreement-signed-for-Romanian-SMR-deployme

[23] Wood, E. “Military microgrids: Four examples of innovation,” Microgrid Knowledge, Dec 3, 2019. https://microgridknowledge.com/military-microgrids-four-examples/

[24] Butrimas, V. “Assessment study of cybersecurity of smart-grid technologies employed in operational camps,” 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

[25] NATO. “Strengthened Resilience Commitment,” NATO, Jun 14, 2021. https://www.nato.int/cps/en/natohq/official_texts_185340.htm

[26] NATO. “Resilience and Article 3,” NATO, Jun 11, 2021. https://www.nato.int/cps/en/natohq/topics_132722.htm

[27] Colomina, C., Margalef, H.S. and Youngs, R. “The impact of disinformation on democratic processes and human rights in the world,” European Parliament, p. 48, Apr 2021. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653635/EXPO_STU(2021)653635_EN.pdf

Annex A – NATO ENERGY SECURITY ANALYSIS

A.1 EUROPEAN ENERGY SECURITY ENVIRONMENT AND RUSSIAN ENERGY DOMINANCE

A.1.1 The European Energy Security Environment

A.1.1.1 Introduction

With 450 million consumers and a $17 trillion economy, the European Union is the world's largest trading block, so its global economic influence is considerable [1]. This influence is more than purely economic, as it also encompasses global, regional, political and social variables. Yet, the EU has insufficient domestic energy production necessary to maintain its vitality, and thus must import most of its requirements. Moreover, this energy deficit is coupled with a concerted effort by the EU to shift to a low-carbon energy infrastructure, based primarily on renewable sources and, in certain cases, nuclear power. The result is a vulnerable energy environment, subject to geo-political pressures and leading to possible shortages or price increases, which could result in generally unstable economic and political conditions. The immediate-term impact of the war in Ukraine is rising energy cost and lower availability in 2022 [2].

This potential instability has an additional national and regional security impact, considering that many NATO states are also EU members and are subject to its energy mandates. Thus, because NATO operates on, and is ultimately dependent upon, EU infrastructure, actions taken at the national and supranational levels directly influence the NATO mission. It is here that the impact of the EU, and more specifically the European Commission, plays a considerable role in this phenomenon. Much of this section looks at the EU's domestic energy programs, which fall broadly under the European Commission's Directorate-General for Energy (DG-ENER).

As energy is essential to maintaining a modern nation state, the ability to source adequate, reliable, and cost-effective energy is critical. Indeed, any significant and long-term disruption to such a supply could be catastrophic, resulting in economic downturn, loss of life, civil unrest, all impacting national security. These risks are juxtaposed, and made more complex by balancing the shift to a low-carbon energy environment while still relying on a traditional fossil fuel-based energy infrastructure. To maintain economic and social equilibrium, certain levels of energy security are required; including supply security, and reliable production and distribution systems. The International Energy Agency (IEA) defines Energy Security as "…the uninterrupted availability of energy sources at an affordable price" [3], [4], [5]. Maintaining energy sector efficiency across the EU is a contributing factor to its broader energy security, necessitating a long-term, harmonized approach.

A.1.1.2 Geo-Political Considerations

Europe's post-war development, and the impetus which enabled it to reach its current state as a political and economic power, should be acknowledged. The EU benefits from its position of relative economic and political strength, and contributes to the changing energy landscape in the region, which also impacts NATO member states' ability to maintain readiness.

The EU is enduring its own set of economic and demographic challenges, also brought about by declining birth rates and an inability to enact reform within some member states. This is further evidenced by the Union's persistent North-South economic divide, in addition to the growing East-West divide. The EU is buttressed by the German economy which, up to now, has demonstrated remarkable strength and stamina, coupled with Berlin's relatively newfound political confidence. Though many Germans, as well as its neighbors, are wary of a politically assertive Berlin, it is generally expected that Germany will ultimately assume a role commensurate with its economic standing. This would include Berlin's ability to coax its EU partners into enacting economic and labor reforms which will ensure greater economic stability. A by-product of Germany's role as Europe's economic engine ensures the EU's center of gravity continues to shift to the east, thereby drawing Eastern Europe into Brussels' economic and political sphere.

The 2022 war in Ukraine awakened many in Europe to the threat posed by a Putin-led Russia. The result has been deeper sanctions and a determination to source non-Russian hydrocarbons. This disruption to the energy supply chain has created higher prices and potential shortages, which could result in hardships during the winter months of 2023 and after.

A.1.1.3 Germany

As Europe's economic engine, Germany deserves special attention. Following the third-longest tenure in German history, Angela Merkel of the center-right Christian Democratic Union was replaced in December 2021 as Federal Chancellor by Chancellor Olaf Scholz of the center-left Social Democratic Party, who must navigate Germany's continued progress toward a pledged carbon neutrality by 2045 – 2050. This transition promises to be neither smooth nor necessarily steady, whether in Germany or elsewhere in the world [6]. Central to this transition are long-standing policies adopted by the previous government to shut down all of Germany's remaining nuclear power plants, as well as all remaining coal mines. While these initiatives have been shelved in the wake of the Ukraine war the subsequent energy crisis, the strong environmental lobby in Germany could resurrect similar policies in the future.

Assuming that these objectives are further pursued (when, and indeed whether, they will be fully accomplished remain separate issues), Chancellor Scholz' government faces certain unavoidable considerations, ones constituting not only an informal inference through a network of evidence but also enjoying probative value. And while current political circumstances in both Germany and Europe demand an acknowledgment that uncertainty is intrinsic to prediction [7], these considerations might reasonably include:

- Berlin needs to further define what constitutes energy security and civil preparedness for Germany in view of the NATO Treaty's Article 3, particularly as regards the cost-effectiveness of wind, solar, and hydro power, as well as the economics, logistics, and timeline for an eventual conversion of domestic pipeline infrastructure and power plants from natural gas to hydrogen [8], [9].
- Determining how much of the stated requirement of natural gas as a "bridging fuel" will continue to be imported from Russia with all that such imports imply for the possibility of Moscow's exerting geo-political pressure on Germany and East Central Europe before that fuel is finally abandoned in favor of renewables and hydrogen.

A.1.1.4 US Geo-Political Engagement

As Europe's primary security guarantor, the US has a strong interest in the Continent's future viability. In the years immediately after the USSR's collapse, the US was perhaps the strongest advocate for self-determination and economic liberalization in the newly independent Eastern Bloc states. Additionally, there was the Dayton Accord and the bipartisan push for new NATO members. Following 9/11, there was a clear US shift to the Middle East, though the George W. Bush administration maintained relations with South East Europe.

Yet, beginning in 2009, there has been a marked period of diminished US attention, brought about by global economic hardship, changing regional priorities and the US pivot to Asia. The relative US withdrawal from the Middle East, hastened by military disengagement in Iraq and Afghanistan, has added to this relative sense of drift. Continued instability in the Middle East and Eastern Europe, particularly in Ukraine, has redirected US attention (reluctantly) back to the Black Sea and South-Eastern Europe. The question must be asked whether this is temporary or a long-term reengagement.

The US became increasingly concerned about Russian energy dominance and its growing market share of Europe's energy imports. US opposition to the Nord Stream II pipeline began under Obama, though continued under the Trump Administration. On August 2, 2017, Countering America's Adversaries Through Sanctions Act (CAATSA), was signed into law by President Donald Trump and enhanced guidance was implemented in 2020 [10], [11]. Yet, it was the 2020 NDAA, with its strong stance against Nord Stream II and TurkStream in the December 2019 threatening stiff sanctions, which effectively brought a temporary halt to construction [12]. The Biden administration waived these sanctions in early 2021, yet, as the Russians began pressuring Ukraine in late 2021, the 2022 NDAA attempted to message the Kremlin, for instance the NDAA notes the "…naval presence in the European Command area of responsibility and its ability to respond to challenges in the Black Sea, Mediterranean, and Arctic", and "…capabilities for countering Russian aggression and hybrid warfare in the European theatre, including cyber capabilities"[13].

A.1.1.5 Migration

Mass migration is mainly internal, inter-state or inter-regional within the African continent [14]. Migration flows were relatively controlled until the Arab Spring and the beginning of the Libyan conflict. The EU cooperated with North African governments, especially Libya, to control migration flows in exchange for financial support as well as technical assistance [15]. EU Member States, mainly Spain, Greece, and Italy, experienced a rapid increase between 2015 and 2016, after the Arab Spring uprisings. The UNHCR estimated between 6,900 and 22,800 sea and land arrivals per month from Northern Africa [16], though these have dropped since 2016. In the future, climate and environment-related migration may increase due to drought, floods and other natural phenomena [17].

The 2015 migration crisis brought its share of security concerns to Europe, such a terrorism, crime, and human trafficking, motivating its involvement in the resolution of conflicts such as in Libya or in counter-terrorism operation in the Sahel. Additionally, as mentioned earlier, terrorist groups benefit from unstable political situation and conflict-induced migration to conquer new territories, including hydrocarbon fields and terminals, giving them more power and resources [14].

A.1.1.6 China's Belt and Road Initiative

China's economic rise has pushed into the EU periphery, notably via the Belt and Road Initiative (BRI), an expansive, multi-trillion-dollar trade and infrastructure project. Established in 2013 as President Xi Jinping's flagship foreign policy platform, China claims that a minimum of sixty-five nations have agreed to jointly participate in the BRI [18]. There has, however, been evidence to the contrary as only twenty nations' representatives attended the May 2017 BRI Summit, nine of whom were not on China's initial list of sixty-five partners. This and other transparency issues have shrouded the BRI's legitimacy in doubt [19].

Simultaneously, the CCP has demonstrated relative disdain for international environmental accords, arguing that they should not be restricted in their mass industrialization efforts just as Western nations in the latter two centuries were not. Climate science has progressed significantly in the last 20 years alone, and the world has been made aware of various pollutant's impact. China, however, sees climate change as an opportunity to further establish themselves as a dominant global trading power. With the potential for melting Arctic ice caps, the CCP has published a 'White Paper' claiming that it is a 'near Arctic nation', to lay future claim to both the resources available in that region and the shipping routes. This signals that, despite domestic policy trends toward electric cars and some renewable energy efforts, the CCP may view non-accordance with international climate protocols as beneficial on multiple fronts [20].

A.1.2 Russian Energy Dominance:

A.1.2.1 Introduction

According to the EIA, Russia's proven oil reserves total 80 billion barrels, considerably below Saudi Arabia's 300 billion barrels, though the two nations are at near parity in production capacity with approximately 11.2 million b/d [21]. Shortly after the Cold War, the energy services and analysis company, DeGolyer & MacNaughton, determined Russia's recoverable reserves at between 150 to 200 billion barrels [22]. In 2020 Russia exported almost 5 million b/d of crude oil and condensate, most of which went to European countries (48%), particularly Germany, the Netherlands, and Poland. China was the largest importing country of Russia's crude oil and condensate, at 31% [21].

One of the world's top energy producers and possessing a formidable (on paper) conventional military and nuclear force, Russia's ability to wield power and influence beyond its borders far outclasses its neighbors. Bolstered by energy revenues, Russia under Vladimir Putin is determined to regain its status as a global power, a position it had humiliatingly lost in the turmoil following the collapse of the Soviet Union. This attempt to regain international standing has been conducted with an aggressive posture vis-à-vis its neighbors, driven by an energy nationalism, whereby Moscow leverages its preponderance in energy resources into a geo-political tool. By all accounts, Russia's invasion of Ukraine in February 2022 has thrown the status quo into disarray. Western sanctions, and deliberate delivery cutbacks on the part of the Kremlin, have cut into Russia's European exports, the high cost of energy has helped soften the economic blow.

A.1.2.2 The Russia-Western Geo-Political and Economic Divide

Shortly into the post-Cold War era, Russia-Western relations, though never warm, did benefit from cooperation on a variety of geo-political issues, notably arms control. Presidents Boris Yeltsin and Bill Clinton appeared to have developed a true personal friendship during this time, which facilitated bilateral relations. Nevertheless, the Kremlin under Putin views expanding Western influence on its borders as intolerable; its determination to retrieve and maintain its great power status has been the central tenet. Much of this is seen as Russia re-exerting influence after the humiliation it suffered following the Cold War, fueled by Moscow's sense of victimhood at the hands of the West. Moreover, there is Western interest in countering Moscow's actions and ensuring an equal opportunity to bring oil and gas products to market without external Russian interference.

Most evident in this fractious geo-political divide is Russia's use of energy as a foreign policy tool. Therefore, it is important to view South-Eastern European energy relations through the lenses of the 2006 and 2009 gas crises, the 2008 war with Georgia, and the current standoff in Ukraine, all of which demonstrate the growing divide between Putin's Russia and the West. There appears no end in sight to the downward trend in relations, which has dashed the hopes of many on both sides of the divide anxious for normalization. The result is that East-West relations are more strained now than at any time in the post-Cold War era, so closing this political and economic divide is daunting.

As a nuclear armed petro-state, Russia will continue to wield considerable geo-political power while creating consternation among its neighbors. In this role, energy policy and economic dividends of fossil fuel sales continue to fund Russian expansionism and influence Eurasian continental stability. Russian actions in the Black Sea and Baltic Sea similarly constrain maritime port access to fuel for NATO members and EU states. It should be kept in mind, however, that Russia is operating from a position of growing weakness; and without political and economic reform the long-term trends, including demographic trends, are not in its favor. As Moscow's stability is particularly dependent on oil and gas revenues, its relative technological backwardness in this sector and limited investment capital is hampering Russia's ability to fully exploit these reserves. In the Cold War a strong Soviet Union was a concern, though there is now fear that a weak Russia is more dangerous. The performance of Russian armed forces in Ukraine demonstrates this weakness. Therefore, a humiliated and paranoid Kremlin, coupled with diminishing state revenues, will lash out unpredictably and countenance further pressure on its near-abroad or its internal political foes.

More recently, we have seen the impact of COVID-19, war in Ukraine and Western sanctions on the Russian economy, which points to a general unease within Russia. These conditions lead to a sense of foreboding and unpredictable circumstances for the future among Russia's neighbors, hardly conducive for long-term economic stability and social development [23].

Russia will vie for a Northern Lake and the oil strata under the Arctic has vast reserves, so the contest for northern resources is bound to involve every participant touching the Arctic including the US, Russia, China, Canada, Sweden, Norway and likely a few more. The recent accession to NATO by Sweden and Finland has also shaken Russia's sense of security in the 'high north'.

A.1.2.3 Nationalization and Russian Energy Strategy – An Industrial Military Complex

It is impossible to discuss Russian domestic politics without considering its close relationship with the energy sector, which is responsible for filling the state coffers and seen as a source of wealth and a steppingstone to national leadership and influence. Surrounding Putin in his inner circle is the siloviki, a clutch of ex-KGB officers in whom Putin has placed considerable trust. In addition to the intelligence contingent are Putin's former colleagues, which combined with the siloviki, create a tight knit group holding key public and private sector management positions. These Putin associates predominate in Russian energy companies, for example, Dmitry Medvedev, Russia's former president and current prime minister, was Gazprom's chairman before being elevated to national leadership. Igor Sechin, a former intelligence officer and Putin's chief of staff before he was put at the head of Rosneft, is one of the most influential men in Russia. Alexei Miller, Gazprom's president, was subordinate to Putin while both were in the St. Petersburg mayor's office [24], [25].

The Ministry of Energy, with control of Russia's primary revenue creator, holds a key position within the government by providing oversight of the energy sector and working closely with the state-run firms. Until 2008 it was the Ministry of Energy and Industry. Under Alexander Novak, a key Putin lieutenant, the Ministry develops and implements national energy priorities and intergovernmental agreements. It also provides guidance to Russian companies operating outside the country to facilitate access to world energy markets. Finally, the ministry promotes stable relations with consumers and negotiates multilateral and bilateral energy agreements [26].

In June 2020, Russia's Energy Strategy to 2035 was released, which called for diversified energy exports, modernization of the country's energy infrastructure, greater competitiveness, and improved energy sector innovation, all designed to increase revenue and expand natural gas infrastructure, in eastern Siberia and the far eastern regions.

It is natural gas where Russia wields considerable geo-political power and holds a decisive competitive advantage. This is partly attributed to the growing popularity of gas in world markets for environmental considerations as well as its relative low cost and increased functionality, ranging from heating, electricity generation and transport. With nearly 50 tcm, Russia holds approximately one quarter of the world's proven reserves, 95 percent of which are located in Siberia or northern Russia [27], [28].

The main player in Russia's gas industry is Gazprom, with 330,000 employees and 80 percent of the country's total natural gas output; the company by itself accounts for 10 percent of GDP and a quarter of state revenues [21], [29]. This dominance is codified through a legally sanctioned state monopoly which allows it to control the gas sector more completely than Rosneft, its closest parallel in the oil sector. Gazprom's monopoly status was legislated in 2005.

A difference from the Russian oil sector is that Rosneft must rely on Transneft to export its product, while Gazprom's pipeline arm is organic. With an imposing position in both upstream and downstream markets, to include control of the domestic pipelines, Gazprom has unique influence in the Kremlin which translates into unrivalled political and economic power. Riding the energy price spike of the mid-2000s, Gazprom reached a market capitalization of $362 billion in 2008 [30], [31], though in October 2022 this had dropped to $85 billion [32]. The Russian economy experienced weakness since the post-Crimea 2015 economic crisis, with average GDP growth to 2020 near 1.5%. The costs of renationalization, corruption, regulations and laws that impair the operations of businesses, and Western sanctions have combined to create considerable uncertainty. Additionally, COVID-19 and the global economic crisis will further lower Russia's growth expectations. The low unemployment rate at roughly 5% is deceptive, as Russian law protects employees from being laid off during economic downturns, so employers are forced to cut wages instead [33].

The early 2020 collapse of the Russia-OPEC agreement on oil production levels lower demand due to the COVID-19 pandemic temporarily pushed prices to $20 a barrel. Moreover, chronic corruption, lack of economic reforms will have long-term negative impact on Russia's GDP growth rates.

The economic crisis has not hampered political and military ambitions: nearly 50% of tax revenue originates from the oil and gas sector, which is indicative of the role oil and gas reserve's role in the Russian domestic economy and explains the Kremlin's Arctic activities. A result of this dependency on world market prices, Russia compensates for the potential trade gap through accumulation of foreign currency and takes measures to keep its foreign debt small [34].

Increased protests indicate that Putin's social contract is no longer valid due to social, economic and demographic reasons. These can be tolerated up to a certain level, social unrest will not likely change Russian government soon due to the state's suppression of protests and methods of influencing public opinion.

Looking at the long-term trends, the oil and gas fields of Western Siberia are more than 40 years old and will require capital and modern technologies to meet current levels of production. Eventually, new fields must be developed, though Gazprom's current debt load, coupled with the impact of sanctions, makes that an unlikely prospect without external investment [35]. Hence there exists an insoluble gap in which investors are reluctant to commit in an untrustworthy climate, and Russia is unable to meet its full economic potential and contractual obligations without foreign capital.

Finally, as has been repeatedly demonstrated is Russia's willingness to use energy as a blunt foreign policy tool. Continued exploitation of its neighbors' energy weaknesses will perpetuate instability in its near-abroad, forcing states to either align closer to the West, enhance their own security postures, or reach an unfavorable accommodation with Moscow. This strategy demonstrates the lack of diplomatic depth available to Russia, whereby Moscow's most potent coercive mechanisms are its energy arm or military intervention. And while this policy bolsters Russia's short-term geo-political standing, it maintains an unhealthy dependence by the state on oil and gas revenues, manifest by resentment and is counterproductive over the long-term by fomenting instability on its borders.

Domestic instability and political machinations are perhaps the most significant challenges to Russia's long-term growth. Putin's authoritarianism has always been buttressed by the high price of oil and gas which masks deep-seated social and economic problems and removes the impetus for long-term reform and allows power consolidation in the Kremlin's top echelon. Most Russians appear to accept such activity as the price of stability and global prestige that has been credited to Putin [36]. Staffed with political allies, this 'trifecta' which is the Russian energy realm encompassing the state, the corporate and the personal, demonstrates there is little doubt that control of the energy sector is firmly held in Vladimir Putin's hands [37]. The impact of Putin's control of Russian energy policy ensures his presence will be felt long after he leaves office.

Russian resentment of the West, brought to light during Putin's 2007 speech at the Munich Security Conference, indicates there continues to be a strong sentiment of victimhood and revenge emanating from the Kremlin and which finds a receptive audience among the populace [38]. Subsequent claims by Putin that US or Western actors are behind the Ukrainian crisis, as well as the exploitation of unconventional plays, such as fracking, reinforce the theme of the Russian victim. This phenomenon whereby Russia's actions under Putin seem determined to settle old scores and make right real or perceived slights at the hands of Russia's enemies falls on sympathetic ears [39]. This notion is further reinforced by the general perception that the Crimean annexation and civil war in Ukraine are being touted as a victory for Moscow in a geo-political tug-of-war reminiscent of the Cold War. Putin still has a firm grip on power, though it remains to be seen if this continues as low oil and gas prices induce greater economic hardship.

A.1.2.4 New Generation Warfare – A Game of Sanctions

The Russian annexation of Crimea set in motion a series of Western tools to force compliance with the Minsk Accord and later Minsk II, the first set after the annexation of Crimea and the second after the Russian involvement in the conflict in Eastern Ukraine. Although the sanctions were effective at a practical level, such as prohibiting trade, financial flows and investments, hampering their economic and technical advancements, the results are inconclusive [40]. Sanctions forced Russia to conduct its own technology research and diversify within the domestic military-technical complex of state companies. The sanctions, seen as an attempt to invoke regime change and not behavioral change, impacted the average Russian citizen, the ruling elite, which could unify the population against a 'common enemy' [40]. Until March 2022, Western nations lacked a strategic vision on the purpose and duration of sanctions necessary to result in a correction of Russia's foreign policy actions. It remains to be seen how Russia withstands the new, harsher sanctions.

Russia's cooperation with China is a logical and convenient move. The sanctions have forced Russia to diversify its economic approach towards the East and redirect commercial flows and develop new partnerships. These encompass finance, redistribution of oil and gas flow and resource exploration in northern Russia and the Arctic [41]. This cooperation will last as long as it serves China's interest, however it does provide Russia relief from Western sanctions.

A.1.2.5 The EU-Russia Energy Dialogue

The EU-Russia Energy Dialogue was an attempt by both sides to create a framework for formalized discussions on energy-related subjects. Over the years the dialogue covered Russia's regulatory framework, energy efficiency, technology transfer and investments. Its roots in the post-Soviet era are traced to June 2000 with the Feira European Council Summit, the significance of which committed the EU to support Russia in its energy development and, in effect, gave Moscow a relative free hand within its sphere of influence [42].

Despite the Dialogue and other cooperative mechanisms, the two sides share fundamentally opposite perspectives on the energy trade, and there is little hope of reconciling these differences in the near term. For the EU the impetus is on competition and free trade utilizing the Commission to break down barriers to entry and unbundle the energy markets for the purpose of providing low cost and best value to the consumer. This contrasts with Russia's desire to implement firm state control and monopolistic conditions and use the power of the state to close off competition. Furthermore, it can be argued from the Russian standpoint, the Russian consumer benefits from cheap, subsidized gas. These competing models demonstrates an interesting example of executive power at play to create opposite goals; the EU notion that liberalized markets create the best options for consumers and promote transparency which, in turn, generate capital flows, whereas the Russian goal of central control, though inefficient and prone to opaque management practices, permits the best opportunities for state control of the markets.

There had long been unease in Brussels over its growing dependence on Russian energy, though, it was impossible to get Union-wide consensus on how to address it. The gas disputes of 2006 and 2009 caused trepidation within the EU about how reliable a partner Russia would be. There was resentment on the part of the EU that Russia did not re-calculate the gas prices which were indexed to the price of oil during the 2008 price spike which saw ever increasing revenues flowing to Gazprom's coffers [43]. Though Gazprom did provide rebates, it was only after EU complaints of Russia's excessive rent-seeking. It was later claimed, "This is not how partners are supposed to behave towards each other". Nevertheless, and with Russia's continued unfair trade practices, the EU was still willing to compromise with Russia. The key event was Crimea, which was considered "too much", and which forced a reconsideration of the EU's relationship with Putin's Russia [43].

Indeed, pre-Ukraine War U.S. and EU sanctions imposed on Russian government officials and business concerns because of the Kremlin's bellicose actions in its near-abroad are having an impact. The result is that Brussels is now pursuing energy diversification by looking more seriously at North African and Central Asian gas, as well as LNG sources outside of the Russian pipeline network. Russia, because of its conflicts and contracting demand in the West, is also anxious to diversify its client base. Asian demand is shifting the global economic focus, though it will be some time and considerable expense before Russia has developed an Eastward-oriented infrastructure.

Putin actions in Ukraine and the Baltic in 2022 have demonstrated his determination to stop the Western realignment, claw back lost territory and assert Moscow's domination over its former empire by controlled energy access and manipulation. It is also designed to send a message to those states dependent on Russian hydrocarbons. Central to this dynamic is Russian willingness to use energy as a coercive tool and a function of state power, which are currently on display.

A.2 NATO, ENERGY SECURITY AND OPERATIONAL ENERGY

A.2.1 NATO, Energy Security and Operational Energy

A.2.1.1 Introduction

As noted in the Lisbon Treaty, energy security is a member state function, whereby its acquisition, storage and distribution are primarily conducted by the private sector based on domestic requirements [44]. Furthermore, member state energy security is predominantly an economic consideration, not necessarily military one, and is generally not viewed as a collective security responsibility. In fact, attempts to usurp this sovereign responsibility are viewed with suspicion or concern. Therefore, the politicization of the energy sector, whereby fossil fuels and energy sector activities are jealously guarded by the member states, is evidenced by the EU's own mixed results liberalizing the energy markets as manifest by the challenge of getting member states to work collectively. NATO's energy security and operational energy viability are dependent on EU dictates and the broader civilian infrastructure, which exists outside the direct control of Alliance logistical considerations. Ultimately, emphasis on the importance of civilian infrastructure to the energy security and operational energy dynamic is key, and NATO logistics must work within this reality.

This is particularly relevant in a sector so closely guarded as a national security asset and tied to domestic political patronage, resulting in energy as a securitized commodity. Nevertheless, in 2008 NATO stated its commitment to "first and foremost ensuring a steady supply of fuel to its military forces" [45]. Despite this statement, and the fact that Alliance military operations are so heavily dependent on the availability of energy supplies, as far as can be determined. NATO does not have a working definition of energy security. Instead, every NATO member state uses its own definition of energy security. In the United States the Fiscal Year 2018 National Defence Authorization Act for defines the terms energy security for the DoD as "having assured access to reliable supplies of energy and the ability to protect and deliver sufficient energy to meet mission essential requirements" [46].

As NATO is foremost a defensive military organization, so it is instructive to consider the essential military applications of energy, or operational energy. Energy security takes on a broader strategic-political connotation, where operational energy, as the name implies, has an operational or tactical application. As with the term energy security, operational energy is vague and loosely defined with multiple meanings under a variety of conditions. Nevertheless, as operational energy is critical to NATO's warfighting mission, a generally accepted terminology is important, particularly regarding this analysis. What becomes important to recognize is that military operational energy becomes a subset of the broader energy security dialogue, and its acquisition, safeguarding and the means of its distribution to military forces must be addressed.

As defined in US law, operational energy is the "energy required for training, moving, and sustaining military forces and weapons platforms for military operations" [47]. This term includes energy used by tactical power systems and generators, as well as by weapons platforms themselves. DoD considers operational energy to be the energy used in military operations, in direct support of military operations, and in training that supports unit readiness for military operations, to include the energy used at non-enduring locations. Traditionally, the scope of operational energy excludes nuclear energy, as well as the energy used for military space launch and operations. This was outlined in in the 2009 Duncan Hunter NDAA, which sought to combine operations and logistics or operational energy, with the creation of Operational Energy Plans and Program (OEPP).

A.2.1.2 Energy Security, Operational Energy and NATO

When viewing the phenomenon of energy security, and more specifically, operational energy, from a 2022 perspective, one might get the impression these have only recently been in the collective NATO mindset has gelled since 2009. In fact, the Alliance has long experience in this field, notably in a military logistics context, as well as a broader geo-political one.

As a military organization NATO has always planned for logistics in liquid fuels as the prime component of operational energy. NATO's relationship with energy security as a function of logistics began to change in the post-Cold War era, notably the momentous period between 1991 through 1999. This also shifted as environmental considerations moved to the front of political and societal discourse, prompting interest in fuel efficiency and demand reduction. It was during this period that natural gas became a readily accepted cleaner alternative to oil or coal. Due to the shift in energy security awareness, this topic has been addressed over the years in key strategic documents, primarily in the Strategic Concepts; a barometer of NATO's political and military posture and thinking. For example, in NATO's 1968 Strategic Concept, the term 'logistics' was mentioned throughout the document, though there were no references to energy security or operational energy.

The Soviet Union's pending collapse in the early 1990s precipitated significant geo-political change throughout Europe, which was reflected in NATO's 1991 Strategic Concept. Memories of Moscow's attempt to coerce the Baltic States from leaving the Soviet Union by withholding energy supplies were still fresh. Article 12 states: "…Alliance security interests can be affected by other risks of a wider nature, including acts of terrorism, sabotage and organized crime, and by the *disruption of the flow of vital resources*" [48].

The 1999 Strategic Concept, as noted in Article 24, in which the phrase regarding 'vital resources,' was taken verbatim from the 1991 document [49]. Yet, the early 21st Century ushered in geo-political changes, notably 9/11 and the economic rise of China and India, which put pressure on the global oil supply, causing dramatic price fluctuations. Furthermore, increasing environmental concerns placed political pressure on member states to shift to low-carbon energy solutions.

The January – June 2004 gas dispute between Russia and Belarus caused Germany only minor disruptions, attributable to the fact that most of its gas imports at the time came from Ukraine. Poland, on the other hand, which was supplied predominantly through Belarusian pipelines, suffered major shortages. A consequence of this dispute forced NATO to focus on supplier countries, to understand their complex energy geopolitics and to forge better ties with them. At the NATO Summit in Istanbul in June 2004, the member states agreed to focus on the Southern Caucasus and Central Asia, where a Special Representative was appointed for both regions. The January 2006 Russia-Ukraine dispute, in which Gazprom reduced the flow of natural gas through its Ukrainian pipelines and impacted its downstream customers, caused a serious re-evaluation in the Alliance. NATO began to address energy security in a more structured manner, and at the 2006 Riga Summit, the Allies mentioned the necessity of defining a role for NATO regarding energy security. Article 45 of the Riga communique highlighted Alliance energy security interests, notably the need to "…assess risks to energy infrastructures and to promote energy infrastructure security," and it was also stated "…we direct the Council in Permanent Session to consult on the most immediate risks in the field of energy security" [50].

The 2008 Bucharest Summit outlined more clearly NATO's role in energy security, notably the exchange of information, promoting international and regional cooperation, supporting the protection of the critical infrastructure, and managing the consequences of a possible crisis. In Article 48, it was noted in a report, "NATO's Role in Energy Security," the Alliance will engage in "…supporting the protection of critical energy infrastructure," and will "… consult on the most immediate risks in the field of energy security" [51].

Following the Chicago Summit of 2012, there was an emphasis on operational energy; "we will work towards significantly improving the energy efficiency of our military forces." Also, at Chicago NATO proposed itself as a facilitator to enhance interoperability, whereby the Emerging Security Challenges Division (ESCD) created the Smart Energy Teams (SENT), a group of experts from six Allied and two partner countries, tasked to identify the best existing 'smart energy' solutions. SENT is funded by the Science for Peace and Security (SPS) Program and plays the role of a steering group for the period 2012 – 2014" [52].

The 2014 NATO Summit in Wales pledged stronger cooperation with Central Asia and the Southern Caucasus. The Wales Declaration noted:

> *We will [...] continue to work towards significantly improving the energy efficiency of our military forces, and in this regard, we note the Green Defence Framework. We will also enhance training and education efforts, continue to engage with partner countries, on a case-by-case basis, and consult with relevant international organizations, including the EU, as appropriate.* [53]

The 2016 Warsaw Summit's Article 135 built on Chicago's statement by ensuring, "…resilience against energy supply disruptions…" and "…include energy security considerations in training, exercises, and advance planning." Additionally, in the Warsaw Summit Declaration, the Alliance stated perhaps the most comprehensive description of energy security in a NATO document:

> *Energy developments can have significant political and security implications for Allies and the Alliance, as demonstrated by the crises to NATO's east and south. A stable and reliable energy supply, the diversification of import routes, suppliers and energy resources, and the interconnectivity of energy networks are of critical importance and increase our resilience against political and economic pressure. While these issues are primarily the responsibility of national governments and other international organizations, NATO closely follows the security implications of relevant energy developments and attaches importance to diversification of energy supply in the Euro-Atlantic region. We will therefore further enhance our strategic awareness in this regard, including through sharing intelligence and through expanding our links with other international organizations such as the International Energy Agency and the EU, as appropriate. We will consult and share information on energy security issues of concern to Allies and the Alliance, with a view to providing a comprehensive picture of the evolving energy landscape, concentrating on areas where NATO can add value. We will also continue to develop NATO's capacity to support national authorities in protecting critical infrastructure, as well as enhancing*

> *their resilience against energy supply disruptions that could affect national and collective defence, including hybrid and cyber threats. In this context, we will include energy security considerations in training, exercises, and advance planning. … We will further improve the energy efficiency of our military forces through establishing common standards, reducing dependence on fossil fuels, and demonstrating energy-efficient solutions for the military. … We task the Council to further refine NATO's role in accordance with established principles and guidelines, and to produce a progress report for our next Summit.* [54]

The 2018 NATO Summit Declaration noted, "We will also further improve the energy efficiency of our military forces, including through the use of sustainable energy sources, when appropriate" (Extract from paragraph 78) [55]. Finally, Article 26, of the new (2022) Strategic Concept, notes, "We will enhance our energy security and invest in a stable and reliable energy supply, suppliers and sources" [56].

A.2.1.3 NATO Energy-Focused Organizations

As NATO became more responsive to post-Cold War energy security concerns, there was a move to create supporting organizational structures. This precedent has produced two important organizations within the Alliance.

A.2.1.4 Hybrid Challenges and Energy Security Section

NATO's Hybrid Challenges and Energy Security Section is in Brussels and falls under the Emerging Security Challenges Division. Established in 2010 and originally called the Energy Security Section, it had a recent name change to incorporate the growing hybrid threat. Headed by Michael Ruhle, the section operates across multiple functions within NATO headquarters and the European Union and member states. It is heavily engaged with the NATO Energy Security COE in Vilnius, the Cyber COE in Tallinn, as well as the European Commission's Hybrid Threats COE in Helsinki.

A.2.1.5 NATO Energy Security COE

The NATO Energy Security Centre of Excellence (NATO ENSEC COE) was accredited by NATO in October 2012 and is composed of military and civilian experts from NATO and Partner Nations. The steering committee guides the activities of the Centre through an annually approved Programme of Work coordinated with NATO Allied Command Transformation (ACT). The largest contribution comes from Lithuania as a Framework Nation filling in the positions of a director, experts, and administrative staff. Sponsoring Nations provide 1-2 representatives and fill positions of Deputy Director, Heads of Divisions, and experts.

A.2.2 NATO and Operational Energy in a 21st Century Context

A.2.2.1 Interoperability/Capability Gap

Interoperability has been a goal since NATO's inception, forces, units and/or systems to operate together and share common doctrine and procedures. This includes infrastructure, communications, and facilities, yet the ability to operate seamlessly between militaries remains key to overall effectiveness. The Alliance defines interoperability as the '*ability for Allies to act together coherently, effectively and efficiently to achieve tactical, operational and strategic objectives*' [57].

After the Cold War, interoperability became more complicated as Western and Eastern European nations began to standardize equipment, coalesce doctrine and conduct joint training. Today the premise is that all Alliance members are vulnerable. The capability gap today involves the ability to coordinate across international or regional 'peer' entities with the same interests yet without an agreed framework; harbor competing agendas to achieve it.

NATO's fuel-sharing protocols are among the best-established of all the supply classes. For, example, there are 10 Standardization Agreements (STANAGS), seven Allied Fuel Logistics Publications (AFLP), and nine Defence and European Union Standards (DEU) related to fuel [58][1]. From the end of the Cold War to the Balkan Wars and the now defunct mission in Afghanistan [59], NATO's resilience in meeting large-scale fuel requirements demonstrate both a united resilience and a sense of organizational dexterity.

Part of this is due to the professional fora and exchanges where protocols are adopted for the purchase or barter of fuel. NATO's AJP-4, for example, is an all-encompassing mandate that fuel is to be forecasted, transported, and stockpiled for potential or ongoing operations [60]. The Operational Logistics Support Partnership (OLSP) is a 25-nation multifunctional partnership established in 2009 [59]. Another example is the annual Fuel Exchange Forum, hosted by the US Defence Logistics Agency's Energy Services Office. DLA Energy, as it is known, has 41 fuel agreements around the world [61]. Through the US European Command (EUCOM), Acquisition and Cross-Servicing Agreements (ACSA) are executed for the provision of fuel throughout the alliance [62].

Beyond the 13 states maintaining the NATO Pipeline System (NPS), there are no pipelines meeting the Alliance's fuel requirements in Central and Eastern Europe. The result is a regional 'fuel desert' where potential operations require extended lines of supply. Although these pipelines were configured under Cold War-era geo-political conditions, the clusters in Western Europe or Turkey did not account for the Alliance's eastward expansion. The challenge today is whether the ability to expand the NPS into Eastern European member states is possible considering the vulnerability of local infrastructure to the hybrid threat, ongoing environmental concerns and potential destabilizing events.

A.2.2.2 Anti-Access/Area Denial (A2/AD)

Modern conventional weapons, notably long-range air, artillery or missiles can deny or limit access to a battlespace and reduce operational effectiveness and unit cohesion. Kinetic disruption of military assets and operational energy stores, either by destroying supplies or rendering it unavailable to units, is an aspect of conventional warfare that must be addressed when considering a 'hybrid' attack on an allied nation.

Anti-Access/Area Denial (A2/AD) is the ability to prevent an adversary from deploying and operating its forces in a certain territory or geographic region, thereby prohibiting or inhibiting permanent control over geographic and operational interests. Such a denial would potentially cause an Alliance failure in both maintaining internal cohesion and in deterring potential geo-political competitors. For this reason, A2/AD deserves to be studied not only through a political and military lens but also in a wider OE context, namely its potential to deny NATO commanders the freedom of action to protect and defend the Alliance's areas of interest.

In January 2018, the National Defence Strategy (NDS) emphasized the re-emergence of long-term strategic competition, rapid dispersion of technologies, and new concepts of warfare and competition that span the spectrum of conflict, all of which require a Joint Force structured to match this reality. The NDS focus on peer competition gave renewed impetus to the trans-Atlantic Alliance and 'Russian adventurism.' NATO member states have responded to recent Russian activities in Eastern Europe, notably Crimea and Ukraine, in the form of sanctions and increased emphasis on training and readiness. Much of which is highlighted by the US-sponsored Operation Atlantic Resolve (OAR) and the European Deterrence Initiative (EDI).

A.2.2.3 Operational Energy Capabilities and Challenges in the USEUCOM AOR

It should be recognized that any resolution to NATO OE challenges must include a US component; the US provides the bulk of logistic support and administration. A key theme highlighted in the NDS and EDI is the

[1] STANAGS: 1135, 3149, 3609, 3681, 3682, 3756, 3967, 4712, 6001, 7102 AFLP: 7, 1110, 3682, 3747, 4712, 7029, 7090. DEU: 91-091, 91-87, 91-090, MIL-STD-3004D, MIL-DTL-83133, EN228, EN590, EU REACH and ADR Regulations.

necessity to enhance mobility in military operations, particularly under an A2/AD environment. The NDS summary identifies ‘resilient and agile logistics’ as a component to a modern warfighting posture. More specifically, the NDS notes that:

> *Investments will prioritize prepositioned forward stocks and munitions, strategic mobility assets, partner and allied support, as well as non-commercially dependent distributed logistics, and maintenance to ensure logistics sustainment while under persistent multi-domain attack.* [63]

Therefore, the acquisition and distribution of energy, primarily liquid fuels as a critical component to operational energy, takes on a significant role in the NDS framework and within NATO.

Regarding the challenges, there is concern among civilian and military leaders that the flow of liquid fuels cannot adequately support the mission, particularly at forward deployed units on Europe’s eastern periphery. Moreover, as noted, the ‘fuel desert’ has the potential to complicate fuel delivery to forward these deployed forces. The geo-political and economic trends which include the long-term effect of European and NATO reliance on Russian energy, highlights the greater need for allied and partner mitigation efforts or even develop new sources.

Although there are constrained budgets for all members of the Alliance, cross-servicing agreements that facilitate bartering can be accomplished in many ways. Under emergency conditions, it can be done bi-laterally with EUCOM and treated as a de facto NATO agreement [64]. If there is time for more deliberate planning, NATO’s Host Nation Support (HNS) is possible based on the guidelines provided by MC 319 and Chapter 2 of the NATO Logistics Handbook [65]. Examples include identified property for landing zones, airstrips, warehouses as well as transportation nodes such as railway stations, docks, and aircraft hangers. Moreover, there is ample opportunity to integrate local infrastructure and private enterprise into a general defence plan.

This, however, raises a different issue. A half-century of planning and preparation in Western Europe has taught the Alliance that populations become displaced when confronted with advancing military formations. The impact this has on any potential agreement is that local assets must prioritize the movement of people away from the conflict, while allowing the Alliance to move towards the point of contact. This goes beyond the scope of a military-to-military agreement. Not fully accounting for the inclusion of Civil-Military Cooperation (CIMIC), national police, IOs and NGOs to name a few, will leave room for fuel shortages hybrid threats. Finally, there is potential competition for energy between EUCOM and the member states’ military and civilian requirements.

From a EUCOM perspective, it is imperative to sustain power projection throughout the AOR as dictated by our national interests. Quite often this presence must be (and will be in the future battlespace) sustained in a contested environment, across the domains and Combatant Commands. Large naval force concentrations as utilized in the past may no longer be an option against near-peer competitors capable of implementing effective A2/AD. The response is distributed operations which leverages an integrated solution that is more dispersed by shifting from large concentrations in favor of smaller assemblies, which are highly mobile and capable of delivering distributed lethality across an expansive battlespace.

This requires the warfighter and supporting organizations to gain and maintain the advantage in distributed operations in contested environments. More specifically, it leverages asymmetric warfare, and challenge the force to expand the warfare and cyber warfare. Ultimately, a force that is mobile, stealthy and lethal, and is relatively easy to sustain.

Advances in warfighting technologies and their battlespace applications can inflict devastating kinetic and non-kinetic effects against US and allied forces across the domains in all theatres and ultimately inhibit US and allied freedom of action. This ability to deny access to geographic space and disrupt operational coherence through a layered and integrated application of long-range fires, air interdiction and air defence, or A2/AD, presents a host of challenges unknown to the current generation of US leaders. Operating distances once considered safe from enemy interdiction, are now in play, requiring a re-evaluation of force posture, whereby strategies based on massed concentrations are in question.

Inherent in this strategy is the necessity for distributed operations in the battlespace, primarily to ensure mission success against peer competitors under a robust A2/AD environment. For instance, U.S. and allied forces to fight and survive in the 21st Century contested battlespace will require greater distribution of forward deployed assets with higher degrees of operational and logistical autonomy. Key to success and survivability in this new distributed environment is greater mobility and highly lethal offensive/defensive power projection, available across all domains. This is essentially, the age-old concept of 'move, shoot and communicate,' but at greater distances and at a higher tempo than seen in previous generations.

A.2.2.4 Defence Fuel Supply Points (DFSP)

A key element to EUCOM's (and NATO's) ability to manage strategic distribution of liquid fuels is the Defence Fuel Supply Point (DFSP) system. The DFSP is a system of regional distribution nodes, bulk storage and transfer terminal, ship ports, and inter-state pipeline and railroad terminals, which support the land, sea and air elements, contingency basing, and host nation energy infrastructure. The NPS and DFSPs are closely interrelated, and their laydown is based on the legacy Cold War-era geo-political configuration. When we consider the resilience of the bulk fuel supply chain from the source of production to the DFSP, there is a concern with the viability of the operational energy supply chain, particularly as it relates to our European partners.

The DFSPs are a vestige of the Cold War, and a large footprint leaves them susceptible to a host of kinetic and non-kinetic attacks. There is also the need to address fuel flows from the DFSP to where the fuel is consumed, at the maneuver element in support of the mission. What are the current volumes, sources, and distribution methods for bulk fuel used in peacetime? Finally, NATO logistics planners may need to rethink the efficacy of the 'hub and spoke' logistics principle under the A2/AD arc, which will require a distributed approach to OE management and delivery.

A.2.2.5 NATO Energy Security/Operational Energy Conclusions

Since the Cold War there has been a clear shift toward a greater awareness of energy security and the value of operational energy. NATO recognizes its role as a common platform to examine and implement change, in both military and political contexts. The Alliance must tread a fine line; on the one hand a determination to respect national sovereignty, while enhancing military readiness on the other. One of the most critical hurdles is NATO member state requirements. As the three (US/NATO/EU) are inextricably linked, greater cooperation in energy security and operational energy is necessary.

Reducing demand and/or deriving new sources for energy on the battlefield is a key task for NATO, with the benefit of extending operational reach and permitting a more effective rotational presence; factors which becomes even more relevant under the conditions seen on the US EUCOM's eastern periphery. Other options are to rely on host nation power, where feasible, which will give Commanders more alternatives and operational flexibility.

There are four focal areas to consider when recommending logistical transformation in a country considered within the 'fuel desert' [66]:

- The redistribution of roles and missions between Ministries of Defence and General Staffs; emphasizing how to buy versus what to buy.
- Departure from the centrally managed depot mindset to one where commanders provide a needs-based assessment that feeds into national defence policy.

- Take into consideration deployed maneuver forces. State-owned enterprises bleed defence budgets, rarely deliver on operational requirements and lack oversight for potential corruption.
- Decentralize decision making to commanders on budgets, resources, and potential areas of outsourcing.

For operational energy planning, command and component staffs are hindered in the performance of OPLAN supportability analyses, as there is a lack of a framework for assessing the resilience of host nation energy infrastructure. They are unable to verify steady-state resilience and calculate the infrastructure's ability to support surge requirements. They lack a framework for assessing the proposed scheme of movement and maneuver as well as the supporting Ground Lines of Communications (GLOC).

The Alliance's energy considerations are absent or unclear. Analyses of the NATO Pipeline System, notably CEPS, is good, though there is relatively little understanding of non-NATO pipelines, to include crude, refined or natural gas pipelines. However, this gap may be addressed in the NATO Petroleum Committees and NATO ENSEC COE development of a cybersecurity guide for the NPS, and other energy installations as noted earlier. There is also a need to explore OE planning tools [resilience measurement] developed by EUCOM or NATO and determine how these tools could be leveraged and shared. The goal of any resilience assessment is to determine weaknesses and highlight areas in need of investment.

What is unclear in the spectrum of analyses is whether there is a need to assess fuel flows by type and specification to the tactical unit. Gaps exist in upstream issues, such as crude production and procurement. Admittedly, this is mainly focused on liquid fuels, though there may be a need to incorporate coal and natural gas into the broader analysis. There is a need for close operational planning coordination between EUCOM, NATO, and the host nation energy requirements necessitates an assessment of resilience under steady-state or normal operations, as well as the ability to handle surge or degraded conditions. The value of distributed logistics as a countermeasure to enhancing flexibility and reduce the overall operational footprint. As an integrated part of NATO, the supply chain and the broader host nation infrastructure to support operational requirements in the USEUCOM AOR. More specifically, to make informed investment decisions to mitigate risk, support force structure development at the strategic level, or targeted investments at the operational level.

The need for trends analysis, to include the long-term effect of European and NATO reliance on Russian energy, all of which highlights the need for allied or partner efforts to diversify sources. The ability to provide clean and continuous power to the war fighter is another vital consideration when analyzing OE vulnerabilities in the region. Reducing demand for energy on the battlefield is a challenge for the DoD, with the goal of extending operational reach and permitting a more effective rotational presence; Other options are to rely on host nation power, where feasible, which will give Commanders more alternatives and operational flexibility.

Space must also be given to the resilience of the European power grid. Indeed, considering the dual-purpose energy infrastructure, both civilian and military applications, its security cannot be minimized. As with the fuels infrastructure, the electricity infrastructure is also vulnerable to the variety of cyber threats, as noted in the SAS-163 Cyber report.

A.3 NATO, ENERGY SECURITY AND OPERATIONAL ENERGY

A.3.1 Hybrid-Energy Warfare Challenges to NATO Operational Success

A.3.1.1 Introduction

This section consolidates the analytic threads within the NATO energy security dynamic. It clarifies what hybrid warfare is and its potential effect on energy security and the consequential impact on the NATO mission. The ability to leverage technology for geo-political gain against an adversary's vulnerabilities, broadly referred to as hybrid warfare, has become increasingly prevalent in the 21st Century. Hybrid warfare has multiple synonyms, such as "grey zone warfare/strategies" [67], "competition short of conflict" [68], "active measures" [69], and "new generation warfare" [70]. Allied Joint Pub 01 (AJP-01), notes, "Hybrid threats occur where conventional, irregular and asymmetric threats are combined in the same time and space" [71]. The International Institute for Strategic Studies (IISS) defines hybrid warfare as: "The use of military and non-military tools in an integrated campaign designed to achieve surprise, seize the initiative and gain psychological as well as physical advantages utilizing diplomatic means; sophisticated and rapid information, electronic and cyber operations; covert and occasionally overt military and intelligence action; and economic pressure" [72].

Despite differences in terminology, these definitions point to the same fundamentals; in its most basic context, hybrid warfare's genesis can be traced to the age-old principle of asymmetrically exploiting an adversary's weaknesses, with clear 21st Century attributes. This is done by using or 'misusing' capabilities meant to serve the public at-large – either through the commodities it consumes in everyday life or the public goods and services by which everyone carries out their daily affairs. The project's focus on energy security is rooted in the pretext that it is fundamentally the most vulnerable sector and possesses the largest potential to destabilize a society. Yet, what does this mean in a practical sense? How can NATO and the member states develop actionable policies and countermeasures? Moreover, from an energy security perspective, this study's primary focus, how can we protect the infrastructure and recover from attacks against this most vital of sectors? Although sovereign nations maintain responsibility for the integrity and defence of their energy infrastructure, NATO operations will require a unified response and a resilient international energy supply coordinated with alliance, European Union, and national objectives.

Acknowledging that NATO has a role at the forefront of the confluence of energy security, cyber security and hybrid warfare; yet these combined threats pose a direct challenge to the Alliance and its members. Within the context of NATO energy security, hybrid threats can be identified as actions by state or non-state actors aimed to undermine or harm NATO's assured access to affordable and acceptable supplies of energy and the ability to protect and deliver sufficient energy to meet mission essential requirements by influencing its decision making at the local, regional, state or institutional level.

Additionally, we need to keep in mind the two main components of the hybrid warfare and energy security dynamic is cyber defence and malign influence. NATO has maintained a constant though evolving role in addressing cyber as a hybrid threat to the Critical Energy Infrastructure (CEI) of its member states. Over the past two decades, cyber-attacks against Industrial Control Systems (ICS) of NATO member states' energy supply chains have grown exponentially.

A.3.1.2 Russian Contribution to Hybrid Warfare Doctrine Development

Since the end of the Cold War, EU and NATO expansion in the former Eastern Bloc has created consternation in the Kremlin, resulting in a hybrid-influenced pushback. Realizing it is unable to compete with NATO on an economic or conventional military footing, the Kremlin must rely on asymmetrical responses to what it feels is Western encroachment. Russia already utilizes an array of hybrid tactics against NATO members and partner countries. Most importantly, as Russia is not interested in provoking the Alliance, these actions must fall below the Article 5 threshold, includes the use of kinetic and non-kinetic tools, to pursue its national interests. Ultimately, the key is to blur this line of inter-state conflict, which allows plausible deniability in meeting the Kremlin's goals. The Kremlin has successfully implemented political and economic leverage, combined with disinformation, against it neighbors to undermine these countries. Even before February 2022, Ukraine received the brunt of these attacks.

As a main practitioner of hybrid warfare, it is imperative to delve into Russia's contribution to hybrid warfare. It can be affirmed that Russia has a long history in asymmetrical warfare, well before the

21st century. During the Cold War the Soviets emphasized "active measures" to influence the European political landscape, notably through supporting leftist political parties, and disinformation efforts that included propaganda and espionage. While these efforts resulted in mixed success, some relatively sophisticated measures employed during the Cold War are still used today.

Arguably, Russia's emphasis on hybrid warfare stems from General Valeri Gerasimov's 2013 article, 'The Value of Science is in the Foresight,' in which he states: "In the 21st century, we have seen a tendency toward blurring the lines between the states of war and peace. Wars are no longer declared, and having begun, proceed according to an unfamiliar template" [73]. This can be called 21st Century warfare with a uniquely Russian imprimatur.

It is important to understand Russia's perception of the threats arrayed against it, which allows for a better NATO response. Activities on Russia's border, notably NATO expansion and the 'color' revolutions in Georgia in 2003 and Ukraine in 2004, have been viewed as intolerable provocations by the West. Realizing it is unable to meet NATO on an economic or purely conventional footing, the Kremlin must rely on asymmetrical responses and, most importantly, actions that fall below the Article 5 threshold. Russia has taken many tactics from the Cold War and infused them with 21st Century technology. For Russia, a "hybrid warfare" solution is needed to advance its national interests, by weakening NATO and the EU, as well as pro-Western governments. This also includes shaping the environment for future conflict; to dominate territory and penetrate European markets [74]. This model has already been successfully employed in the so-called "frozen conflicts" of Ukraine and Georgia to thwart interaction or integration with Western Europe.

Perhaps Gerasimov's reference to 'blurring' this line allows plausible deniability in meeting the Kremlin's goals. In his 2017 Congressional testimony, Christopher Chivvis of the Rand Corporation outlines Russia's broad hybrid warfare goals or objectives.

These goals can be broadly identified:

1) Controlling territory: Russia used similar tactics prior to the 2008 invasion of Georgia, though the most infamous example is the virtually bloodless occupation and annexation of Crimea in 2014.
2) Shape the geo-political environment and the operational battlespace by fomenting discord between the native and minority Russian populations. The Kremlin creates the narrative that portrays the government as repressive, justifying intervention.
3) Undermine Western or pro-Western governments, whereby the Kremlin has utilized a 'divide and conquer' approach to keep competitors off-balance and uncoordinated.

This continual effort to erode stability and changing the intensity of conflict by maintaining fluidity between kinetic and non-kinetic actions. To maintain this constant level of tension, the Russian Foreign Policy Concept openly states Moscow will develop "…its own effective ways to influence foreign audiences" by using information and communication technologies [75].

Hybrid Warfare is accomplished through two primary and interrelated methods; cyber domain and malign influence.

A.3.1.3 Cyber Domain

The 2016 Russian Information Security Doctrine recognized the importance of cyberspace, whereby the Kremlin is determined to control this domain by increasing internet oversight and "eliminating the dependence of domestic industries on foreign information technologies and information security means by creating, developing and widely implementing Russian solutions, as well as producing goods and providing services based on such solutions" [75] (see Article 25, Section b). For a more detailed description of the cyber realm in the broader hybrid warfare-energy security dynamic, see the Cyber section within this report.

Additionally, big data analytics and artificial intelligence-assisted tools provide information weaponization, designed to influence public opinion. Finally, cyber exists as a component of military planning and operations, notably through the creation of cybersecurity units within the armed forces [76].

A.3.1.4 Malign Influence

The manipulation of strategic communications to shape political narratives is not a new phenomenon and was used extensively during the Cold War. More recently, Kremlin-sponsored media, such as Russia Today (RT) or Sputnik, both of which are available in multiple languages, allows the spread of disinformation campaigns against the West [77]. Russia also funds European think tanks, internet trolls, bots, and fake news farms. Fake media and websites exploit social fissures, which are effective and harder to detect, while artificial intelligence, deep fakes, or manipulated videos allow Moscow to effectively shape the news (see also Ref. [78]).

Moreover, special operations (little green men), to include clandestine efforts, such as bribery, extortion, and political influence, seek to undermine the EU and NATO's credibility and governance, resulting in challenges for decision making at the political level. This is especially true in organizations, such as NATO and the EU, which require consensus decision-making [77].

A.3.1.5 The Hybrid Threat to NATO's Energy Security

Interoperability/capability gap: the hybrid threat is far more fluid if not elusive to the Alliance. Each member of the Alliance addresses hybrid threats based on its own resources and human capital. The challenge for the member and the Alliance is reconciling the mix of military, law enforcement, intelligence, academic and commercial spheres of security practice that differ in each country.

A.3.1.6 Cyber as a Component of the Hybrid Threat to Energy Security

The level of cyber threats against NATO energy security is "capable of holding multiple dimensions and taking on different specificities depending on the country." In other words, each NATO member state handles cyber-attacks against their CEI using cyber capabilities that vary from state to state. Furthermore, both NATO and the European Union are developing their own means and ways to respond to the growing number of cyber-attacks against both national and regional/interconnected CEI. Our purpose is to define a cyber-attack as "an attack on a computer and network system, consisting of computer actions (e.g., remote or local connection, computer file access, program execution, etc.)" to compromise the secure operation of "automated systems for storing, processing, and distributing information" and "computer-controlled physical processes such as industrial control systems or other types of control systems."

A cyber-attack against IT and OT components of the CEI represents a cheap and impactful manifestation of hybrid threats to the energy security of NATO member states. As early as December of 2002, "hackers were able to penetrate the SCADA system responsible for tanker loading at a marine terminal in eastern Venezuela, [preventing] tanker loading for eight hours." Energy can influence foreign policy, the most notorious examples being the Russia-Ukraine gas disputes in the winters of 2006 and 2009, which impacted politics and economics of many NATO members.

Having established a general awareness of Russian hybrid warfare activities, we must now consider the hybrid warfare and energy security implications. Russia's energy supply can be used as a 'carrot' or a 'stick,' this is most recently seen in the construction of the Nord Stream II gas pipeline project, the undersea natural gas pipeline from Vyborg, Russia to Greifswald, Germany bypasses the traditional transit countries of Ukraine. An attempt to influence the Eastern European nations while supplying energy to Western Europe.

Cyber threats to the interconnected liquid fuel supply chains and grids that support NATO operations have the capacity to directly impact the NATO mission, highlighting the need for unified civil-military responses in the cyber domain. Vulnerable energy systems range from the refinery, bulk transport, storage, transit, and delivery of fuels that are critical for forward deployed units, to the electrical grids that power NATO members' critical energy infrastructure. These energy systems can be attacked through any number of vectors with devastating results to Alliance military effectiveness and could negatively impact mission success; this highlights the importance of these energy systems as critical components across all aspects of the battlespace. Any impediment to NATO infrastructure and forward deployed units accessing affordable and acceptable energy supplies via power grids, pipeline, road, rail, air, or water transport, will inhibit NATO's ability to operate seamlessly across the five domains (land, sea, air, space and cyber) and will severely undermine interoperability among the NATO allies.

On land, tanks and artillery can occupy positions. Ships can anchor at sea or at port. For the air domain however, nothing happens without fuel. Any hybrid threat actor who has studied NATO would focus on the Wales Summit Declaration. At this forum, NATO's Heads of State concluded that a cyber-attack would meet the criteria of Article 5 only on a 'case-by-case' basis. In addition to no shared applicability of Article 5 [79]. The same could be said of force majeure; a legal term that grants a member state considerable license [80] to divert fuel to support a NATO action. Short of Article 5, there is no uniform legal justification to support a NATO action at the expense of domestic commercial activities however sympathetic a national government may be.

A.3.1.7 Malign Influence and Energy

While we are still evaluating the lessons from the current war in Ukraine, it can be determined that Russia's hybrid warfare efforts have had mixed results. There has been no reported large-scale cyber-attacks and any malign influence campaigns have been unsuccessful. This early assessment merely reinforces the notion that hybrid warfare tactics directed against a defender's energy sector could have damaging consequences, though mostly relegated to the local or operational level. Therefore, a well-prepared and vigilant defender can detect, defeat or recover from most hybrid threats directed against the energy infrastructure. The goal must be to deter or mitigate the impacts. Moreover, recognizing that from a military operational perspective, hybrid warfare attacks can be deployed across all five domains.

A.3.1.8 NATO Mitigation Tools

How has/will NATO addressed the hybrid warfare-energy security threat?

The Alliance has pushed forward on the topic, such as at Wales, creating cyber defence organizations and coordinating studies and analyses, essentially developing greater resilience among the member states. However, NATO is hamstrung by limitations inherent within its structure, whereby sovereign member states will ultimately do what is in their own best interests, which is often at odds with NATO's goals. Moreover, many member states are reluctance to share intelligence or technologies, creating an atmosphere of mistrust within the Alliance.

Russia's assault on Ukraine in early 2022 has led to the biggest re-evaluation of NATO's collective defence for a generation, requiring broad-based improvements in capabilities and interoperability, particularly regarding energy security.

Mitigation efforts require a whole government approach, to include the intelligence community, which will provide the basis of sober analysis, while developing and implementing an effective strategy and consensus.

It is also essential to promote greater transparency and anticorruption efforts. Institution-building can help to sustain and strengthen core elements of the NATO mission, whilst simultaneously weaken and render legacy ties with Russian security services unnecessary. This will enable member nations to detect and resist covert Russian operations. Strengthening good governance and the rule of law will also complicate Moscow's hybrid efforts. Nations must respond to Russian influence operations by discrediting sources whenever they appear. Civil society must also be encouraged to play a larger role in combatting Russian disinformation, which can be accomplished by promoting positive information and possibly halt access to Russian media outlets as needed.

Greater support for European efforts to combat Russian hybrid warfare are critical. Reliance on the front-line defence of NATO and/or EU member states is no longer sufficient, and other member nations must be brought up to speed both in terms of infrastructure and organization. Stronger US interaction will not only help to achieve these aims, it is essential to do so. The authors of this report support the creation of a strategic communications task force of full-time professionals dedicated to countering Russian malign influence.

Per Chivvis, the "Russian hybrid threat is real and not going away." Though it is also important not to exaggerate the threat; Russia's GDP is approximately the size of Italy's and will be vulnerable to the fluctuating price of crude oil and Western (US) sanctions. Over the last 10-15 years heightened geo-political tensions in Eastern Europe has placed renewed emphasis on countering Russian military, political and economic threats to regional stability. Kinetic disruption would entail cruise/ballistic missile, rockets, artillery, air interdiction, sabotage, fouling, etc., while non-kinetic includes cyber-based degradation, manipulation, or disruption [74].

SAS-163 recognizes the strength of Russian security of supply and demand, and that European-Russian relations are dominated by their energy interdependence. The dependence on Russia remains a critical aspect for maintaining prosperity and the Western way of life for NATO and EU countries, as well as a national security concern for those member countries highly dependent upon a single energy source. Reducing dependence over the next two decades could also decrease Russia's ability to use these resources to coerce and influence; conversely, Russia could become more isolated and aggressive if marginalized in the energy sector.

By raising awareness of the threat in the Baltic and Black Sea states, as well as the governments of the Nordic countries, NATO helps to strengthen their defences and resilience against hybrid strategies. State security and military agencies work synergistically, with clear division of labor, to carry out offensive cyber operations. Engineering and planting deep fakes from synthetic imagery and videos to bot-operated fake social media accounts is a new trend in Russian cyber warfare operations. An upcoming concern is the potential use of AI-assisted tools for cyber operations and information warfare operations, notably regarding facial recognition software, against which the West remains poorly prepared.

A.3.2 Additional Considerations

A.3.2.1 Effects of Net-Zero Emission Goals

Short to medium-term NATO Member State energy insecurity may embolden Russian aggression. For example, as NATO member states shift toward low-carbon solutions. It should be granted that Russia will not stand idly by as a major source of revenue dries up; the Kremlin will almost certainly continue to undermine such decarbonization efforts and push traditional sources of energy, as seen with both Nord Stream 2 and Turkstream. It should be expected that during this 'bridge period' and beyond, the Kremlin will aggressively seek to protect its interests. Furthermore, this aggressive activity has already (and will continue to) entailed a variety of hybrid warfare tactics, concentrating on vulnerable NATO member or partner states' energy sectors and civil society.

A.3.2.2 China's Emergence as a Player

Until a few years ago, Russia was considered NATO's primary competitor in the hybrid warfare arena. China's actions prove that Beijing is becoming a hybrid actor. What are the Chinese hybrid warfare activities in the region including economic expansion and BRI projects, energy deals? Finally, China's interest as a function of its Belt and Road Initiative, must also be considered. What are the potential implications of Russia-China technology collaboration, such as 5G, on hybrid warfare? [81]

A.3.2.3 Thoughts for Future Contingencies

Any attempt to predict the future is fraught with challenges, though it is a necessary exercise, as it gives NATO leaders a range of possibilities to allocate investments, contemplate force posture and shift resources. Ultimately, the level of mutual mistrust will largely depend on the Kremlin's attitude toward its neighbors. However, even with a 'status quo' posture, it is safe to say the Baltic and wider Black Sea regions will continue to be a critical and contested geographic space, whereby a host of hybrid warfare tools will be employed. In the case of these regions, the potential exists for a classic example of a hybrid warfare security dilemma. At a general level, Russian hybrid tools of 2040 will be very similar to those employed in 2022; operating across military domains and economic sectors to asymmetrically challenge its opponents.

To effectively determine the future hybrid warfare threat deployed against NATO energy sector must determine:

1) How aggressively these tools could be utilized;
2) How effective they might be;
3) Technological and governance mitigations; and
4) How do Alliance and partner respond to these tools once deployed?

Therefore, any attempt to determine how aggressively Russia will employ these hybrid tools should be viewed through these lenses. Perhaps key to addressing hybrid warfare is through non-linear thinking, which entails a reappraisal on realistic goals which account for member state security and the Alliance's broader mission.

Ultimately, NATO leaders will require a proactive and adaptive response to the growing list of security challenges. With increased digitalization, threats will require a greater evaluation of cyber security risk and countermeasures. To date, hybrid protection and responses have had limited efficiency, requiring new approaches and greater adaptability to meet the evolutionary challenges, requiring new approaches to detect and prevent threats.

A.3.3 The European Union and the Demand for Energy Security

The EU's quest for a uniform energy strategy can be traced to the Rome Treaty of 1952 and the creation of the European Coal and Steel Community (ECSC), designed to control the primary war-making elements of the mid-20th century. It could then be argued that supranational energy management was the core unifying element of the EU. In this period, European economies were predominantly coal-driven, thus the importance of the ECSCand its impact. Moreover, because of their place as the foundation of state viability, coal and steel acted as catalysts for bilateral and multilateral interaction. By controlling access to commodities vital to national livelihood, member states were forced to cooperate at the highest political and economic levels. In 1957 the European Atomic Energy Community (Euratom) was founded to consolidate atomic trade and safety regulations while addressing non-proliferation issues [82], [83].

This reliance on coal diminished in the post-war years when Europe turned to oil as the primary energy resource, and as the European economic recovery began to accelerate in the 1950s and 60s, this principle of energy cohesion was largely forgotten [84] p. 24. Post-war reconstruction required increasing quantities of energy (oil and coal, initially) to feed the expanding economies, but there was no coherent energy policy at the European level; energy policies were a function of the member states. Additionally, national oil, gas and electricity entities held considerable economic and political power, erecting entry barriers and ultimately distorting market forces, resulting in uncompetitive and unrealistic consumer prices coupled with shoddy services.

The oil shocks of the 1970s highlighted the EU's vulnerability and European leaders began to consider conservation measures and source diversity to ensure security. The UK and the Netherlands exploited oil and gas reserves under the North Sea, and in 1973 West Germany began importing Soviet gas via newly installed pipelines. The USSR was a reliable partner, and in the 1980's other Western European countries, as well as Greece and Turkey, began taking deliveries [85], [86]. During this period, Eastern European nations continued to draw from segregated pipelines installed to service the Warsaw Pact nations with heavy dependence on Russian gas, oil, and atomic fuels.

A.3.3.1 The Energy Charter Treaty

By the early 1990s the EU realized that more robust provisions were needed than those found in the ECSC and its successor organizations. At the June 1990 European Council summit in Dublin, Ireland, discussion touched on broad-based liberalization and energy cooperation motivated by the political and economic changes in Eastern Europe. The Council tasked the Commission to support such interaction, and in December 1991 the European Energy Charter was proposed. Explicit in the Charter's mandate was the promotion of market-led pricing via sector competition which would in turn create energy efficiencies and sustainable development [87].

A.3.3.2 European Union Policies

As the EU's executive and enforcement body, the European Commission was best placed to craft and negotiate the Union's energy strategy. More specifically, the Commission's function was to initiate action and legislation, implement Union policies, and act as the decision-making authority on competition. Thus, the Commission has considerable power and leeway in energy-related activity, and through the Directorate-General of Energy (DG-ENER), acts as the primary force behind the EU's push in energy competition and integration [88].

The Commission's depth of intervention and influence is, arguably, unmatched in any other economic sector. Less than a year after the Energy Charter's birth, the Commission launched the first in a series of "Green Papers," which established the foundation of a coherent energy policy. In January 1995, 'For a European Union Energy Policy' was issued, which focused on consolidating energy markets and creating "a sound and coherent energy policy framework." The paper announced a 5-year program to address three pillars of energy security; *competitiveness, conservation (to include sustainable development) and security of supply* [89]. In November 2000, the Commission published a follow-on Green Paper, 'Towards a European Strategy for the Security of Energy Supply.' Produced in the wake of a dramatic increase in oil prices over the previous 5 years, it underlined the Union's challenge of energy security, and reinforced the notion that the EU would never escape its energy dependence without a comprehensive policy [90].

In March 2006, the Commission published a third and final Green Paper, entitled 'A European Strategy for Sustainable, Competitive and Secure Energy,' which outlined the three pillars in a more coherent manner. The paper addressed the need for a common energy policy which would allow the EU to speak as a single entity, as well as implement provisions of the Energy Charter Treaty within a free and open energy market. It also promised to establish European technological leadership in the energy field and develop renewable energy emphasizing alternative transport fuels to reduce CO_2 emissions. Solutions were also presented to stimulate investment and develop new infrastructure necessary to enhance energy access for consumers [91].

A.3.4 Demand for Energy Security: Liberalization Efforts and the Lisbon Treaty

A.3.4.1 Electricity and Gas Sector Liberalization: The Energy Packages

Since the mid-1990s, a series of legislative "packages" have been enacted to liberalize the EU's energy sectors, operating alongside the Green Papers and other energy initiatives. The European Commission submitted the packages to the European Parliament for legislative review and approval by the Council. The main emphasis has been on the member states' electricity and gas sectors, which are often uncompetitive, opaque and unaccountable, with the aim of injecting transparency into the market. A total of three packages have been approved, each successively more stringent and demanding than the previous, which demonstrate Brussels' willingness to reach across national boundaries and erode the corrosive impact of these state-level commercial energy players.

In September 2007, the Commission began work on the 'Third Energy Legislative Package,' designed to address flaws in the previous two packages and further open the gas and electricity markets [92]. The Third Package was adopted by the European Parliament and the European Council in July 2009, and became effective on September 3, 2009. Thanks to a stronger enforcement regime, powers provided by the Lisbon Treaty, the new enforcement tools include the Agency for the Cooperation of Energy Regulators (ACER) and the Energy Networks of Transmission System Operators for Electricity (ENTSO-E) and a similar one for Gas and Energy Networks of Transmission System Operators for Electricity (ENTSO-G). Essentially, these tools allow for more effective oversight, such as better sector coordination and the ability to levy fines for non-compliance [93].

A.3.4.2 Lisbon Treaty, September 2007

While the Green Papers and the Energy Charter established the theoretical structure and organizational principles for a comprehensive energy strategy, it was the September 2007 Lisbon Treaty which enshrined these principles in the EU's political and legal environments. Lisbon highlighted the three pillars, though there were several additional elements. For instance, the value of pipelines were noted to "…promote the interconnection of energy networks" but also impacted road and rail, as well as market-based interactions. The Treaty also introduced climate change as a major policy platform following the Commission's "20-20-20" directive. Finally, Lisbon gave the Commission unprecedented power to liberalize the European energy industry, particularly gas and electricity, which has been useful in Brussels' attempt to impose market discipline [83], pp. 50-51, [94]. Perhaps Lisbon's most important contribution is its attempt to consolidate the wide-ranging and disparate energy initiatives under the Commission's control. Indeed, the EU's post-Lisbon energy policies have been marked by a series of aggressive policy efforts by Brussels which will be discussed further.

A.3.4.3 European Energy Strategy to 2020 and European Energy Roadmap 2050

In 2010, the Commission published two 'over the horizon' strategies, an indication of the Commission's long-term perspective in the energy sector. Released in November 2010 was the 'European Energy Strategy (EES) 2020,' which highlighted the Commission's approach to 'decarbonization,' a principle firmly grounded in the Lisbon Treaty and earlier environmental directives. Such long-term strategy was necessary, as it was estimated in 2010 that $1.1 trillion in investments would be required over the following ten years to upgrade equipment and infrastructure to implement the strategy [95]. In December 2011, as a compendium to the EES 2020, the Commission released the 'European Energy Roadmap 2050,' which reinforced the EU's long-term demand for diversified sources of oil and gas, as well as interest in sustainable energy development. In this strategy, the EU committed to reduce 2050 levels of CO_2 emissions to 80 – 95 percent below 1990 levels. These back-to-back publications acted as a proverbial stake in the ground, indicating the Commission's post-Lisbon policy directions and priorities [96].

A.3.4.4 May 2014 Summit: A New Energy Strategy and Climate Package

With the unfolding Ukraine crisis and the South Stream pipeline tensions as a backdrop, on May 28, 2014, the Commission released a new energy strategy which superseded the EES 2020. For the short term it proposed stress tests to simulate a gas supply disruption with the goal of determining how the member states would respond to such an event. The intent was to formulate emergency plans which require increased gas stocks and reverse flow pipelines to reduce short-term demand. Medium to long-term challenges were also presented, which include increased energy efficiency toward reaching climate goals, effective negotiations with export partners, (notably Russia, Norway, Saudi Arabia, and Caspian Basin states) and "speaking with one voice" regarding EU energy policy. With South Stream in mind, the Member States were asked to inform the Commission about agreements which may impact Brussels' freedom of action [97].

Additionally, new climate and energy targets to 2030 were released on October 23, 2014, which were even more ambitious than the 20-20-20 provisions. The new targets required reduced emissions of 40 percent, as well as 27 percent renewables and 27 percent energy efficiency. Poland and several Central and Eastern European countries received financial concessions for their support of the package. Environmentalists accused the Commission of backing away from more stringent directives, while industry groups were equally dissatisfied with claims that further regulations would drive up energy costs and make them less competitive [98]. The 2014 directives build on the post-Lisbon documents of 2010 and 2011 and attempted to further consolidate the various energy and environmental efforts underway, all pointing to a culminating event in Riga in early 2015.

A.3.4.5 The Riga Summit of February 2015: The European Energy Union

Rounding out the 2014 energy strategy and 2030 climate package was the European Energy Union (EEU), outlined at the Riga energy summit in February 2015. The Commission was determined to conclude far-reaching directives across the energy sector, particularly in the electricity market. In fact, Riga was hailed by the European Commission's Vice President for the Energy Union, Maroš Šefčovič, as "…the most ambitious European project since the formation of the coal and steel community" [99]. In 2015 the Commission's Energy Directorate position was expanded to include a higher level, Vice President for Energy Union under Maroš Šefčovič. Miguel Aria Canete is the commissioner for the newly formed Climate Action and Energy directorate.

The EEU is comprised of five dimensions:

1) Energy security, solidarity and trust;
2) A fully-integrated internal energy market;
3) Energy efficiency contributing to moderation of demand;
4) Decarbonizing the economy; and
5) Research, innovation and competitiveness [100].

Though, the EEU is merely a compilation of guidelines with no legal authority, it has the potential to extend Brussels' influence over the European energy sector. Attempts to impose stricter unbundling provisions are essentially extensions of the Third Package, however, there is interest in negotiating a single EU price, particularly in gas, to break Russian price manipulation.

A.3.4.6 The EU Green Deal

The Commission places strong emphasis on the security of energy supply in the wake of the 2014 Ukraine crisis and tensions with Russia [101]. However, from the beginning of its 2019 appointment, the European

Commission, headed by Ursula von der Leyen, declared climate policy a top priority. The Green Deal, a roadmap of key policies on the EU's climate agenda, whereby the main goal is to transform Europe into a resource-efficient, competitive economy; achieving zero net GreenHouse Gas (GHG) emissions by 2050, and becoming climate neutral by decoupling economic growth from resource use. The EU has already made some progress in this effort; between 1990 and 2018 it reduced GHG emissions by 23%, while the economy grew by 61%. It is estimated, however, that current policies will only result in a 60% decrease in emissions by 2050 [102]. For this reason, the new Commission presented a plan to reduce the EU's GHG emission reductions target for 2030 by at least 50%. To reach de-carbonization it aims to transform industry and transport sectors, committing to foster a circular economy and multimodal transport [102].

These efforts require significant financial effort, and the Commission estimates that reaching the current 2030 climate and energy targets will require €260 billion additional annual investment [102]. The Sustainable Europe Investment Plan (SEIP) and the Just Transition Mechanism (JTM) have been established to ensure an equitable shift to carbon neutrality. These funds are largely financed by the EU budget, and there is a strain on Member States which rely on coal and carbon heavy industries for their power generation [103].

A.3.4.7 The Green Deal in the Aftermath of COVID-19

On the 21st of July 2020, EU leaders negotiated a €1.8 trillion package to boost the EU economy in the aftermath of Covid-19 and advance key goals such as climate transition. This deal has been welcomed by analysts as the greenest economic stimulus, with at least 30% of the recovery fund going towards climate objectives [104]. Yet, the JTM saw a budget cut from €40 billion to €17.5 billion, a blow to those Member States that will suffer most from the transition to a carbon-neutral Europe [105] There are critics of the EU Green Deal, noting unrealistic cost projections and minimizing the dangers of such a heavy reliance on renewables without adequate backup options. Notably the criticism centers on the lack of emphasis in nuclear power as a viable emissions reduction mechanism [106].

A.3.4.8 EU Fit-for-55

On 14 July 2021, the European Commission announced the "Fit-for-55" initiative, designed reduce emissions by 55% by 2030 and climate neutrality by 2050. The Fit-for-55 package includes a revision of the EU Emissions Trading System (ETS), including maritime and aviation, as well as changes to the Energy Tax Directive. Other changes under "Fit-for-55" are revisions to the Directive on deployment of alternative fuels infrastructure and regulations setting CO_2 emission performance standards for new passenger cars and light commercial vehicles [107].

A.3.5 EU-Turkey Energy Relations

The current EU-Turkish tensions have been exacerbated by Turkey's regional ambitions and illiberal actions under President Erdogan. These regional ambitions have centered on Turkey's desire to be a regional energy hub. In the early 2000s, there was cooperation on Nabucco and the Southern Gas Corridor; Turkey was anxious to portray itself as a worthy European partner and regional leader. Yet, as time passed, cost estimates mounted and organizational problems surfaced, most notably how the pipeline was to be filled, giving way to frustration in Ankara at the slow pace of progress. Meanwhile, further upstream, Azerbaijan was becoming equally frustrated at the delays in moving its gas. Ankara and Baku began discussion of a Trans-Anatolian Pipeline (TANAP) project, built and managed outside of European control. Turkey and Baku delivered the death blow to Nabucco in June 2013. Turkish resentment with the EU over lost time, money and goodwill is palpable and further demonstrates Ankara's desire to 'go it alone' outside of Western influence. A divergence that has been introduced under Erdogan and is at odds with Turkish foreign policy dating back to Ataturk.

Despite these differing paths and cooling relations, Turkey's role in the EU's energy security strategy is significant and will likely grow over time. There is the potential for as much as 30 bcm of natural gas per year passing through TANAP into EU-based pipelines; this includes not only Azerbaijani, but also Iraqi, Persian Gulf and, possibly, Iranian gas. This also places Turkey in a position of strength, a position which Erdogan clearly relishes given his desire for a greater political and economic role in the region [108], [109].

The completion of Turk Stream in December 2019 indicated a growing Moscow-Ankara nexus at the expense of European energy security. Turkey must contend with shaky relations with Greece, Cyprus, and Israel, three prospective gas exporters from the Eastern Mediterranean. [Syria…] Additionally, considering the traditional Turkish-Russian rivalry, any gas projects may not stand the test of time. It is possible that if Turkey continues its geo-political realignment away from Europe, it will become a gas rival to the West, defeating the purpose of the Southern Gas Corridor and setting back the EU's effort at source diversity. Ultimately, the EU-Russia-Turkey trifecta could devolve into a tense, though functional relationship based on mutual needs. The Turkey and Azerbaijan dynamic also bears discussion; the two states often operate in tandem, as demonstrated by strong cultural ties, and even though Turkey is predominantly Sunni and Azerbaijan is Shia. Though Turkey and Azerbaijan are on generally friendly terms with the EU, there is concern that the former is realigning itself as a neutral or even Middle East-centric state which could jeopardize long-term relations with the latter two.

A.3.5.1 The Caucasus

The Caucasus occupies a strategic and contested region on Europe's eastern periphery. Focusing on the region's two powers, Russia and Turkey, provides an interesting contrast. The traditional power rivalry still exists, though perhaps in a more benign state than a century ago, when both were locked in a brutal conflict in the Caucasus and eastern Turkey. A conflict which is emblematic of the deep political, and ethnic religious animosities of the region, and which are present to this day. … this balance of power falls decidedly in Russia's favor, though the ratio is counterbalanced somewhat by Turkey's membership in NATO. Turkey lacks the coercive influence that Russia enjoys in the Black Sea region, while Erdogan is distancing himself from traditional Western-oriented posture. To be sure, attempts to permanently change the balance of power by Ankara would be considered highly provocative to Moscow, as well as Brussels, Washington, and Tehran.

One must also consider the implications for the two Western regional security entities, the EU and NATO. The EU is relegated to its role as a soft power for the foreseeable future, leaving the use of hard power to a US-dominated NATO. The Alliance's position as a Black Sea military power began with Turkey's admittance in 1952, while the accession of Romania and Bulgaria in 2004 further anchored NATO on the Western and Southern littoral. Furthermore, it is too soon to tell the implications of the NATO's presence, particularly in its relations with Russia, as demonstrated by Moscow's ability and willingness to wield political and military force in its sphere of influence. For the time being, hard power resides to the north and any long-term power polarity analyses which deviate from this fact are fraught with risks.

As one of the world's main purveyors of soft power, as well as a regional neighbor, it is necessary to consider the EU as a component of the South-East European construct. The presence of Bulgaria and Romania, as well as long-term member Greece, as both EU states and components, demonstrates the Union's ability to straddle both organizations and thereby wield influence.

A.3.5.2 Eurasian Energy Corridor

Europe has always had relatively plentiful coal resources, though it has been a net oil and gas importer since the beginning of the Petroleum Age. For this reason, a crucial element to Europe's economic vitality is maintaining a secure, cheap, and predictable supply of energy, notably oil and gas. The genesis of the Eurasian Energy Corridor can be traced to Washington, which wanted the Central Asian and the Caucasus states to gain the ability to export oil and gas to the West outside of the Russian pipeline network; thereby giving these newly liberated states' relative economic and political independence [110]. In fact, US Secretary of State, Madeleine Albright, highlighted the US position:

> *The US does not recognize Moscow's rights to spread the sphere of its interests outside of Russia's borders. We openly declare that the US does not recognize Russia's or somebody else's right to have special commissions or spheres of influence outside of its borders.* [111]

Another consideration when establishing the corridor was to operate outside of Iranian territory. Isolating Iran was justified because of its sponsorship of terrorism and overt hostility to the West, not to mention the 2002 revelation that it had a covert nuclear development program. The result is a narrow corridor traversing a fractious and violent region, fraught with geo-political, geological, and financial challenges, all of which demanded a safe energy transit route. Black Sea geopolitics have a great deal to do with this independence, separate from overland pipelines though rivalry in this area is a significant concern that will only increase – with the discovery of abundant reserves of gas and oil in the Black Sea.

As the Soviet Union began to open in the early 1990s, an exciting prospect emerged for Western governments and energy companies which eagerly looked at the Caspian Casin, notably Azerbaijan, Kazakhstan, and Turkmenistan. Due to its existing infrastructure and friendly disposition toward the West, Azerbaijan was the centerpiece of the Caspian energy strategy [112]. At the time it was believed that Azerbaijan's aging oil fields had limited lifespan and, long-term, more productive areas existed further east. This notion was reinforced by a 1997 US Department of State report based on a US Geological Survey, which estimated considerable oil and gas reserves in the eastern Caspian Basin. More specifically, the report helped spur interest in Kazakhstan and Turkmenistan, creating the impetus for a Trans-Caspian pipeline which would allow the oil and gas to reach global markets outside of Russian and Iranian territory [113].

The great distances between the Caspian Basin's oil and gas fields and the European markets make pipelines the most feasible solution, reducing the reliance on poor road or rail networks and the inefficiency or corruption of the local governments. By breaking out of the traditional Soviet era network, the non-Russian Caspian Basin energy producers were given political/ economic freedom, albeit at considerable financial cost. The emergence of the Eurasian Energy Corridor gave these former Soviet states options outside of the Russian network, so it was considered a threat to Russian domination and has been actively challenged by the Kremlin. These initiatives began a new form of geo-economic competition known as "pipeline politics."

It is the relatively recent popularity of natural gas that has altered the broader European energy dynamic. Because its transportability via marine tanker allows oil and its derivative products to be delivered to European markets from a variety of global sources, the main concern has been natural gas, which lacks this capability. As LNG still provides a small amount of Europe's yearly gas consumption, estimated at 47 bcm or 10-15 percent in 2009, the vast majority is produced domestically or is piped in from external sources. To address this weakness, European leaders sought to diversify their gas sources by establishing energy corridors loosely based on the four Cardinal directions. For instance, a Northwest corridor is supplied by the North Sea's gas fields, a Southwestern one from Algeria, and a Northeast corridor from Russia. The one missing direction, from the Southeast, has only been recently addressed in the form of the Southern Gas Corridor. It is the Southern Gas Corridor, which is the most challenging, notably because of the difficult terrain, numerous international boundaries and the generally contested relations nested in the region.

The 1999 discovery of the Shah-Deniz gas fields, approximately 100 kilometers east of Baku, set a host of new regional dynamics in motion. This new discovery by Azerbaijan, coupled with the realization that the Central Asian states were unwilling to annoy Moscow at that time by circumventing the Russian pipeline system, was instrumental in shifting Washington's focus back to Azerbaijan and set in motion what would be the Nabucco Pipeline and ultimately, TANAP. Additionally, the goal would be expanded to include a greater emphasis on European access, particularly considering the 2006 and 2009 gas disputes; therefore, the

Southern Gas Corridor was not only a vehicle for Central Asian independence, but a venue for European energy security. Finally, it lessened the importance of an expensive and politically and legally contentious underwater pipeline across the Caspian.

A.3.6 Out of Area Considerations

The European Union has a range of geo-political challenges outside its recognized borders, many of which impact its energy security.

A.3.6.1 Eastern Mediterranean

Discoveries of natural gas deposits in the Levantine Basin have created a host of opportunities and problems, much of them around Cyprus. Central to the dispute is Turkey's refusal to acknowledge the ethnic-Greek controlled Republic of Cyprus, which it claims was illegally created following a 1974 coup. Moreover, Ankara says it will not allow Cyprus to export gas from the island and has occasionally dispatched naval vessels into Cypriot waters.

Within Greek Cyprus' disputed EEZ is the Block 12 offshore concession, also known as the Aphrodite field. These developments have created talk of a "second Southern Gas Corridor," yet the logistical and political challenges are perhaps even more daunting than the first, land-based corridor. At the December 2013 Frankfurt Gas Forum, former US Ambassador to Azerbaijan, Mathew Bryza, claimed that the potential gas wealth in the Eastern Mediterranean could be the incentive for long-term dispute resolution. Bryza noted the need to "line up" the political environment in which to facilitate a potential Israeli-Turkish natural gas alliance or even the possibility of a satisfactory resolution to the Cyprus issue. In 1995 Greece ratified the Law of the Sea Treaty; Turkey is not a signatory, which has put it at a legal and diplomatic disadvantage in the negotiations. Israel and Turkey had generally solid relations for decades, though this has taken a decided downturn during the Erdogan years. This was further exacerbated when Israeli Special Forces killed 8 Turks in May 2010 on a flotilla trying to break the Israeli-imposed Gaza blockade. Finally, Bryza referenced the importance of US involvement, citing Washington's influence in the Eurasian corridor development in the 1990s, but cautioned that any deals between these parties will require considerable patience [114].

A.3.6.2 Subsurface Gas Deposits

The Eastern Mediterranean Sea has proven to be fertile ground for hydrocarbon exploration. According to the 2010 US Geological Survey, the East Mediterranean region contained over 10 TCM of gas. Large gas deposits were discovered off the coasts of Egypt, Israel, and Cyprus. In November 2019, Turkey signed an exclusive bilateral maritime boundaries deal with the Libyan GNA, excluding the rest of its neighbors, including the Greek island of Crete, and thus overlapping with Greece's EEZ. This deal threatens ongoing and future gas explorations and pipelines projects in the Eastern Mediterranean [115]. Given the regional tensions, Russia offered to mediate talks over energy exploration disputes. Scholars have qualified this offer as surprising. Indeed, if the Cyprus-Turkey dispute is resolved, the neighboring countries would become more energy independent, negatively affecting Russian gas exports [116].

Egypt first discovered gas deposits in the late 1960s at the Abu Madi, Abu Qir (offshore) and Abu El Gharadig fields. New offshore natural gas deposits were found in 2015; the Nooros, North Alex, West Nile Delta and Zohr fields. The latter was estimated to contain approximately 849 bcm. Three smaller deposits were found since: Yunis-1, Nour-1, and Swan East-1. In 2019, BP estimated the Egyptian confirmed natural gas reserves at 2.1 TCM, and national production at 64.9 bcm. That same year, Egypt produced 53 TB per day of NGL, exported 1.7 BCM export of LNG to Europe and 0.9 bcm to Pakistan (its biggest client after Europe) [117]. The Egyptian Mediterranean region had the biggest output (58% of the national production) [118].

The Heletz-Brur-Kokhav oil field was discovered in the 1950s, producing 18MMBL of oil. Other small oil quantities were found in Zuk Tamrur and South Judean Desert. Israel discovered its first significant gas deposits, the Noa and Marie-B fields, in its southern EEZ in the late 1990s and early 2000s. Mari-B contained 45 billion bcm of gas. Many oil companies, such as Noble Energy, Delek Drilling, and the Tethys Sea partners, were granted exploration licenses by the government. The Tamar field was found in 2009, estimated to contain 240 BCM of gas. A year later, Israel's largest oil field, Leviathan, was discovered, estimated to contain 500 BCM of gas and 3 BB of oil. Smaller gas deposits were found in the Tanin, Dolphin, Karish, Tamar SW and Aphrodita-Ishai fields. To date, Israel's offshore deposits are estimated at approximately 900 BCM. Until 2019, the date of Leviathan's first production, Israeli gas deposits were essentially used for the domestic electricity production [119].

Israel aims to set itself as a key player for regional energy security. To date, Jordan and Egypt are the main importers of Israeli gas, buying 60 bcm and 25.3 bcm respectively in 2020. (Export, n.d.). In the perspective of expanding its reach to European states, Israel, in collaboration with Egypt, organized the East Med Gas Forum in January 2020. Cyprus, Greece, Italy, Jordan, and the Palestinian Authority participated. The Cyprus-Greece-Israel-Egypt partnership is a means to counterbalance Turkey. The 'East Med pipeline' project linking Israel, Cyprus, Greece, and Italy was launched 2013, and the East Med pipeline accord were signed in January 2020. The EU supports the project, as the East Med pipeline is considered as an 'EU project of common interest' given its potential to enhance EU's energy diversification. The pipeline, developed by IGI Poseidon and to be operational in 2025, will have a capacity of 20 bcm p.a. of natural gas [120], [121], [122]

Noble Energy, now Chevron, discovered Cyprus' first gas deposit in the Aphrodite field, off Cyprus's coasts, in 2011. Reserves were estimated at 129 bcm [123]. A 25-year-long exploitation license, renewable for 10 years, has been granted to Chevron [124]. If fiscally feasible, future investments include building an onshore LNG plant in the Vassilikos area. Aphrodite's gas production will most likely be sold to Egypt, considered as the most economic viable option. The recent discoveries in the north of the Egyptian EEZ indicate that Cyprus' EEZ also has strong potential. The government of Cyprus started a third licensing round in 2017, granting IOC exploration rights [125], [126].

A.3.6.3 North Africa

Cooperative relations between the EU and the North African countries have been in place for decades. The Barcelona Process, also known as the Euro-Mediterranean Partnership (EMP), began in 1995 and expanded as new countries signed the accord [127]. The EMP is a framework aiming to strengthen inter-regional political and economic relations to enhance regional development and stability [128], [129]. Although the EMP has had success liberalizing trade, increasing stability, and improving living standards in those countries, it has faced limitations, such as slow trade integration, limited FDI, and a general lack of progress reforming flexibility and overregulation in those countries. This was due to the limited tools offered for economic integration, a level of unpreparedness from the signatories, and the absence of mechanisms and incentives within the EMP to push for structural reforms [127]. Moreover, North Africa has experienced chaotic events in the past decade, including terrorism, the Arab Spring and civil wars. This not only created politically and economically unstable contexts for foreign investment, but also for the extraction, production, and export of energy resources, which negatively impacted regional energy security [130]. Yearly imports from North Africa to Europe amount to 59.1 million tons of crude oil and 10.3 million tons of refined products per year [129].

A.3.6.4 Algeria

Algeria is a key player for North African political stability. Attempting to reduce security threats at the national and regional level after the Arab Spring, Algeria has supported negotiations in Mali, Libya, and Tunisia. Additionally, Algeria agreed to pursue its role as a mediator, fighting terrorism in the North African region as well as in the Sahel [131]. Since the end of its civil war in the 1990s, Algeria has been stable. Unlike its neighbors, the country faced the Arab Spring without much violence and impact on its politics.

Despite Algeria's relative stability, three southern territories, Salah, Ouargla, and Ghardaia, faced unrest in 2013 fueled by socio-economic demands from local populations, the lack of benefits from its resources and ethno-sectarian differences. Abdelaziz Bouteflika, then-President of Algeria, resigned under military pressure in March 2019 after weeks of popular uprisings against the pouvoir, or the entrenched power base.

Algeria is central to oil and gas production and exports, and has reformed trade and investment policies to encourage Foreign Direct Investments (FDI) and joint ventures between Sonatrach, the national oil company, and other International Oil Companies (IOCs) [131]. Moreover, the EU-Algeria Association Agreement, signed in 2002 and enforced in 2005, aims to strengthen this development and cooperation effort in trade. This was supplemented in 2017 by the new Partnership Priorities, focusing on energy, sustainable development, and the environment. Algeria is an energy partner with the EU and is one of the major producers and exporter of liquefied natural gas, exporting through pipelines such as the Trans-Mediterranean line reaching France, Italy, and Spain. In 2019, 21.4 bcm of natural gas, and 15.2 bcm of LNG were exported to Europe [128], [131].

In January 2013, the In Amenas joint venture gas facility located 50 km west of the Libyan border was the target of a terrorist attack led by Katibat al-Mulathameen, a Belmohkatar's jihadist organization. The lack of awareness of the worsening security environment and the limited communication with locals and the personnel were highlighted as the main factors of political-security risks in the post-attack investigation reports [132]. The gas production at In Amenas dropped for a year and a half after the attack, going from 22,000 barrels of oil equivalent (boe) per day (before the attack) to 16,000 boe (until September 2014).

A.3.6.5 Libya

Libya is a politically and culturally diverse country divided into three regions: Cyrenaica, Tripolitania, and Fezzan [133]. What started as Arab Spring protests in 2011 have turned into an almost-decade-long and complex civil war. The Libyan conflict involves the Tripoli-based Government of National Accord (GNA), which was established in 2015 and succeeded the Government National Congress, and the Libyan National Army (LNA), based in Tobruk, and led by Field Marshal Khalifa Haftar. Each side is aided by external parties, seeking to protect their own national interests.

Moreover, the Libyan conflict allowed for the external actors to demonstrate relative power to other regional competitors. On the one hand, the GNA is officially supported by the United Nations, the European Union, the UK, Turkey, and Qatar [134], [135], [136]. The British and EU's interventions were motivated by economic interest, as well as by the potential threat of migration and terrorism. Qatar and Turkey are suspected of supporting the GNA to indirectly arm terrorist groups affiliated with Islamic State. Turkey supports the 2011 NATO humanitarian military intervention, and now has economic and oil interests in the conflict [137], [138]. In 2019 Ankara signed a bilateral maritime boundary memorandum of understanding with the GNA; excluding all other parties from the deal. On the other hand, the LNA is aided by Russia, Italy, Egypt, and France [136], [137].

In February 2014, the Libyan civil war broke out following violent uprisings against the GNC, fueled by political, religious, tribal, and regional motives. In May, Khalifa Haftar, a former officer in Qaddafi's regime and then leader of the LNA, launched Operation Dignity in Benghazi, aimed at eliminating Islamist factions in eastern Libya. This operation quickly extended to the rest of the country and called for the dissolution of the GNC, democratically elected that same year. In response, Tripoli's Islamist Misrata launched a military campaign to seize control of Tripoli and re-establish the GNC. However, the GNC failed to be recognized by the international community, which approved the new House of Representatives instead. The conflict, led by Haftar, extended to resource-rich territories, such as the Nafusa Mountains and the Western coast [139].

Libyan energy security has been deteriorating since 2011, leading to power shortages lost revenues, negatively impacting the national economy (oil revenues made up 96% of Libya's income). Before 2011, Libya was Africa's third-largest oil producer, extracting 1.6 million barrels per day. At its lowest, the country had an output of 150.000 barrels per day in May 2014. Two-thirds of hydrocarbon sites are located in the eastern part of the country. Consequently, oil and gas facilities have been controlled by pro-Haftar militias but exploited by the National Oil Company (NOC) since 2011 [140]. One federalist movement, the Petroleum Facilities Guard militia has controlled the most important crude oil export terminals in eastern Libya, using its own sales channels and thus contributing to the divide within the country. Between 2013 and 2014, the militia held a blockade of oil export terminals, choking the national economy. In 2015, the Mabruk and Ghani oil and gas facilities were attacked by IS, considered easy targets due to their dysfunctional security systems. As of 2019, approximately 10,000 km of hydrocarbon facilities and pipelines have been targeted by attacks and shutdowns.

Natural gas extraction and exports have been more stable as they are mainly offshore, and thus unreachable by militias. The remaining unaffected offshore facilities in the West contributed to Libya's small revenue during the conflict. Since oil blockades were lifted in September 2020, Libyan oil production has increased to 1.3 million barrels per day in early December [141]. However, experts predict another fall in production as the conflict over oil revenue management has not been settled as of December 2020 [142].

A.3.6.6 Syria

The Syrian conflict started in 2011 after protests against the Assad regime escalated into a civil war. The two main warring parties, backed by external powers: the Syrian forces led by Bashar al-Assad, the current Alawi President of Syria; and the predominantly Sunni anti-government rebel groups. On one hand, the Syrian regime is supported by Russia, Iran, and Hezbollah. Russia's participation is based on its interests in protecting its Tartus military base, and direct access to the Mediterranean Sea. Experts argue that Russian forces also targeted rebel groups and civilians during their operations. Furthermore, the Russian air force helped Assad's regime in the successful campaign against the rebel siege in Aleppo in late 2016. Russia and other foreign powers attempted to establish ceasefires in September 2016; December 2016; July 2017, and March 2020. Iran's intervention in the Syrian conflict is motivated by its fear of Syria's potential alignment with its Sunni neighbor, Saudi Arabia if Assad loses power.

Syria's oil fields are in the eastern (Deir al Azour) and northern-eastern (Hassakeeh) parts of the country [142]. In 2018, oil reserves were estimated at 2.5 billion barrels [142]. Before the conflict broke out, Syria produced approximately 400,000 barrels per day (b/d) of crude oil, of which 150,000 b/d were exported, mainly to the EU. The Netherlands, Italy, Germany, and France were Syria's crude oil main importers, receiving 80% of Syria's crude oil exports. Syria's gas and oil production has drastically dropped since the beginning of the conflict. In 2019, Syria produced 598,411 boe against 12,532,447 boe in 2009 [143], [144]. In 2011, Iran, Iraq and Syria signed a preliminary agreement on the creation of a natural gas pipeline linking all three countries.

Domestic hydrocarbon fields and facilities (plants and pipelines) have been at stake since the beginning of the conflict, becoming key elements in the warring parties' quest for territory. Shortly after it joined the civil war, IS gained control over gas and oil infrastructures in the eastern part of the country, which they damaged before losing it to the Kurdish-led forces in 2017. Syrian rebel groups do not control any oil resources; consequently, they rely on the other parties for their military and civilian uses. Despite President Trump's withdrawal from Syria, US troops remain to protect hydrocarbon fields and facilities, preventing IS and Assad's take over. As of November 2019, the Kurdish-led forces and the SDF controlled the two main hydrocarbon facilities, Hassakeh and Deir al-Zour, and numerous smaller fields while the Syrian government controlled the remaining fields. For all parties, hydrocarbons, especially oil, are important sources of income and means to achieve their political agenda: Assad's regime uses it for civilian and military purposes; the Kurdish forces use it for military operations and to establish domestic authority. IS uses it to finance its state and its terrorist attacks.

Given that very few hydrocarbon resources are controlled by the Assad regime, the latter had been relying on Iranian imports, paid on credit. This reliance, however, has been compromised by US-imposed sanctions on Syria's trading partners, including Iran. This pressure, backed by Saudi Arabia, Israel and the U.A.E. aimed to push Assad and Russia to make political concessions with regards to the conflict. Egypt blockaded oil deliveries to Syria, regardless of the oil's country of origin. Consequently, Syria faced oil shortages between the end of 2018 and June 2019, the date at which Iran slowly resumed its trading activities with Syria. The government implemented oil product consumption rations and raised prices to overcome the shortages. As of late 2019, oil imports remained insufficient to meet the domestic demand, while the Banyias and Homs refineries remained operational throughout the conflict.

A.3.6.7 Sub-Saharan Africa

Since the end of decolonization, the Sahel region has seen terrorist and/or ethnic violence. The region's political climate has degraded rapidly in the past decade, and states are facing strong socio-economic and political instability fueled by coups, most recently in Mali in August 2020. There have been instances of electoral and governmental scandals, such as misappropriation of military equipment in Niger in early 2020. This instability has allowed the rise of terrorist groups such as IS, but also rebel groups such as the Tuaregs. Northern Mali, Burkina Faso, Northern Niger, and the Tillabery regions are the primary territories suffering from terrorism and human trafficking [145], [146]. The international community has responded to this instability in various ways; French troops have been mobilized in the Sahel since 2013 as part of a cooperative anti-terrorism mission with the G5 Sahel, the African Union's African-led International Support Mission to Mali (AFISMA), and the international peacekeeping mission led by the United Nations Multidimensional Integrated Stabilization Mission in Mali. French President Emmanuel Macron announced a potential partial withdrawal of French troop in early 2021 after other European forces agreed to join the mission [147]. With regards to energy, Niger is a leader in uranium mining though foreign companies, France's Orano, and China's SinoUranium, have a monopoly on extraction and global exports. The Cominak site was shut down in March 2021 due to the mine's exhaustion. French nuclear reactors are fueled by Niger's uranium, and Orano is the world leader constructing those reactors.

Arguably, the Alliance's venture into the energy security sphere can be traced to December 1956 with the release of the report from the Committee on Non-Military Cooperation, headed by foreign ministers Lester B. Pearson (CAN), Gaetano Martino (ITA) and Halvard Lange (NOR), or 'The Three Wise Men.' The report acknowledged the importance of non-military cooperation, notably in the political and economic sectors, which were reinforced by the Suez Crisis and Hungarian uprising of November 1956. Implicit in the Wise Men Report was the importance of economics as a function of regional security and, more specifically, European access to Middle Eastern oil [148].

Over a decade later, and following the 1967 Six-Day War, the Council on the Future Tasks of the Alliance, or The Harmel Report, was released to address so-called out of area actions. The report's central premise was the need "…to maintain adequate military strength and political solidarity to deter aggression and other forms of pressure …" and "…to pursue the search for progress towards a more stable relationship in which the underlying political issues can be solved." The result was to seek more flexible and proactive responses to the East-West confrontation, and consider "exposed areas," such as the South-Eastern flank and the Mediterranean, as well as reinforcing the importance of the Middle East as a critical energy source [148]. The Wise Men and Harmel reports forced the Alliance to consider grand strategic implications of European security, primarily by stepping outside of NATO's purely military role and acknowledging the political and economic realms. Additionally, these two documents laid the foundation to the current NATO perceptions of energy security (and operational energy), by acknowledging that NATO's areas of interest concerned non-traditional threats, which extended outside the Alliance's collective border and purely military purposes. Moreover, the Harmel Report highlighted the value of Article 4 as a consulting mechanism whereby the member states could convene and address issues of concern.

A.3.7 NATO's Legacy Cold War Configuration: The Central European 'Fuel Desert'

Beyond the 13 states maintaining the NATO Pipeline System (NPS), there are no pipelines meeting the Alliance's fuel requirements in Central and Eastern Europe. The result is a regional 'fuel desert' where potential operations require extended lines of supply.

The NPS continues to supply the needs of the member nations with petroleum products. Today this system is in operation with links to storage depots, military airbases, civilian airports, pumping stations, truck and rail loading stations, refineries and entry/discharge points. It totals approximately 10,000 kilometers of interconnected pipelines and supplies petroleum products to 12 NATO nations. The NPS currently has a storage capacity of 4.1 million cubic meters [149].

The system is comprised of eight national and two multinational, or regional pipelines. The national pipeline systems are the Greek Pipeline System (GRPS), Icelandic Pipeline System (ICPS), Northern Italy Pipeline System (NIPS), Norwegian Pipeline System (NOPS), Portuguese Pipeline System (POPS), Turkish Pipeline Systems (TUPS) and the United Kingdom Government Pipeline and Storage System (UKGPSS).

The two multinational or regional pipeline systems are the North European Pipeline System NEPS and the Central Europe Pipeline System (CEPS). NEPS runs from Frederikshavn, Denmark on the northeast coast of Jutland, to the German border and is designed to store and transport fuel to airports and military facilities in Denmark [150]. CEPS is the largest and most significant of the cross-border pipeline systems. It is a multi-purposed and multi-product system, with a length of 5,314 km, a storage capacity of over 1 million m^3, intersecting Belgium, France, Germany, Luxembourg, and the Netherlands. The sixth member nation is the US. The North Atlantic Council allows CEPS to be used for non-military purposes yet maintaining the military function through the 'Military Priority Clause [151].

Each host nation is responsible for its the system within its boundaries. Oversight is provided by a National Organization, which is responsible for the operations, maintenance, administration, and legal support in each country. These include the Belgian Pipeline Organization, BPO (Belgium and Luxemburg), Service National des Leduc's Interalliés, the SNOI (France), Fernleitungs-Betriebsgesellschaft, the FBG (Germany), and the Defensie Pijpleiding Organisatie, DPO (The Netherlands).

There are five maritime ports in CEPS; Rotterdam, Antwerp, Gent, Le Havre and Marseille/Fos/Lavera, and 18 refineries with 14 large civil depots. Furthermore, there are nine non-CEPS military depots, four civil pipelines, 28 military airbases and six international airports (Amsterdam, Liège, Bruxelles-Zaventem, Köln/Bonn, Frankfurt, and Luxembourg). CEPS comprises 24 depots with truck/rail loading stations permitting delivery to non-connected clients. In addition to the national and multinational systems, there are also fuel systems in Bulgaria, the Czech Republic, Estonia, Hungary, Latvia, Lithuania, Poland, Romania, Slovakia, Slovenia, and Spain.

In 2017, the CEPS Program Office requested that the NATO ENSEC COE conduct a Cyber Risk Study of the Industrial Control Systems used in CEPS. Site visits to the four designated national operators (France, Germany, Holland, and Belgium) were conducted in 2018 and an individual report with recommendations was provided. This comprehensive report was presented to NATO in November 2019 [151]. During 2020, NATO ENSEC COE, at the request of the NATO Petroleum Committee agreed to prepare a follow up Cybersecurity guide for the NATO Pipeline System and other energy installations.

A.3.8 Relationship with US European Command

The United States European Command (EUCOM,) established in 1952, has continually maintained its Headquarters in Stuttgart, Germany. During the Cold War, the European theatre was a primary focus for US defence and national security with a concentration on the Former Soviet Union [153]. Traditionally, the EUCOM commander is also the Supreme Allied Commander of NATO, which ensures US control of military forces in Europe [154]. The location of its Headquarters (and SHAPE in Mons) offered a buffer of survivability during this period. At the height of the Cold War, there were more than 400,000 US troops stationed in Europe, and the primary concern was a penetration of Germany's Fulda Gap by Soviet or Warsaw Pact armored and mechanized forces [155]. Today it is a US unified command with its areas of interest and responsibility covering 51 countries [153].

On February 11, 2020, the US Secretary of Defence announced the reactivation of the V Corps headquarters in Fort Knox, Kentucky (USA). Poland was selected as the forward site for V Corps where approximately 200 personnel will rotate to that site to prepare for personnel deployment from the United States to Poland [153]. This is significant given that V Corps' location at the time of German reunification was Frankfurt – also deployed further West for the same survivability reasons as EUCOM. Also significant is that the presence of a US corps headquarters is now located in a former Warsaw Pact country as a counterweight to Moscow.

Russian wariness of EUCOM's intentions is rooted in the belief that the core target of American interests is to destabilize Moscow. The Russians themselves acknowledge that Chinese intentions do not factor into their framework, nor do they offer a hypothesis how the US intends to destabilize both Moscow and Beijing at the same time [156]. For NATO and EUCOM, there is evidence to suggest that something else is afoot; Russian maneuvers near the Ukrainian border [157] serves more than one purpose. Consider the recent war between Azerbaijan and Armenia [158], clashes between Kyrgyzstan, Tajikistan [159] and Kazakhstan outlawing large-scale Chinese land acquisitions [160] – all within the course of five months. From the Kremlin's perspective, the maneuvers serve as a warning to the Alliance while at the same time concealing their options in Eurasia. Compounding this is the unimpeded return of the Taliban in Afghanistan.

In January 2018, the National Defence Strategy (NDS) emphasized the re-emergence of long-term strategic competition, rapid dispersion of technologies, and new concepts of warfare and competition that span the spectrum of conflict, all of which require a Joint Force structured to match this reality. The NDS focus on peer competition gave renewed impetus to the trans-Atlantic Alliance and 'Russian adventurism.' NATO member states have responded to recent Russian activities in Eastern Europe, notably Crimea and Ukraine, in the form of sanctions and increased emphasis on training and readiness. Much of which is highlighted by the US-sponsored Operation Atlantic Resolve (OAR) and the European Deterrence Initiative (EDI).

EDI enables the United States to strengthen its deterrence posture with enhanced forces in Europe and support the collective defence and security of NATO allies and partners. The FY 2020 EDI request does not fund an increase in the number of US forces permanently stationed in Europe, though it does support the presence of additional US rotational forces. The five Elements of EUCOM's plan to implement EDI in FY2020/21 are:

- Increased Presence ($2,051M): The US will continue to support a rotational presence throughout the European theatre capable of deterring, and, if required, responding to regional threats.
- Exercises and Training ($609M): Increased training opportunities to improve readiness and interoperability of NATO's allies and partners.
- Enhanced Prepositioning ($2,359M): The placement of prepositioned equipment throughout the theatre to support steady-state activities, while enabling the rapid deployment of forces to theatre.
- Improved Infrastructure ($517M): Key infrastructure improvements in theatre to support US military operational requirements.
- Build Partnership Capacity ($374M): Expanded engagements and exercises and enable full participation as operational partners [161].

A.3.9 NATO at Mid-Century; Geo-Political Trajectories and Hybrid Tools

To adequately address this paper's analytic requirement, there is the need to identify a handful of notions that will carry into mid-Century, from which leaders can make educated assumptions based on historical precedent and current realities. For instance, it is unlikely the current President, Vladimir Putin, will be in power by 2040, though his influence will be felt well into this century. It is equally likely that Russia will have an interest in its near-abroad, yet whether this interest will be as aggressive remains to be seen. To envision Russia in 2040, we must consider three broad geo-political trajectories:

1) Status quo; strong nationalist sentiment with an aggressive posture,
2) Liberalizing, though maintaining regional dominance, and
3) Hyper nationalism, whereby the Kremlin engages in overt kinetic and non-kinetic actions against its neighbors.

These three trajectories allow a range of assessments and evaluation of the effectiveness of hybrid tools. For the purposes of this paper, it will be assumed that a 'status quo' posture will be implemented by the Kremlin. What is presented below are merely broad assumptions based on historical precedent and current geo-political dynamics of the region; they are rough guides for possible future actions and responses.

In this context, we can identify a handful of overlapping and mutually supporting tools and mitigation options.

A.3.9.1 Diplomatic/Coercive Tools

Russia is determined to halt or impede what it sees as NATO and EU inroads into its sphere of influence, and it is unlikely this attitude will change dramatically over the next two decades. Without clear red-lines articulated from NATO and the member states, the Kremlin will continue to employ hybrid tactics to coerce and intimidate its weaker neighbors, all designed to shape, control and undermine regional government and social/democratic institutions. The Kremlin's propensity to 'divide and conquer' will be a favorite method used against the states well into the future. Indeed, the widely divergent nature of the states' social, political and economic composition will give Russia plenty of opportunities.

The most susceptible to hybrid-instigated coercion will be the non-NATO countries in the region; Georgia, Moldova and Ukraine. Without a significant change in relations by 2040, it is unlikely these countries will be afforded NATO or EU membership. Therefore, without the benefit of Article 5, these states will undoubtedly receive most of the Kremlin's hybrid warfare-oriented attention. While the Black Sea's NATO member states, notably Romania and Bulgaria, are susceptible, future activity from Russia, which still have a deep respect for Article 5, will be careful not to cross that threshold.

A.3.9.1.1 NATO Mitigations

The Wales Summit of 2014 attempted to define hybrid warfare activities, particularly in the Article 5 context. Yet, there is still much ambiguity over what a hybrid-induced Article 5 event might entail. Additionally, the Alliance is in the difficult position of crafting responses to hybrid warfare events, which houses both NATO and non-NATO member states.

Nevertheless, NATO does provide considerable benefits, merely by its standing as an organization which provides standardization and uniformity across its member states. In other words, leveraging its position as a common venue for the members to meet, train and share best practices in a common language, and adhering to recognized standards. Perhaps the most effective mitigating efforts from NATO up to 2040 and beyond is to help strengthen good governance, civil/democratic institutions, anticorruption efforts, and promote greater interaction between Eastern European states and the EU and the United States.

A.3.9.2 Information/Technological Tools

The ability of information warfare and communications technology to act as a levelling component to the East-West competition dynamic cannot be ignored. By 2040, we can anticipate greater penetration of information technology into civil society and governance, creating additional and impactful attack vectors within the hybrid warfare realm. Also, leapfrogging offensive and defensive technologies over the next two decades will contribute to a classic security dilemma environment, and contributing to greater levels of mistrust.

Democracies are vulnerable to attacks that include disinformation or manipulations of reality; a prime example is the US 2016 Presidential election, which attracted the attention of Advanced Persistent Threats (APTs) from a variety of state sponsors. Furthermore, unless corrective action is taken, Russia by 2040 could exploit mis-aligned cyber security strategies in the West, such as differing US and EU strategies and standards of cyber security certification, privacy and data protection and public-private information sharing. Indeed, without effective countermeasures, in 20 years we can anticipate a greater ability to leverage information to sway public opinion, through more effective (believable) deep fakes and video manipulation [162].

Much of any future success in hybrid warfare, will depend on weaponizing existing and new information and operational technologies. Here is a sample of some future technologies implemented by a hybrid aggressor in 2040:

a) Counter-Blockchain Technologies, which attack the chain links' integrity and undermine its security credibility.

b) Advanced Autonomous Systems and Robotics, whereby adversaries could utilize both lethal and non-lethal systems.

c) Offensive Nanomachines, which are to gain access to secure facilities and report or disrupt activities.

d) Deep Learning AI could provide accurate fakes, resulting in lost credibility or questionable military orders, which would undermine the chain of command and compromise.

e) Quantum computers, which expand the physical limitations of computing by harnessing the power of multiple networked computers.

A.3.9.2.1 NATO Mitigations

NATO states will need to maintain a vigilant and proactive posture going into the next 20 years regarding information and technological weapons. Additionally, this will require greater collaboration between NATO entities, the member state governments, the private sector and academia. More specifically, there is the necessity to develop and retain skilled and trained personnel operating within these organizations.

One overlooked area that NATO states will be effective strategic communications departments, capable of immediately refuting false news or media. Additionally, emphasis will need to be placed on Early Warning System (EWS), capable of detecting cyber threats, as well as the misidentification of malign actors, inaccurate lists of prioritized targets, faulty predictions of courses of action, and unrealistic scenario and training events [162]. Along similar lines are new technologies to detect hard-to recognize threats, such as worms and unknown malware; most notably Deep Packet Inspection (DPI), which allows in depth evaluation of header information [162].

Finally, there is better future allocation of cyber defence policies, which streamline working principles to harmonize trans-Atlantic cyber security standards and certifications. Ultimately, this lack of coordination between the EU and US continuing into the 2040s directly will impact the readiness of NATO [162].

A.3.9.3 Military Tools

In the next 20 years, Russia will still be the primary power in the region and will be determined to control or, at best, influence, its 'near-abroad'. Even with a relatively benign Kremlin, the eastern tier will be militarized well into the 21st Century. As noted earlier, Russia will be reticent to engage in wide scale kinetic, particularly against a NATO member state. However, Russian conventional capabilities should never be overlooked or underestimated.

Russian military reforms, though sporadic and often underfunded, have made gains in the last 12 years, or since the August 2008 war with Georgia unearthed many operational deficiencies. These reforms have entailed organizational and structural changes in order of battle and equipment. Future Russian conventional posture will rely on effective use of autonomous systems, special operators, as well as legacy assets [163] We can also expect the use of new technologies, blending both kinetic and non-kinetic attributes, will prove difficult to counter. Advanced weapon technologies will increase standoff capabilities and enhance lethality within the anti-area/access denial (A2/AD) arc. Combined with Russia's already robust air defence capabilities, land and sea-based cruise missiles and hypersonics will make any operations within the A2/AD arc [164] even more hazardous, resulting in greater dispersion of forces. Moreover, this will require fielding highly mobile and flexible force, which must effectively utilize cover and concealment in the battlespace.

It can also be anticipated that Russia will make good use of Crimea and Kaliningrad as a key operational and staging area. Indeed, the Maritime Doctrine of the Russian Federation, 2015 notes upgrades and reforms to the Baltic and Black Sea Fleets [165] could challenge NATO's naval presence. Finally, to field such a force capable of operating and surviving conventional warfare of 2040, will require a highly trained, technologically savvy and experienced cadre of professionals. By focusing on a professional force [166], as opposed to its traditional reliance on conscripts, Russia in 20 years could have a well-trained and battle-hardened conventional force, capable of performing a variety of kinetic and non-kinetic missions in the Black Sea region.

A.3.9.3.1 NATO Mitigations

The Alliance's response to Russia's growing military potential over the next 20 years would most likely entail a classic deterrence posture; maintaining technical and operational superiority and implementing an ever more effective A2/AD systems. For instance, an emphasis on technological innovation in missile defence, as well as advance anti-air and anti-ship capabilities, to overlap with Russia's, creating fluid and highly distributed operations across all the domains. What becomes clear is that static or slow-moving platforms will be increasingly vulnerable, which could necessitate a so-called modified 'porcupine defence' [167], with forward deployed forces, where feasible, and the ability to quickly shift and relocate to enhance survivability. The result will be greater unit autonomy and distributed lethality and logistics; shifting away from the traditional troop and supply concentrations, which will be increasingly vulnerable to both kinetic and non-kinetic attacks.

To meet the conventional military challenges of 2040, NATO will require an equally trained and experienced professional force. Maintaining such a force will be expensive and require frequent and realistic training exercises, all of which demonstrate capabilities across all the domains and stress interoperability.

A.3.9.4 Economic Tools

The Black Sea region's location as an economic crossroads will become more pronounced over the next 20 years. More specifically, its value as a transportation hub will be critical, leading to increased vulnerability of infrastructure to hybrid threats and concomitant economic pressures. Regional supply chains will become at risk across all economic sectors. In the realm of maritime trade, the Turkish Straits as a chokepoint cannot be minimized [168]. Internal waterways, notably the Danube, could also be impeded through a variety of non-kinetic means, as would rail, road and air nodes. However, damaging or overtly interdicting trade routes could be self-defeating for the Kremlin. While such an eventuality should not be overlooked, a more realistic hybrid option would be Russian-sponsored targeted economic pressures, such as commodity price manipulation, work stoppages or slowdowns, or cyber-attacks against specific companies or transportation nodes. Moreover, orchestrated military actions with strong political and economic overtones, such as Russia's naval action against Ukraine in the Sea of Azov in November 2018, should also be expected in the future [169].

The Black Sea region's importance in 2040 will be compounded by its value as conduit for EU-bound fossil fuels. Though the sources of energy will be more diverse with a greater mix of renewables, Russian natural gas and the pipeline delivery systems will factor in the European energy mix well into this century. Ultimately, natural gas pipelines will be important feature of the region's political and economic landscape will continue to be susceptible to cyber or kinetic action from adversaries, a recent example being the Colonial Pipeline ransomware hack of May 2021 [170].

Finally, Russian investment in Black Sea infrastructure and the private sector, notably ports and energy systems, could compromise these assets [171]. Often these investments are directly tied to the Kremlin and lack transparency [172].

A.4 REFERENCES

[1] CIA Factbook. https://www.cia.gov/the-world-factbook/ Accessed 18 August 2020.

[2] Wallace, J. and Schechner, S. Follow Europe's industrial firms flash warning on energy costs. The Wall Street Journal, Dec 24, 2021. https://www.wsj.com/articles/europes-industrial-firms-flash-warning-on-energy-costs-11640345803?mod=Searchresults_pos5&page=1

[3] International Energy Agency. https://www.iea.org/topics/energy-security Accessed Dec 5, 2021.

[4] Åslund, A. and Snegovaya, M. The impact of Western sanctions on Russia and how they can be made even more effective. The Atlantic Council, May 3, 2021. https://www.atlanticcouncil.org/in-depth-research-reports/report/the-impact-of-western-sanctions-on-russia/

[5] FEMA. https://www.fema.gov/sites/default/files/2020-07/supply-chain-resilience-guide.pdf

[6] Bordoff, J. and O'Sullivan, M. Green upheaval: The new geopolitics of energy. Foreign Affairs, 101(1) (January/February 2022): 68-84.

[7] Schell, F. The Fate of the Earth, Stanford Nuclear Age Series 1982, 25-26.

[8] NATO's Role in Energy Security. https://www.nato.int/cps/en/natohq/topics_49208.htm Accessed 4 January 2022.

[9] Resilience and Article 3. https://www.nato.int/cps/en/natohq/topics_132722.htm Accessed 1 January 2022.

[10] US Congress, Public Law 115-44, Countering America's Adversaries Through Sanctions Act (CAATSA), July 27, 2017. https://congress.gov/115/plaws/publ44/PLAW-115publ44.pdf;

[11] Updated Public Guidance for Section 232 of the Countering America's Adversaries through Sanctions Act (CAATSA), July 15, 2020. https://ua.usembassy.gov/updated-public-guidance-for-section-232-of-the-countering-americas-adversaries-through-sanctions-act/

[12] National Defence Authorization Act for Fiscal Year 2020. Public Law 116–92—Dec. 20, 2019, see Section 7503. Imposition of Sanctions with Respect to Provision of Certain Vessels for The Construction of Certain Russian Energy Export Pipelines. https://congress.gov/116/plaws/publ92/PLAW-116publ92.pdf

[13] H.R.4350 – National Defence Authorization Act for Fiscal Year 2022, October 18, 2021. https://www.congress.gov/bill/117th-congress/house-bill/4350/text

[14] Flahaux, M.L., and De Haas, H. 2016. African migration: trends, patterns, drivers. Comparative Migration Studies, 4(1), 1, 2016.

[15] Paoletti, E. (2011) Power relations and international migration: The case of Italy and Libya. Political Studies, 59(2), 269–89.

[16] United Nations High Commissioner for Refugees. (2021, January). Situation Mediterranean (January 2021) [Land and sea arrivals monthly in Europe]. United Nations High Commissioner for Refugees. https://data2.unhcr.org/en/situations/mediterranean

[17] Goff, L., Zarin, H., and Goodman, S. (2012). Climate-induced migration from Northern Africa to Europe: Security challenges and opportunities. The Brown Journal of World Affairs, 18(2), 195-213.

[18] Belt and road initiative. (n.d.). Retrieved April 02, 2021, from https://www.beltroadinitiative.com/belt-and-road/ Accessed 02 February 2021.

[19] Council on Foreign Relations. (2020, January 28). China's Massive Belt and Road Initiative. Retrieved April 02, 2021, https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative

[20] Lino, M. Understanding China's Arctic activities. (n.d.). Retrieved April 02, 2021, from https://www.iiss.org/blogs/analysis/2020/02/china-arctic

[21] EIA, Russian Country Analysis, 2021: 5. https://www.eia.gov/international/content/analysis/countries_long/Russia/russia.pdf

[22] Makarova, V.N. Gazprom: Gas giant under strain, Working Paper #71, Program on Energy and Sustainable Development, Freeman Spogli Institute for International Studies, Stanford University, January 2008, 17.

[23] The Economist, Vladimir Putin is still rattled by Alexei Navalny, September 18, 2021. https://www.economist.com/europe/2021/09/18/vladimir-putin-is-still-rattled-by-alexei-navalny

[24] Shevstova, L. Putin's Russia, Revised and Expanded Edition, Washington, DC: Carnegie Endowment for Peace, 2005: 86;

[25] Smith, Keith C., Russian energy politics in the Baltics, Poland, and Ukraine: A new stealth imperialism? Washington, DC: Center for Strategic and International Studies (CSIS), 2004: 24-26;

[26] Gustafson, Thane, Wheel of Fortune: The Battle for Oil and Power in Russia, Cambridge, MA: Harvard University Press, 2012: 247-248.

[27] Kommersant, restructuring without repopulating: The faces are nearly all the same, but in different places, May 13, 2008. http://commersant.com/p891024/r_1/Prime_Minister_Vladimir_Putin_government/Kommersant

[28] Russian Ministry of Energy website. https://www.worldometers.info/gas/gas-reserves-by-country/ Accessed 18 January 2014.

[29] Aslund, Anders, Sergei Guriev and Andrew C. Kuchins, ed. Russia After the Global Economic Crisis, Peterson Institute for International Economics, Center for Strategic and International Studies, Washington, DC: New Economic School, 2010, 152-153.

[30] Global Security, Russian State Budget, From: Main Results and Trends of Budget Policy 2008 – 2010, 2013. http://www.globalsecurity.org/military/world/russia/budget.htm;

[31] The Economist, "Viktor Chernomyrdin, a Russian prime minister, died on November 3rd, aged 72", Obituary, November 4, 2010. http://www.economist.com/node/17414237

[32] "Gazprom (Gazp.Me) – Market Capitalization." CompaniesMarketCap.Com – Companies Ranked by Market Capitalization. https://companiesmarketcap.com/gazprom/marketcap/ Accessed 24 November 2023.

[33] Yegorov, O. "Why does Russia have such a low unemployment rate?" Russia Beyond, 2019. https://www.rbth.com/business/330166-russia-low-unemployment

[34] Lavikainen, Jyri, Pynnöniemi, K., and Saari, S. "Russia's foreign policy", in Russia of Power, 2019. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161710/Russia%20of%20Power.pdf?sequence=1&isAllowed=y

[35] Victor, N. 2008, 20-21.

[36] Shevstova, L. Russia: Lost in Transition: The Yeltsin and Putin Legacies, Washington, DC: Carnegie Endowment for Peace, 2007: 25.

[37] Balmaceda, M. "Russia's Central and Eastern European energy transit corridor: Ukraine and Belarus", in P. Alto (Ed.), Russia's Energy Policies: National, Interregional and Global Levels, Edward Elgar, 2012, 144-145.

[38] Putin, V. Speech and the Following Discussion at the Munich Conference on Security Policy, February 10, 2007. http://en.kremlin.ru/events/president/transcripts/24034

[39] Smith, H., "Russian foreign policy and energy: the case of the Nord Stream gas pipeline", in P. Alto (Ed.), Russia's Energy Policies: National, Interregional and Global Levels, Edward Elgar, 2012, 126-127.

[40] Newlin, C. and Mankoff, J. "U.S. sanctions against Russia: What you need to know", Center for Strategic and International Studies, 2018. https://www.csis.org/analysis/us-sanctions-against-russia-what-you-need-know

[41] Malle, S. "Economic sovereignty. An agenda for Militant Russia", Russian Journal of EconomicsVolume 2, Issue 2, June 2016: 126. https://reader.elsevier.com/reader/sd/pii/S2405473916300150?token=BE2563837A571590E5C71B85B31B521D03AE48798A341562B9D9A53148A810814C3ABEEC840D51660207BE57A34C0F1D&originRegion=us-east-1&originCreation=20211220193428

[42] Romanova, T., "Energy Dialogue from Strategic Partnership to the Regional Level of the Northern Dimension", In P. Aalto (Ed.), The EU-Russian Energy Dialogue: Europe's Future Energy Security. Ashgate Publishing, Ltd., 2008.

[43] Interview with Samuel Furfari 2015.

[44] Treaty of Lisbon, 2007, Title XX, Energy, Article 176 A. Note: EU measures should not affect the right of a member state to determine the conditions for exploiting its energy resources, its choice between different energy sources and the general structure of its energy supply. http://publications.europa.eu/resource/cellar/688a7a98-3110-4ffe-a6b3-8972d8445325.0007.01/DOC_19

[45] Khamashuridze, Z. Energy security and NATO: Any role for the Alliance? Connections The Quarterly Journal 07(4):43-58, 2008. https://www.researchgate.net/publication/270347493_Energy_Security_and_NATO_Any_Role_for_the_Alliance

[46] National Defence Authorization Act for Fiscal Year 2018, 2017: 2831. https://www.congress.gov/115/crpt/hrpt404/CRPT-115hrpt404.pdf

[47] 10 US Code § 2924, referenced in Department of Defence, 2016 Operational Energy Strategy. https://www.acq.osd.mil/eie/Downloads/OE/2016%20DoD%20Operational%20Energy%20Strategy%20WEBc.pdf#:~:text=Accordingly%2C%20the%20Department%20will%20pursue%20the%20following%20objectives,logistics%20and%20operational%20risks%20from%20operational%20energy%20vulnerabilities

[48] NATO 1991 Strategic Concept. https://www.nato.int/cps/en/natohq/official_texts_23847.htm

[49] NATO 1999 Strategic Concept. https://www.nato.int/cps/en/natolive/official_texts_27433.htm

[50] NATO, 2006 Riga Summit. https://www.nato.int/docu/pr/2006/p06-150e.htm

[51] NATO, 2008 Bucharest Summit. https://www.nato.int/cps/en/natohq/events_7344.htm

[52] NATO, Chicago Summit. https://www.nato.int/cps/en/natohq/official_texts_87593.htm?selectedLocale=en

[53] NATO, Wales Summit. https://www.nato.int/cps/en/natohq/official_texts_112964.htm

[54] NATO, Warsaw Summit. https://www.nato.int/cps/en/natohq/official_texts_133169.htm

[55] NATO, Brussels Summit. https://www.nato.int/cps/en/natohq/official_texts_156624.htm

[56] NATO Strategic Concept, 2022, https://www.nato.int/strategic-concept/index.html

[57] Interoperability: Connecting NATO Forces. Last updated: 24 March 2020. https://www.nato.int/cps/en/natohq/topics_84112.htm

[58] NATO, Statement of Work for Provision of OLSP Global Fuel Services: Short Notice Tasks in Europe, NATO Support and Procurement Agency, 28 August 2020. https://eportal.nspa.nato.int/eProcurement/RFP/PublicRFPList.aspx

[59] Evans, M. The silent revolution within NATO logistics: A study in Afghanistan fuel and future applications (2012 – 12). Naval Postgraduate School: Monterrey, CA. https://core.ac.uk/download/pdf/36720657.pdf

[60] NATO Standard, AJP-4: Allied Joint Doctrine for Logistics, Edition B, Version 1, Dec 2018. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/907825/doctrine_nato_logistics_ajp_4.pdf

[61] Braesch, C. DLA Energy's International Agreements Program Supports a Network of Global Relationships. https://www.dla.mil/AboutDLA/News/NewsArticleView/Article/1731115/dla-energys-international-agreements-program-supports-a-network-of-global-relat/ Accessed 15 January 2021.

[62] EUCOM, Acquisition and Cross-Servicing Agreements (ACSA) Guide: ECJ4-ML, November 1, 2001. https://www.acq.osd.mil/ic/ACSA.html

[63] National Defence Strategy, 2018: 7. https://dod.defence.gov/Portals/1/Documents/pubs/2018-National-Defence-Strategy-Summary.pdf

[64] EUCOM, Acquisition and Cross-Servicing Agreements (ACSA) Guide: ECJ4-ML, 1 November 2001. https://www.acq.osd.mil/ic/ACSA.html

[65] NATO, NATO Logistics Handbook: Chapter 2, November 2012. https://www.nato.int/docu/logi-en/logistics_hndbk_2012-en.pdf

[66] Young, T.-D. The challenge of reforming European Communist legacy 'logistics.' Journal of Slavic Military Studies 2016, Vol. 29(3), 352-370. https://www.tandfonline.com/doi/abs/10.1080/13518046.2016.1200376?journalCode=fslv20

[67] Votel, J.L., Cleveland, C.T., Connett, C.T. and Irwin, W. Unconventional warfare in the gray zone. JFQ 80, 1st Quarter 2016. https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-80/jfq-80_101-109_Votel-et-al.pdf

[68] Jones, R.C. Deterring competition short of war. Small Wars Journal, May 14, 2019. https://smallwarsjournal.com/index.php/jrnl/art/deterring-competition-short-war-are-gray-zones-ardennes-our-modern-maginot-line

[69] Galeotti, M. Active measures: Russia's covert geopolitical operations. Marshall Center, June 2019, Number 031. https://www.marshallcenter.org/en/publications/security-insights/active-measures-russias-covert-geopolitical-operations-0

[70] Derleth, J. Russian New Generation Warfare: Deterring and Winning at the Tactical Level, Army University Press, September-October 2020. https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/September-October-2020/Derleth-New-Generation-War/

[71] NATO Standardization Office (NSO). Allied Joint Publication 01 (AJP-01).

[72] International Institute for Strategic Studies (IISS). Complex crises call for adaptable and durable capabilities. Military Balance, 1 (1 January 2015): 5–8. https://infosec-journal.com/article/complex-crises-call-adaptable-and-durable-capabilities

[73] Bartles, C.K. Getting Gerasimov right. Military Review, 2016, 34. https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20160228_art009.pdf

[74] Chivvis, C.S. Understanding Russian hybrid warfare and what can be done about it. Testimony presented before the House Armed Services Committee on March 22, 2017. https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf

[75] Foreign Policy Concept of the Russian Federation (approved by President of the Russian Federation Vladimir Putin on November 30, 2016), December 1, 2016. https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2542248

[76] Lilly, B. and Cheravitch, J. The past, present, and future of Russia's cyber strategy and forces, in: 2020, 12th International Conference on Cyber Conflict (2020). October 22, 2020. https://www.rand.org/pubs/external_publications/EP68319.html

[77] Lansing, John. Statement before the House Appropriations Subcommittee on State, Foreign Operations, and Related Programs, United States Efforts to Counter Russian Disinformation and Malign Influence. 10 July 2019. https://docs.house.gov/meetings/AP/AP04/20190710/109748/HHRG-116-AP04-Wstate-LansingJ-20190710.pdf

[78] CRS, Deep Fakes and National Security, 6 June 2021. https://crsreports.congress.gov/product/pdf/IF/IF11333

[79] Binnendijk, A. and Priebe, M. (2019). An attack against them all? Drivers of decisions to contribute to NATO's collective defence. Rand: Santa Monica, CA: 33. https://www.rand.org/content/dam/rand/pubs/research_reports/RR2900/RR2964/RAND_RR2964.pdf

[80] Smith, R. Force majeure' clauses in commodity sale agreements – what you should be thinking about? ReedSmith Law Firm. Critical Alert, 13-167, June 2013.

[81] Doffman, Z. Huawei just launched 5G in Russia with Putin's support: 'Hello Splinternet'. Forbes, 1 September 2019. https://www.forbes.com/sites/zakdoffman/2019/09/01/hello-splinternet-huawei-deploys-5g-in-russia-with-putins-support/?sh=6aef6169199d

[82] European Information Association, Finding out about EU energy policy, 2007. http://eia.org.uk/finding/0711-energy.pdf;

[83] Furfari, S., Politique et Geopolitique de l'energie: une analyse des tensions internationals au XXIeme siècle, Brussels: Editions Technip, 2012: 47-48, 288.

[84] Aalto, P., ed., The EU-Russian Energy Dialogue: Europe's Future Energy Security. Hampshire, UK: Ashgate, 2008.

[85] Westphal, K. "Germany and the EU-Russia energy dialogue.", In P. Aalto (Ed.), The EU-Russian Energy Dialogue: Europe's Future Energy Security. Ashgate Publishing, Ltd, 2008, 94.

[86] US Library of Congress, A Country Study: Soviet Union, May 1989. https://www.loc.gov/item/90025756/

[87] Europa, Summaries of EU Legislation, European Energy Charter. Last update May 25, 2020. http://europa.eu/legislation_summaries/energy/external_dimension_enlargement/l27028_en.htm

[88] Egenhofer, C. et al. The Ever-Changing Union: An Introduction to the History, Institutions and Decision-Making Processes of the European Union. 2nd Edition, Brussels: Centre for European Policy Studies, 2011, 34-42.

[89] European Commission. For a European Union energy policy. Green Paper. COM (94) 659 final/2, 23 February 1995. http://aei.pitt.edu/1185/

[90] European Commission. Towards a European strategy for the security of energy supply. Green Paper, COM, 2000. https://op.europa.eu/en/publication-detail/-/publication/0ef8d03f-7c54-41b6-ab89-6b93e61fd37c/language-en

[91] European Commission. A European strategy for sustainable, competitive and secure energy. Green Paper, COM, 2006. http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/ec/93135.pdf

[92] European Commission. Questions and Answers, Memo/07/362. 19 September 2007. http://ec.europa.eu/energy/gas_electricity/legislation/third_legislative_package_en.htm

[93] European Commission. Directive 2009/72/EC of the European Parliament. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0072#:~:text=Directive%202009%2F72%2FEC%20of%20the%20European%20Parliament%20and%20of,internal%20market%20in%20electricity%20and%20repealing%20Directive%202003%2F54%2FEC

[94] Information Network for Sustainable Europe (INFORSE). The Lisbon Treaty and Sustainable Energy. Accessed 30 September 2013. http://www.inforse.org/europe/eu_table_lisbon.htm

[95] European Commission, Energy 2020: A strategy for competitive, sustainable and secure energy, Brussels, 10.11.2010, COM(2010) 639 final, 2010: 2. http://eur-lex.europa.eu/legal-content/EN/TXT/? uri=CELEX:52010DC0639

[96] European Commission. Background paper: Energy Roadmap 2050 – State of Play. 3 May 2011. http://ec.europa.eu/energy/strategies/2011/doc/roadmap_2050/20110503_energy_roadmap_2050_state_of_play.pdf

[97] European Commission. Energy: Security of Energy Supply, European Energy Security Strategy. Accessed 10 August 2014. http://ec.europa.eu/energy/security_of_supply_en.htm

[98] Van Renssen, S. The EU's great 2030 energy and climate compromise. Energypost, October 24, 2014. http://www.energypost.eu/eus-great-2030-energy-climate-compromise/

[99] Van Renssen, S. Brussels tests limits of its powers with Energy Union, EnergyPost.eu, February 27, 2015. https://energypost.eu/brussels-tests-limits-powers-energy-union/#:~:text=%E2%80%9CThis%20is%20undoubtedly%20the%20most%20ambitious%20European%20project,for%20Europe%20package%20on%2025%20February%20in%20Brussels

[100] European Commission, Energy Union. https://ec.europa.eu/energy/topics/energy-strategy/energy-union_en#:~:text=%20The%20energy%20union%20builds%20five%20 closely%20related,efficiency%20-%20improved%20energy%20efficiency%20will...%20More%20 Accessed 26 December 2021.

[101] Siddi, M. The European Green Deal: assessing its current state and future implementation. Climate Policy, 16(5), 2020, 543-547. https://www.researchgate.net/publication/341701815_The_European_Green_Deal_Assessing_its_current_state_and_future_implementation

[102] EC. The European Green Deal. COM (2019) 640 final. Brussels: European Commission, 2019. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2019%3A640%3AFIN

[103] Hafner, M., and Raimondi, P.P. Priorities and challenges of the EU energy transition: From the European Green Package to the new Green Deal. Russian Journal of Economics, 6, 374, 2020.

[104] EC. EU Budget: European Commission welcomes agreement on €1.8 trillion package to help build greener, more digital and resilient Europe. European Commission Press Release, 2020. Retrieved from: https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2073

[105] Casier L. The EU's financing of a resilient recovery. IISD, 23 July 2020. https://www.iisd.org/sustainable-recovery/the-eus-financing-of-a-resilient-recovery/

[106] Furfari, S. and Mund, E. The European Green Plan will be ruinous and destructive. Clintel, 14 October 2021. https://clintel.org/europes-green-plans-are-ruinous-and-destructive/

[107] Stiftung, H.B. The EU's Fit-for-55 Package, 14 July 2021. https://eu.boell.org/en/fit-for-55

[108] Tagliapietro, S. The EU-Turkey energy relations after the 2014 Ukraine crisis: Enhancing the partnership in a rapidly changing environment. Fondazione Eni, Enrico Mattei, 2014. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2493665.

[109] Marketos, T. EU energy geopolitics: The potential role of Iran and the Turkish route. Natural Gas Europe, 15 December 2014. http://www.naturalgaseurope.com/eu-energy-geopolitics-iran-russia-turkey?utm_source=Natural+Gas+Europe+Newsletter&utm_campaign=36379996f9-RSS_EMAIL_CAMPAIGN&utm_medium=email&utm_term=0_c95c702d4c-36379996f9-303821421

[110] LeVine, S. The world's first pipeline war has officially come to an end, Quartz, Dec 2, 2014. http://qz.com/304742/the-worlds-first-pipeline-war-has-officially-come-to-an-end/

[111] Sagheb, N. and Javadi, M. US permanent representative in the UN does not recognize Russia's Special Rights outside of its border. Turan News Agency, 27 October 1994.

[112] Pflüger, F. The Southern Gas Corridor: Reaching the home stretch. European Energy Review, 12 January 2012. http://www.europeanenergyreview.eu/site/pagina.php?id_mailing=381&id=3455

[113] US Geologic Survey. World petroleum resources project fact sheet, assessment of undiscovered oil and gas resources of the North Caspian Basin, Middle Caspian Basin, North Ustyurt Basin, and South Caspian Basin Provinces, Caspian Sea Area. November 2010. https://pubs.usgs.gov/fs/2010/3094/pdf/FS10-3094.pdf

[114] Natural Gas Europe. Eastern Mediterranean gas: Economics first, then politics. 12 December 2013. http://www.naturalgaseurope.com/frankfurt-gas-forum-eastern-mediterranean-energy?utm_source=Natural+Gas+Europe+Newsletter&utm_campaign=b6c26d4132-RSS_EMAIL_CAMPAIGN&utm_medium=email&utm_term=0_c95c702d4c-b6c26d4132-303821421

[115] Stanicek, B. Turkey: Remodelling the eastern Mediterranean (PE 652.048). European Parliamentary Research Service, September 2020. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/652048/EPRS_BRI(2020)652048_EN.pdf

[116] Reuters staff. Russia offers to mediate any Cyprus-Turkey talks. Reuters, 8 September, 2020. https://www.reuters.com/article/us-cyprus-turkey-russia-idUSKBN25Z19Y

[117] British Petroleum. (2020). Statistical Review of World Energy (69th edition). https://www.bp.com/content/dam/bp/business-sites/en/global/corporate/pdfs/energy-economics/statistical-review/bp-stats-review-2020-full-report.pdf

[118] EGAS. (n.d.). Exploration. Retrieved 24 January 2021, from https://www.egas.com.eg/activities/exploration

[119] Exploration history. (n.d.). The Ministry of National for Infrastructure, Energy and Water Resources. Retrieved 24 January 2021, from https://www.energy-sea.gov.il/English-Site/Pages/Oil%20And%20Gas%20in%20Israel/History-of-Oil--Gas-Exploration-and-Production-in-Israel.aspx

[120] IGI Poseidon. Eastmed, July 10 2019. http://www.igi-poseidon.com/en/eastmed

[121] Oskonbaeva, 2020.

[122] Export. (n.d.). The Ministry of National for Infrastructure, Energy and Water Resources. Retrieved 24 January 2021, from https://www.energy-sea.gov.il/English-Site/Pages/Gas%20Markets/Israels-Export-Options.aspx

[123] Aphrodite Gas Field. (n.d.). Delek Drilling. Retrieved 24 January 2021, from https://www.delekdrilling.com/project/aphrodite-gas-field

[124] Eastern Mediterranean. (2020). Noble Energy. https://www.nblenergy.com/operations/eastern-mediterranean

[125] Hadjitofi, M. (2017, July). Gas in Cyprus: Opportunities for Dutch business & knowledge institutions. Octagon. https://www.nederlandwereldwijd.nl/binaries/nederlandwereldwijd/documenten/publicaties/2017/11/20/kansen-in-de-gassector-in-cyprus/Gas+in+Cyprus.pdf

[126] Kumar, D. K. (2019, May 3). Cyprus expects first natgas output from Aphrodite field by 2025. Reuters. https://www.reuters.com/article/us-cyprus-energy/cyprus-expects-first-natgas-output-from-aphrodite-field-by-2025-idUSKCN1S91Z6

[127] Nsouli, S.M. The Euro-Mediterranean partnership ten years on: Reassessing readiness and prospects, statement by Saleh M. Nsouli, Director of Offices in Europe. IMF, 23 June 2006. https://www.imf.org/en/News/Articles/2015/09/28/04/53/sp062306

[128] Bahgat, G. The geopolitics of energy: Europe and North Africa. The Journal of North African Studies, 15:1, 39-49, 2010. DOI: 10.1080/13629380902731975;

[129] British Petroleum. Statistical Review of World Energy, 69th edition. 2020. https://www.bp.com/content/dam/bp/business-sites/en/global/corporate/pdfs/energy-economics/statistical-review/bp-stats-review-2020-full-report.pdf

[130] Lambrechts, D., and Blomquist, L.B. (2017). Political-security risk in the oil and gas industry: The impact of terrorism on risk management and mitigation. Journal of Risk Research, 20(10), 1320-1337, 2017.

[131] Conseil d'Association entre l'Union Européenne et l'Algérie. 7 March 2017. Priorités communes de Partenariat entre la République Algérienne Démocratique et Populaire (Algérie) et l'Union européenne (UE) au titre de la Politique européenne de voisinage révisée. Retrieved on 15 December 2020, from https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/10._pps_alg_text_council_09_03_2017_st03101.fr17.pdf

[132] Hagen, T., Grung-Olsen, R., Fulcher, M.A., Handal, E., and Bunn, J. The In Amenas attack – Report of the investigation into the terrorist attack on In Amenas. Prepared for Statoil ASA's Board of Directors, September 2013. https://www.equinor.com/en/where-we-are/algeria/the-main-conclusions-of-the-investigation.html

[133] Gartenstein-Ross, D., and Barr, N. Dignity and dawn: Libya's escalating civil war. Terrorism and Counter-Terrorism Studies, 1, 2015. DOI: 10.19165/2015.1.01.

[134] European Council. The European Union will step up efforts towards a peaceful and political solution in Libya [Press release], January 8, 2020. https://www.consilium.europa.eu/en/press/press-releases/2020/01/08/readout-of-the-meeting-between-charles-michel-president-of-the-european-council-and-prime-minister-of-the-government-of-national-accord-of-libya-fayez-al-sarraj/

[135] Foreign & Commonwealth Office. UK reiterates support for Libya's legitimate institutions. GOV.UK, 30 April, 2020. https://www.gov.uk/government/news/uk-reiterates-support-for-libyas-legitimate-institutions

[136] Oskonbaeva, Z. General Haftar and Libya's game of musical chairs. Research Institute for European and American Studies, 18 April 2019. https://rieas.gr/images/editorial/libyazil.pdf

[137] Tekir, G. Russian-Turkish involvement in the Civil War in Libya. Türkiye Rusya Araştırmaları Dergisi, 2(3), 190-215, 2020.

[138] North Atlantic Treaty Organization. NATO and Libya (archived). NATO, 9 November, 2015. https://www.nato.int/cps/ic/natohq/topics_71652.htm

[139] Gartenstein-Ross, D., and Barr, N. Dignity and dawn: Libya's escalating civil war. Terrorism and Counter-Terrorism Studies, 1, 2015. DOI: 10.19165/2015.1.01.

[140] Ghaddar, A., and Lewis, A. Explainer: What's at stake for Libya's oil as conflict flares? Reuters, 29 April 2019. https://www.reuters.com/article/us-libya-security-oil-explainer-idUSKCN1S51H6

[141] International Crisis Group. Crisis group Libya update #1. 11 December 2020c. https://www.crisisgroup.org/middle-east-north-africa/north-africa/libya/crisis-group-libya-update-1

[142] Reality Check team. Syria war: Who benefits from its oil production? BBC News, 21 November 2019. https://www.bbc.com/news/50464561#:%7E:text=In%202018%2C%20Syria%20had%20an,and%20Iraq's%20147%20billion%20barrels.&text=In%202008%2C%20Syria%20produced%20406%2C000,of%20World%20Energy%20for%202019

[143] IEA Oil Information. 2020. https://www.iea.org/subscribe-to-data-services/oil-statistics

[144] IEA Natural Gas Information. 2020. https://www.iea.org/subscribe-to-data-services/natural-gas-statistics

[145] Cafiero, G. Algeria's northern Mali headache: North Africa-issue in focus. Africa Conflict Monthly Monitor, March 2014, 25-29.

[146] International Crisis group. Sidelining the Islamic state in Niger's Tillabery. Report No. 289, June 2020. https://www.crisisgroup.org/africa/sahel/niger/289-sidelining-islamic-state-nigers-tillabery

[147] SC Res 2100, UNSC, 68 YEAR, UN Doc S/RES/2100, 2013.

[148] Report of the Committee of Three, NATO Website. https://www.nato. int/cps/en/natohq/topics_65237.htm Accessed 26 November 2021.

[149] Harmel Report, NATO website. https://www.nato.int/cps/en/natohq/topics_67927.htm Accessed 26 November 2021

[150] NATO Pipeline System (NPS). https://www.nato.int/cps/en/natohq/topics_56600.htm Accessed 26 November 2021.

[151] Central Europe Pipeline System (CEPS). https://www.nato.int/cps/en/natohq/topics_49151.htm Accessed 26 November 2021.

[152] NATO ENSEC COE Subject Matter Expert presented a report at the NATO HQ. 14 November 2019. https://www.enseccoe.org/en/newsroom/nato-ensec-coe-subject-matter-expert-presented-a-report-at-the-nato-hq/458

[153] Congressional Research Service. United States European Command: Overview and Key Issues. In Focus – Congressional Research Service: Updated 4 August 2020. https://sgp.fas.org/crs/natsec/IF11130.pdf

[154] NATO, Supreme Allied Commander Europe. Official NATO Website. Accessed 26 November 2021. https://www.nato.int/cps/en/natohq/topics_50110.htm

[155] LA Times. Fulda Gap is the key point in NATO defence against Soviet forces. LA Times, 1 March 1987. https://www.latimes.com/archives/la-xpm-1987-03-01-mn-6926-story.html

[156] Qureshi, W.A. The rise of hybrid warfare. Notre Dame Journal of International & Comparative Law, 10(2), Article 5, 2 June 2020. https://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=1124&context=ndjicl

[157] Balmforth, T. and Williams, M. Russia orders troops back to base after buildup near Ukraine. Reuters [online], 23 April 2021. https://www.reuters.com/world/europe/russia-orders-troops-back-base-after-buildup-near-ukraine-2021-04-22/

[158] ReliefWeb, Azerbaijan: Pre-existing situation and the impact of the 2020 Nagorno-Karabakh conflict, 21 December 2020. ReliefWeb. https://reliefweb.int/report/azerbaijan/azerbaijan-pre-existing-situation-and-impact-2020-nagorno-karabakh-conflict-21

[159] BBC. Deadly fighting on Kyrgyzstan-Tajikistan border kills at Least 31. BBC, 30 April 2021. https://www.bbc.com/news/world-asia-56940011#:~:text=File%20picture%20of%20a%20military%20drill%20held%20in,clashes%20in%20years%20on%20a%20disputed%20Kyrgyzstan-Tajikistan%20border

[160] Putz, C. Kazakhstan bans sale of agricultural land to foreigners. The Diplomat, 18 May 2021. https://thediplomat.com/2021/05/kazakhstan-bans-sale-of-agricultural-lands-to-foreigners/

[161] EUCOM, FY 2020 European Deterrence Initiative (EDI Factsheet). https://www.eucom.mil/document/39921/fy-2020-european-deterrence-initiative-fact-s

[162] Dupuy, A.C., Nussbaun, D., Butrimas, V., and Granitsas, A. Energy security in the era of hybrid warfare. NATO Review. 13 January 2021. https://www.nato.int/docu/review/articles/2021/01/13/energy-security-in-the-era-of-hybrid-warfare/index.html

[163] Tadjdeh, Y., Algorithmic warfare: Russia expanding fleet of AI-enabled weapons. National Defence, 20 July 2021. https://missiledefenceadvocacy.org/missile-threat-and-proliferation/todays-missile-threat/russia/russia-anti-access-area-denial/

[164] Giles, K. and Boulegue, M. Russia's A2/AD capabilities: Real and imagined. The US Army War College Quarterly: Parameters, 49(1), Parameters Spring/Summer 2019, 1 March 2019. https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=2860&context=parameters

[165] Davis, A. (translator). The 2015 Maritime Doctrine of the Russian Federation. Russia Maritime Studies Institute, U.S. Naval War College, U.S. Naval War College Digital Commons, 2015. https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1002&context=rmsi_research

[166] Congressional Research Service, Russian Armed Forces: Military Modernization and Reforms, 20 July 2020. https://crsreports.congress.gov/product/pdf/IF/IF11603

[167] US Naval War College. Breaking the mold: War and strategy in the 21st century. 7 March 2018. https://usnwc.edu/News-and-Events/Events/Breaking-the-Mold-War-and-Strategy-in-the-21st-Century

[168] Pală, D. The geostrategic choke points of Bosporus and Dardanelles in the context of the New Silk Road. The Romanian Economic Journal. Year XXII(73) September 2019. http://www.rejournal.eu/sites/rejournal.versatech.ro/files/articole/2019-10-03/3577/5ypala.pdf

[169] Coffey, L. Russian dominance in the Black Sea: The Sea of Azov. Middle East Institute 75, 25 September 2020. https://www.mei.edu/publications/russian-dominance-black-sea-sea-azov

[170] Department of Energy. Colonial Pipeline cyber incident. Accessed 29 November 2021. https://www.energy.gov/ceser/colonial-pipeline-cyber-incident

[171] Stronski, P. and Himes, A. Russia's game in The Balkans. Carnegie Endowment for International Peace, January 2019. https://carnegieendowment.org/files/Stronski_Himes_Balkans_formatted.pdf

[172] GAN Integrity. Russia Corruption Report. Updated: June 2020. https://www.ganintegrity.com/portal/country-profiles/russia/

Annex B – NATO ENERGY SECURITY ANALYSIS – CYBER REPORT[1]

Sarah Lohman
US Army War College
UNITED STATES

Vytautas Butrimas
NATO ENSEC COE
LITHUANIA

Georgios Giannoulis
NATO HYBRID COE
GREECE

Gabriel Raicu
Constanta Maritime University
ROMANIA

SUMMARY

The two main findings of the SAS-163 cyber team are that NATO countries are under increasing and persistent threat to their critical energy infrastructure through at least 2024, and that malign influence, specifically from Russia and China, are directly impacting critical energy infrastructure in NATO member states. Solutions outlined in this report include developing a new generation of Cyber Early Warning System which includes energy critical infrastructure virtualization and developing non-hackable energy sources such as microgrids for military installations that can successfully island. In addition, to fight disinformation, a NATO-based disinformation rapid response force is proposed.

B.1 INTRODUCTION

Dr. Sarah J. Lohmann

On the day that Ukraine was supposed to start "isolation mode" tests for its new power network, beginning the process of decoupling from the Russian grid, Russia started a full-scale invasion of the country [1]. While this current 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, using cyber-attacks on the grid, disinformation campaigns, and malign influence targeted at dividing 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. Step by step, Russia has used hybrid warfare to challenge energy security, not just in Ukraine, but across NATO member states as Russia seeks to beat back NATO influence and expand its power vortex on the world stage. Now escalating into 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.

Hybrid warfare can be defined as 'grey area' warfare, which exists beneath the threshold of armed conflict. According to NATO: "Hybrid threats combine military and non-military as well as covert and overt means, including disinformation, cyber-attacks, economic pressure, deployment of irregular armed groups and use of regular forces" [2]. For NATO's adversaries, malicious cyber activity directed at the critical infrastructure of another state is effective, cheap, and deniable.

This cyber study examines how hybrid warfare including disinformation, cyber-attacks and malign influence aimed at the energy sector is shaping the battlefield, and rattling energy security across NATO states and beyond. In this era of hybrid warfare, cyber-attacks or disinformation campaigns and kinetic attacks happen in coordination in the same limited time frame. Alternatively, cyber and information operations can cause the

[1] Preliminary research conducted by the SAS-163 cyber team and reflected in this report has been published in altered form in: Lohmann, S. What Ukraine Taught NATO About Hybrid Warfare, US Army War College, 2022. The research findings presented here occur with the express copyright permission of the authors.

destruction or disablement of energy critical infrastructure even more potently, and at a lesser cost, than kinetic attacks. As hybrid warfare gradually escalates against NATO members in the context of the current Ukraine conflict, energy security continues to be the target.

For the purposes of 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" [3]. Energy sources can include electricity, nuclear, oil, gas, coal, as well as 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" [4].

As part of the broader NATO Science and Technology Organization study, this cyber report examines how hybrid warfare is being used by NATO's adversaries to disrupt energy security, what cyber vulnerabilities in energy critical infrastructure exist across the Alliance, and what mitigation strategies can be used to protect cybersecurity and enhance energy independence on military installations.

Specifically, the first section assesses key vulnerabilities in energy critical infrastructure in a hybrid warfare context. It starts with an examination of the main grey warfare threats to energy critical infrastructure, including to information technology, operational technology, and industrial control systems. It then looks at malign influence and disinformation's impact on energy security.

The second section provides new research on key hybrid warfare mitigation technologies, including a new generation of early warning systems and analysis of independent, non-hackable energy sources such as microgrids. Finally, it provides a categorization and history of cyber threats and a glossary of cybersecurity terms for reference.

B.1.1 Finding One

NATO countries are under immediate and persistent cyber threats to critical energy infrastructure through 2024

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 of 2021. In fact, 93% 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 [5]. More than 40% of the Russian-backed destructive cyber-attacks were on Ukraine's critical infrastructure sector, including nuclear and transportation [5].

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.

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 [6]. Since the invasion of the Ukraine, significant cyber-attacks have impacted NATO member states. A Feb. 24 cyber-attack on a satellite providing services to Ukraine caused a region-wide internet connection outage in the Ukraine, but it also caused 40,000 users in Poland, Germany, Greece, France, Hungary, and Italy to have an Internet outage. The same cyber-attack knocked 5,800 wind turbines in Germany and Central Europe offline affecting 11 gigawatts of power.[7] On April 12, another cyber-attack 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 [7]. The pro-Russian government ransomware group Conti launched a cyber-attack against another turbine maker, Nordex SE, and forced the company to shut down its IT systems [7]. Interrupting Europe's energy supply through a cyber-attack can be much cheaper than kinetic attacks because the current state of microgrids and wind turbines often do not yet have comprehensive cybersecurity protection [8]. Now, eight months into the war, energy is one of the most attacked sectors in Ukraine, both through kinetic and cyber-attacks. Russia has continued and increased its deliberate cyber-attacks on energy critical infrastructure as part of its hybrid war, from a DDOS attack on a Kyiv gas company in October to one on a Ukrainian heat provider in August [9].

Step by step, Russia has used hybrid warfare to challenge energy security, not just in Ukraine, but across NATO member states as Russia seeks to beat back NATO influence and expand its power on the world stage. Now escalating into 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. Lithuania, Latvia, Poland and Romania and Central European states such as Germany continue to be targeted.

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 both 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, Turkey and Greece have critical infrastructure strongly tied to China and Russia. This dependence is already causing energy insecurity. And Western and Central Europe, with its up-till-now reliance on Russia oil and gas, is now involved in a cyber, information, and economic war which has rattled markets and caused gas and oil prices to soar to historic levels not seen since the 1970s.

Cyber-attacks 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 those countries. China's malign investments in Southern and Mediterranean Europe, is enabling Beijing to control some NATO member states' energy critical infrastructure at a critical moment in the global balance of power (see Country Case Studies in Ref. [10]).

B.1.2 Finding Two

Malign Influence is Directly Impacting Energy Critical Infrastructure

Digital democracies, which respect individual freedoms and openness, have been targets for malign influence campaigns. Hybrid activities, including cyber-attacks and disinformation campaigns, are attractive tools for state and non-state actors to achieve political objectives without military force [11]. Russia views cyber-attacks, hacking, and the spread of disinformation as instruments of foreign policy and security interests.

Russia also conducts information operations to spread disinformation and promote narratives aligned with Russian security interests [12]. 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 targeted 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 [13].

Russia's disinformation apparatus is active in Poland's energy sector. In March 2021, after Poland announced its strategic partnership with the US 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 [14].

Another recent example is the fate of Chevron's shale exploration in Romania, which received strong and unexpected local opposition, ostensibly based on environmental concerns. It was later determined that this opposition was funded by the Kremlin [15]. Finally, there is the question of ownership of European energy assets by Kremlin-affiliated companies. This lack of visibility into these actions presents questions of Russian influence and possible interference on critical energy assets within NATO member states.

B.1.3 Cyber Mitigation Strategies for Critical Energy Infrastructure

The SAS-163 cyber team identified three potential solutions to mitigate cyber-attacks and increase energy independence for militaries of NATO member states and to prevent cyber vulnerabilities to energy critical infrastructure. These options include new Cyber Early Warning Systems (CEWS) that include virtual modelling, small modular reactors and microgridding.

Solution One: Cyber early warning systems that include virtual modelling of energy critical infrastructure for early mitigation of malicious intrusions is 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 cyber-attacks. By using the virtual model of a natural gas pipeline and combining it with machine learning, cyber-attacks can be identified early and mitigated. Threat intelligence modelling and identification systems, based on heterogeneous information networks that use cyber entanglement capabilities are also helpful in this effort. The modelling 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 implementation of successful prototypes, grids, gas pipelines and other energy sources can be more adequately protected from cyber-attacks. Any CEWS development must be in addition to anomaly detection monitoring in critical energy infrastructure.

Solution Two: Small modular reactors (SMRs) are advanced nuclear reactors that have a power capacity of up to 300 MW(e) per unit, which is about one-third of the generating capacity of traditional nuclear power reactors. Given their smaller footprint, SMRs can be used on locations not suitable for larger nuclear power plants. SMRs offer savings in cost and construction time, and they can be deployed by NATO states incrementally to match increasing energy demand.

In areas lacking sufficient lines of transmission and grid capacity, SMRs can be installed by militaries into an existing grid or remotely off-grid, as a function of its smaller electrical output, providing necessary energy for military, industry, and the population. SMRs have reduced fuel requirements. Power plants based on SMRs may require refuelling only every three to seven years, in comparison to between one and two years for conventional nuclear plants. Some SMRs are designed to operate for up to 30 years without refuelling. 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 SMR between NATO nations is the recent intergovernmental agreement between Romania and the United States signed December 2020 for the US 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 be deployed in the Baltics, Poland, Bulgaria, Turkey, and Greece as well [16]. A more complete analysis of SMR will be included in the final report.

Solution Three: Microgrids are another alternative source of energy 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. However, they often need a lead time of several years to model, install and to produce enough independent energy in the case that it must be decoupled from a grid as they must be suited to each installations' unique infrastructures and energy needs.

Microgrids have had success on US bases such as the Marine Corps Air Station Miramar in San Diego, the Otis Air National Guard Base, and the Parris Island microgrid at the US Marine Corps Recruit Depot [17]. Before these success stories can be transferred to other US military installations in Europe or North America, however, a few considerations must be made. 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. At the same time, European militaries are actively developing prototype systems for mobile military camps, however, these often lack cybersecurity considerations in the design [18].

Solution Four: Countering Malign Influence through a Disinformation Rapid Response Force. Early detection of disinformation campaigns is crucial to prevent malicious actors from escalating and exploiting this activity. Because of its ubiquity and importance in virtually all sectors of modern society, critical energy infrastructure is a natural target for malign actors [19]. Additionally, the immediacy of this threat, weaponized by modern technology and mass media, requires near-instantaneous response. 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 their nascent stages. This task force could be staffed by local credible actors with a strong presence at the community level. Their focus would be on building a network to ensure that every state is able to evaluate disinformation from different perspectives. This 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.

Malign influence is not limited to communication channels, but to long-term investment by hostile actors as well. There is a need for greater accountability for hostile investors, particularly when this external interest targets NATO member state critical energy infrastructure. Where necessary, stronger parliamentary approval should be considered based on national security assessments. An example of how this process is addressed in the US is The Committee on Foreign Investment in the United States (CFIUS), which is an interagency committee chaired by the Department of the Treasury and is responsible for reviewing foreign investments in, or acquisitions of, US businesses and real estate to determine if the transaction threatens to impair US national security.

B.1.4 Bibliography

Abrams, M. "Malicious Control System Cyber Security Attack Case Study–Maroochy Water Services, Australia." 3 July 2008. https://www.mitre.org/sites/default/files/pdf/08_1145.pdf.

AL Arabiya with AFP. "Saudi Aramco Says Cyber-Attack Targeted Kingdom's Economy." Al Arabiya News, 9 December 2012. https://www.thecre.com/fisma/?p=4177

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

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

Butrimas, V. “National Security and International Policy Challenges in a Post Stuxnet World.” Lithuanian Annual Strategic Review. 2014, 11-32. https://www.researchgate.net/publication/271726264_National_Security_and_International_Policy_Challenges_in_a_Post_Stuxnet_World

Crozier, R. “Maersk Had to Reinstall all IT Systems after NotPetya Infection.” ITNews., 25 January 2018.

Demchak, C. and Dombrowsky, P. “Rise of a Cybered Westphalian Age.” Strategic Studies Quarterly, Spring 2011, 32-61. https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-05_Issue-1/Demchak-Dombrowski.pdf

Dragos, Inc. “SolarWinds Compromise and ICS/OT Networks Webinar Recording.” 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

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

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

Greenberg, A. “The Untold Story of NotPetya, the Most Devastating Cyberattack in History.” Wire, 22 August 2018. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Healey, J., and Jervis, R. “The Escalation Inversion and Other Oddities of Situational Cyber Stability.” Texas National Security Review, 3(4) Fall 2020, 30-53. https://tnsr.org/2020/09/the-escalation-inversion-and-other-oddities-of-situational-cyber-stability/

Infracritical. “Debate over IT, OT and Control Systems.” 22 November 2019. http://icsmodel.infracritical.com/

Kirk, K. “Latest Ransomware Wave Never Intended to Make Money.” Data Breach Today. 29 June 2017. https://www.databreachtoday.com/latest-ransomware-wave-never-intended-to-make-money-a-10069

Krebs, B. “Cyber Incident Blamed for Nuclear Power Plant Shutdown.” The Washington Post. June 5, 2008. http://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958.html

Langner, R. “To Kill a Centrifuge: A Technical Analysis of What Stuxnet’s Creators Tried to Achieve.” Langner Group. 2013. https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf

Lee, R. Assante, M. and Conway, T. “German Steel Mill Cyber Attack, ICS Defence Use Case (DUC).” Dec 30 2014. SANS ICS 2014. https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf

Lee, R., Assante, M., and Conway, T. “Analysis of the Cyber Attack on the Ukrainian Power Grid.” SANS 2016. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

Lloyds and Cambridge University. “Business Blackout: The Insurance Implications of a Cyber-Attack on the US Power Grid.” Lloyds 2015. https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-lloyds-business-blackout-scenario.pdf

Pagliery, J. “The Inside Story of the Biggest Hack in History.” CNN Business, 2015. https://money.cnn.com/2015/08/05/technology/aramco-hack/

Perlroth, N. and Krauss, C. “A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try.” The New York Times, 15 March 2018. https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html

Perlroth, N. “Russian Hackers Targeting Oil and Gas Companies.” The New York Times, 30 June 2014. http://www.nytimes.com/2014/07/01/technology/energy-sector-faces-attacks-from-hackers-in-russia.html?_r=2

Prebs, B. “Cyber Incident Blamed for Nuclear Power Plant Shutdown.” The Washington Post, June 5, 2008. https://www.homelandsecuritynewswire.com/cyber-mishap-causes-nuclear-power-plant-shutdown

Sanger, D. and Perlroth, N. “U.S. Escalates Online Attacks on Russia’s Power Grid.” The New York Times, 15 June 2019. https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html?auth=login-google

Schneier, B. “The US Has Suffered a Massive Cyberbreach. It’s Hard to Overstate How Bad It Is.” The Guardian, 23 December 2020. https://amptheguardiancom.cdn.ampproject.org/c/s/amp.theguardian.com/commentisfree/2020/dec/23/cyber-attack-us-security-protocols

Schwartz, M. “Ukraine Power Supplier Hit by WannaCry Lookalike.” June 30, 2017. http://www.inforisktoday.com/ukraine-power-supplier-hit-by-wannacry-lookalike-a-10071. June 30, 2017.

Slovik, J. “CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack.” Dragos Inc. 2019. https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf

Slowik, J. “Spyware Stealer Locker Wiper: Lockergoga Revisited.” Dragos 2020. https://pylos.co/wp-content/uploads/2020/04/Spyware_Stealer_Locker_Wiper-_LockerGoga_Revisited.pdf

Smith, R. “U.S. Seizure of Chinese-Built Transformer Raises Specter of Closer Scrutiny.” The Wall Street Journal, 27 May 2020. https://www.wsj.com/articles/u-s-seizure-of-chinese-built-transformer-raises-specter-of-closer-scrutiny-11590598710

Stone, J. “Norsk Hydro’s Cyber Insurance Has Paid Just a Fraction of Its Breach-Related Losses So Far.” Cyberscoop, 28 October 2019. https://www.cyberscoop.com/cyber-insurance-norsk-hydro-lockergoga-attack/

Symantec. “Dragonfly: Cyber Espionage Attacks Against Energy Suppliers.” Symantic 2014, 3. https://web.archive.org/web/20150206103228/http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf

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

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

U.S. Cybersecurity and Infrastructure Security Agency. “ICS Advisory (ICSA-14-178-01).” 30 June 2014. https://us-cert.cisa.gov/ics/advisories/ICSA-14-178-01

Zetter, K. “SolarWinds Hack Infected Critical Infrastructure, Including Power Industry.” The Intercept, 24 December 2020. https://theintercept.com/2020/12/24/solarwinds-hack-power-infrastruct

B.2 MALIGN INFLUENCE AND THE UKRAINE INVASION

Dr. Georgios Giannoulis and Dr. Erin Hodges

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 offers better oversight and remote accessibility but introduces potential vulnerabilities to malicious activities such as hybrid threats.

According to The Landscape of Hybrid Threats: A Conceptual Model, "Hybrid threat can be characterized as coordinated and synchronized action, that deliberately targets the systemic vulnerabilities of democratic states and institutions through a wide range of means. Activities exploit the thresholds of detection and attribution as well as the border between war and peace" [20].

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

The diagram in Figure B-1 shows how 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 on actions. Unlike traditional operational plans, the attacker is relieved of the stress and cost of gathering and consuming resources at a specific time and place, as the targeted Centre of Gravity, "the source of power that provides moral or physical strength, freedom of action, or will to act, can be shifted in time" [21].

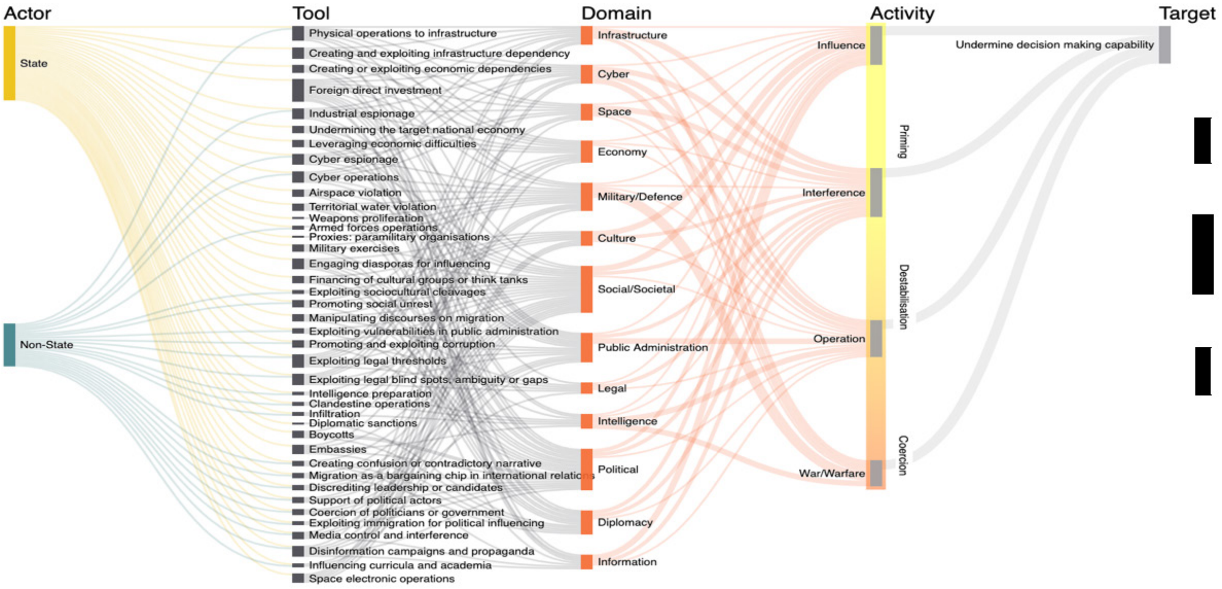

Actor
Tool
Domain
Activity
Target
State
Non-State
Physical operations to infrastructure
Creating and exploiting infrastructure dependency
Creating or exploiting economic dependencies
Foreign direct investment
Industrial espionage
Undermining the target national economy
Leveraging economic difficulties
Cyber espionage
Cyber operations
Airspace violation
Territorial water violation
Weapons proliferation
Armed forces operations
Proxies: paramilitary organisations
Military exercises
Engaging diasporas for influencing
Financing of cultural groups or think tanks
Exploiting sociocultural cleavages
Promoting social unrest
Manipulating discourses on migration
Exploiting vulnerabilities in public administration
Promoting and exploiting corruption
Exploiting legal thresholds
Exploiting legal blind spots, ambiguity or gaps
Intelligence preparation
Clandestine operations
Infiltration
Diplomatic sanctions
Boycotts
Embassies
Creating confusion or contradictory narrative
Migration as a bargaining chip in international relations
Discrediting leadership or candidates
Support of political actors
Coercion of politicians or government
Exploiting immigration for political influencing
Media control and interference
Disinformation campaigns and propaganda
Influencing curricula and academia
Space electronic operations
Infrastructure
Cyber
Space
Economy
Military/Defence
Culture
Social/Societal
Public Administration
Legal
Intelligence
Political
Diplomacy
Information
Influence
Interference
Operation
War/Warfare
Priming
Destabilisation
Coercion
Undermine decision making capability
[redacted]
[redacted]
[redacted]

Figure B-1 Diagram of the Conceptual Model. From Giannopoulos et al., The Landscape of Hybrid Threats: A Conceptual Model. Used with Permission.

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

B.2.1 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 that is circulated in isolated and mostly in interdependent networks around the globe. Internet, 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 a fertile ground to state actors, non-sate actors or even 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, which can be processed individually or studied in correlation with similar samples taken in different time periods. This is a way of revealing and learning multi-level behavioural patterns of the target state and gaining intelligence, while at the same time reducing the chance of detection.

B.2.2 Cascading Effects

In a multi-dimensional space of action, the hybrid actor sets up his operational plan, driven by systemic vulnerabilities and exposures of his target. 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 the hybrid actor to exploit more domains by engaging diverse tools, in synchronized and coordinated actions, which can be used as a force multiplier in the field.

B.2.3 Influence and Disinformation

According to Figure B-1, influence is a low intensity activity in which a hybrid actor has the chance to act in a “grey zone,” remaining under the threshold of detection and attribution. Influence is usually a prolonged process and effective as well, 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 that 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” [22].

In the energy era, we have experienced how coordinated disinformation campaigns target energy diversification [23] 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 nuclear accident have impacted conversations about energy diversification. In addition, instrumentalizing ideological active organizations who fight for environment protection against hazardous materials and the proliferation of nuclear power installations could be considered as a coordinated information activity towards the same goal [24].

B.2.4 The Russian Invasion of Ukraine

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 networks to further its invasion while attempting to divide Western powers. While it should be noted that this invasion has had a unifying effect on most of NATO and the EU, it has also identified some 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, which warrants a higher risk of Russian hybrid attacks in the NATO bloc.

The role of Russian disinformation in conjunction with the war has played out very differently than it has in the past. Much of this 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 disinformation of the Kremlin has been focused on Russian nationals and the Russian-speaking diaspora in neighbouring 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 that its military was conducting defensive operations, as opposed to an offensive invasion of its neighbour. 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 [25]. 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 to mislabel NATO as an aggressor towards Russia and Ukraine [26].

The cohesive efforts by both governments and corporations in the US 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, it is much more difficult for the Russian regime to narrate international events falsely. Furthermore, this information warfare has not done what the Russians usually do best: capitalize on pre-existing divisions within nations and organizations. This has proven to be to 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, both 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 [27].

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 protestors have been arrested. In early March, draft legislation proposed that anti-war protestors could be conscripted into military service [28]. Moreover, Russia’s own considerable disinformation networks have turned almost 90% of their efforts inward [29]. There is no viable way to accurately measure the efficacy of these efforts while so little information is coming in 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 both unaware of the truth and hostile towards Western states because of hardships their own government caused. Moreover, a population of misled citizens could prove to provide Russia with more vectors for disinformation in much the same way that it incentivizes hackers without necessarily employing them.

The success of the Western world in the light of a 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 doesn't only occur in information spaces. The invasion of Ukraine has highlighted that a hostile actor can leverage economic and infrastructural investment to further its own needs. Diverse supply chains will diminish this effect.

B.2.5 Recommendations

Some of the following measures could be suggested to safeguard the credibility of the information against malicious influential activities:

B.2.5.1 Create 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 their 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 that every state is able to evaluate disinformation from multi-national and multi-cultural perspectives to determine identity and motives of the perpetrator 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 a local, state, national or international level.

B.2.5.2 Shape the Legal and Regulatory Framework of Media Platforms

Although many countries have established such 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 along with the 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 [30].

B.2.5.3 Diversification of Supply Chains

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

B.2.5.4 Educate 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 nowadays where the majority of the information is provided through social media. It is a culture that must be acquired from the early stages of education so that it can be assimilated more easily in the future. Hence, due to the digitalization of learning methods, it would be advisable that children should be taught the methodology and the value of analysing and exploiting the content of information through the web. The Council of Europe has advocated for the promotion of media literacy through its European Media Literacy Week since 2019 and 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 both children and adults. The most convenient and easy way to protect from disinformation is by following a diversity of people or groups and perspectives not only on the website, but also in the traditional media. Relying upon limited biased news and resources increases the odds of falling victim to false rumours [31].

In conclusion, although many practices for countering malign information exist, it is questionable whether and to what extent they can be applied. Surveillance and censorship of journalists opposes many of the fundamental principles of democracy, such as freedom of speech, expression, and 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 be dominant in the global market. Instead, NATO nations must work to candidly analyse areas of influence dominated by hostile actors and build contingency plans to address those areas of weakness.

B.2.6 Bibliography

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

Colomina, C., Margalef, H.S. and Youngs, R. "The Impact of Disinformation on Democratic Processes and Human Rights in the World." European Parliament. April 2021. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653635/EXPO_STU(2021)653635_EN.pdf

DoD Dictionary of Military and Associated Terms. August 2021.

Domo. "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

European Commission. "Tackling Disinformation Online." 23 February 2022. https://digital-strategy.ec.europa.eu/en/policies/online-disinformation

Giannopoulos, G., Smith, H. and Theocharidu, M. "The Landscape of Hybrid Threats: A Conceptual Model." 2021.

Hybrid CoE. "Countering Disinformation: News Media and Legal Resilience." Apr 2019.

Krol, A. "Information Warfare Against Strategic Investments in the Baltic States and Poland." The Warsaw Institute Review, 19 July 2017. https://warsawinstitute.org/information-warfare-strategic-investments-baltic-states-poland/

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

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

Ukrinform. "A Digest of Russia Propaganda for May 31." Center for Strategic Communications – Ministry of Culture and Information Policy of Ukraine. June 1, 2022.

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

B.3 MITIGATIONS – A NEW GENERATION OF CYBER EARLY WARNING SYSTEMS

Dr. Gabriel T. Raicu and Dr. Sarah J. Lohmann

Cyber early warning systems predicting malicious intrusions on Energy Critical Infrastructure can make a major contribution to preventing attacks at an Alliance level. Early Warning Systems for Cyber Defence in Energy Security are vital to ensuring NATO's medium- and long-term goals. This section first identifies the challenges with predicting today's cyber-attacks. It then analyses the limitations of current Cyber Early Warning Systems (CEWS). Finally, it proposes a new generation of EWS that is having success due to its virtualization of energy critical infrastructure and effective use of Artificial Intelligence.

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 pre-emptive action against real or virtual aggressors. Most current Early Warning Systems are not adequate to repel cyber-attacks on energy critical infrastructure in the emerging technology environment.

The design and implementation of CEWS includes 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 cyber-attacks. 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 [32].

One of the major problems with older generation EWS is the difficulty 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 [33].

B.3.1 Traditional Cyber EWS Challenges

There are several limitations to classical Cyber Early Warning Systems. Systems that try to monitor network status and detect new network threats and anomalies have a number of drawbacks. Global monitoring systems like Network telescopes, which is an Internet system that allows the observation of large-scale network attacks, are based on dark address space with high detection rate of worms, network intrusions, etc. However, focused attacks are difficult to be recognized and attributed in these global systems [34].

Deep Packet Inspection (DPI) can detect lots of threats and anomalies. However, DPI cannot be scaled at the level of a large-scale network or Internet backbone [35]. Data flows, or reactive programming, is one of the most important sources for information based on the evaluation of sampled flow technology which is not able to provide 100% accurate results [36].

Most IDS systems are limited to evaluating only logs, flows, or packet counts. There is a weakness in the inherent division between network-based and host-based indicators. It is almost impossible to efficiently correlate these disparate data streams.

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 [37].

Finally, 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 System of Artificial Neural Networks, a computational model with processing elements with inputs and outputs based on predefined functions, provide the average False Positive rate percentage of 0.03 [38]. The System is particularly useful in detecting and classification of botnet attacks, as well as analysis of standard cyber traffic, cyber-physical systems traffic, as well real-time traffic analysis.

A modern IDS is also good at detecting regular intrusions but has low efficiency against AI powered adversary 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 own AI to strengthen machine learning against deception technology. This technology relies on strategical 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 [39].

Although the deception system is essentially effective, the defence is generally static, making it easier for the opponent to distinguish over time, using his own AI, a honeypot from a real asset, and defeating the decoy defence.

A few applications provide solutions to the problem of the static defence, 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' behaviour." [40], [41]. DeepDig uses the behaviour of real systems that it mimics by transforming each cyberattack into a training session for IDS system AI capabilities [42].

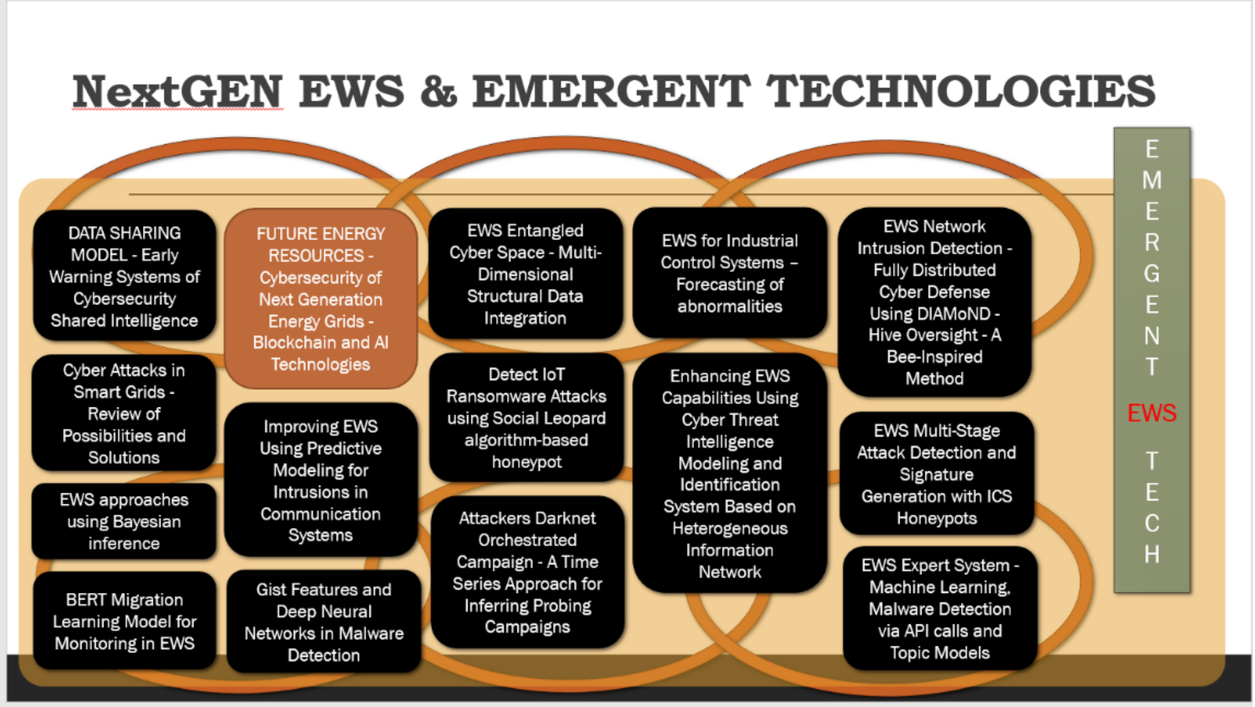
B.3.2 Emergent Technologies Address Hybrid Threats

Classical cyber security 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 behaviour analysis and learning algorithms need to be developed to build the new generation of EWS system.

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 [43]. New architectures, sophisticated network behavioural analysis models – which conduct network monitoring to ensure security – and learning algorithms can be used to build Next Generation EWS (Figure B-2). The goal of this system is also to develop approaches and models for detecting anomalies and behaviours considered within normal limits for systems, sharing information between multiple EWS depending on threat levels. The approach must be holistic, considering the latest general security management initiatives.

This is done by developing new methods for malware detection and behavioural 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 is then interpreted by enhancing distributed analysing capabilities [44]. EWS cybersecurity systems are dependent on the efficiency of the technology and the accuracy of the logic of recognizing a cyber threat.


NextGEN EWS & EMERGENT TECHNOLOGIES

DATA SHARING MODEL - Early Warning Systems of Cybersecurity Shared Intelligence

FUTURE ENERGY RESOURCES - Cybersecurity of Next Generation Energy Grids - Blockchain and AI Technologies

EWS Entangled Cyber Space - Multi-Dimensional Structural Data Integration

EWS for Industrial Control Systems – Forecasting of abnormalities

EWS Network Intrusion Detection - Fully Distributed Cyber Defense Using DIAMoND - Hive Oversight - A Bee-Inspired Method

Cyber Attacks in Smart Grids - Review of Possibilities and Solutions

Detect IoT Ransomware Attacks using Social Leopard algorithm-based honeypot

Enhancing EWS Capabilities Using Cyber Threat Intelligence Modeling and Identification System Based on Heterogeneous Information Network

Improving EWS Using Predictive Modeling for Intrusions in Communication Systems

EWS Multi-Stage Attack Detection and Signature Generation with ICS Honeypots

EWS approaches using Bayesian inference

Attackers Darknet Orchestrated Campaign - A Time Series Approach for Inferring Probing Campaigns

EWS Expert System - Machine Learning, Malware Detection via API calls and Topic Models

BERT Migration Learning Model for Monitoring in EWS

Gist Features and Deep Neural Networks in Malware Detection

Figure B-2 EWS Extended Research Directions and Development Areas Explored by the SAS-163 Scientific Team [45].

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 new areas of constructive approach to EWS.

To increase 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.

Smart grid risks pose a unique challenge to EWS.Smart grid networks tend to replace traditional networks due to the inherent advantages of efficient management and adaptability to transient regimes, reduced back-up requirements, increased resilience and efficiency and self-healing capacity, elasticity in the integration of renewable energy resources, innovative distribution systems to final consumers, etc. [46]. However, there are several 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.

Smart Grids provide a number of cyber vulnerabilities. These 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, unauthorized access by stealing or leaking credentials, false alerts, distorted messages, denial of service, and traffic analysis and network mapping for future exploitation [47].

A holistic approach to detection is vital since attackers can range from non-malicious users who may harm the system out of sheer curiosity, 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 renewable energy sources are being used for sustainability, Blockchain and AI Technologies must be considered as a base for cybersecurity of Next Generation Energy Grids.

Even though renewables' contribution to the energy sector brings many advantages, it also expands the attack surface of the energy grid, which becomes susceptible to cyber-attacks. Advancements in AI and blockchain technologies are helping to address these emerging cybersecurity challenges. In the following, a series of technologies that approach the problem of threat detection and ensuring resilience are reviewed.

B.3.3 Forecasting ICS Abnormalities Through Virtualization

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 cyber-attacks and differentiate them from naturally occurring errors and failures [48]. The system can have a dual role, that of preventing cyber-attacks, and that of early signalling of defects. The signals captured from the monitoring nodes are translated into behaviours using feature discovery techniques. Each characteristic has its own behaviour and well-defined decision limits between normal and abnormal behaviour. A virtual model of the monitored installation such as a power plant is used [49].

State models selected by a cluster Gaussian Mixture Model (GMM) address the problem of characteristic variation over time. This means that not all subpopulation data points are assigned, but the subpopulations can be learned by the model automatically through a probability distribution [50]. As such, it is the fastest algorithm for learning mixture models [50]. 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. This is 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 [51].

One example of a successful use of EWS for Industrial Control Systems is with General Electric's (GE) Digital Ghost, which can protect from malicious cyber-attacks. It was developed at GE's Research Lab [52]. Digital Ghost provides an additional layer of protection by combining Artificial Intelligence and machine learning technologies with sensing and controls to locate and neutralize cyber-attacks. GE used the physics of a natural gas pipeline, creating a Digital Twin, and combined it with machine learning to protect critical infrastructure. In the testing phase, Digital Ghost found and neutralized a cyber-attack in the virtualized operating gas turbine at GE Power's manufacturing facility in Greenville, SC. In validation studies, it has located over 98% of cyber-attacks. However, it has only been able to neutralize them when over 50% of the assets' sensors have already been compromised [52].

B.3.4 Improving Anomaly Detection via Distributed Decision-Making Algorithms

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 quickly detect anomalies, using little memory and using 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 used have a non-parametric, fully distributed coordination framework that translates the biological success of these methods into similar operations useful in cyber defence [53].

B.3.5 EWS Based on Entangled Cyber Space

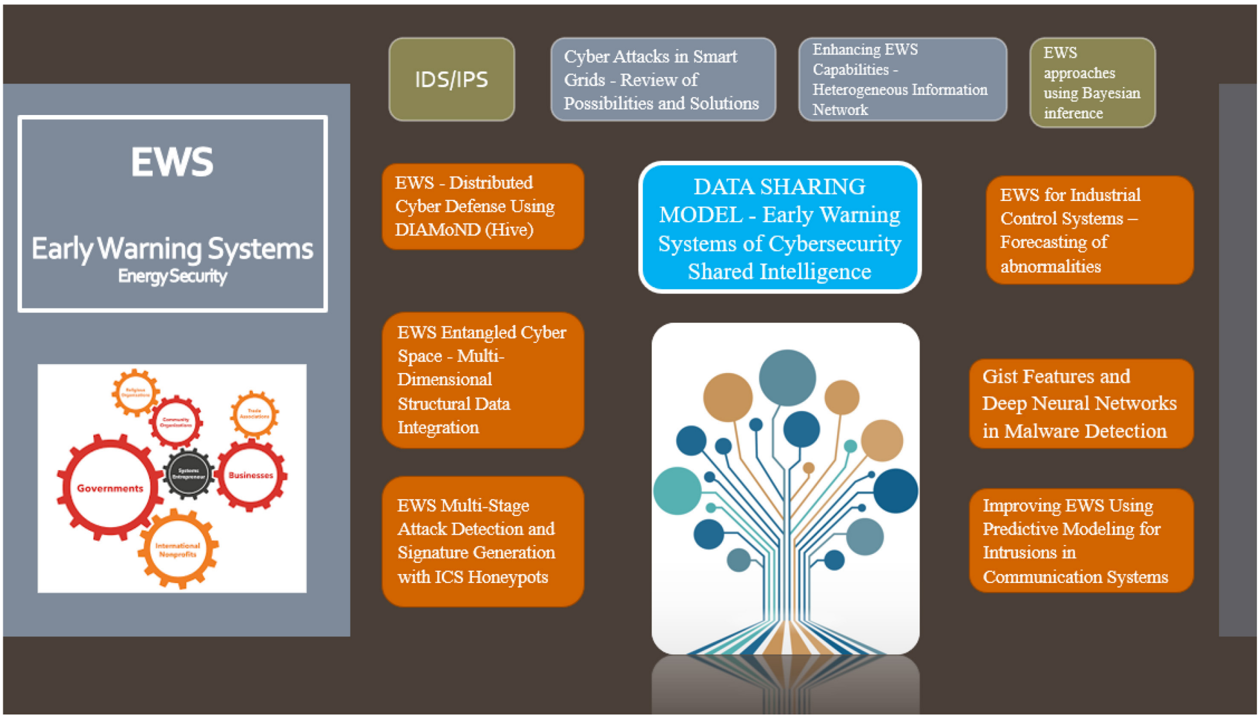
The major challenge of cyber defence is the inefficiency of counteracting the sophisticated attacks of opponents given the interconnection of modern societies at the level of physical and cyber events. To counteract the effects of this situation, it is necessary to build proactive cyber defence models that consider the interconnection and relations between events and activities in the physical, social, media and economic realities of cyberspace [54]. The concept of proactive cyber defence models can use entanglement principles to overcome loosely connected events. Entangled cyberspace is an integrated approach for predicting cyber-attacks. It can provide a solid foundation for building proactive cyber defence models in a seemingly tangled space where there are always major correlations between the physical and the cyber environment [55].

To generate an efficient early warning system component, continuously adaptable to multi-dimensional realities and with advanced prediction capabilities, an analytical framework of cyber analysis must be introduced. This achieves the intersection and correlation of events from multiple physical, social, economic, and virtual layers [56].

B.3.6 EWS Capabilities Using Heterogeneous Information Networks

Open exchange of Cyber Threat Information (ITC) provides a complete real-time picture of the cyber threat situation. One mandatory step is to design a meta schema of threat information to describe the semantic relationship of the infrastructure nodes, and in second step, to model information about cyber threats on a Heterogeneous Information Network (HIN) is mandatory [57]. To do this, 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. The Alliance's security is only as strong as its protection of the energy sector. Any disruption affects the continuity of the supply chain and the effectiveness of the defence. 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 defence 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 through hardened AI and the use of virtualization of energy critical infrastructure can make the difference between pre-emptive efficiency and merely reactive measures if old generation EWS continues to be used. These new generation EWS should be used in Allied exercises to improve logistic support and integrated infrastructures. Dual-use critical infrastructures for energy, transport on land, in the air and on water and cyber can be modelled and simulated using virtualization and Artificial Intelligence which uses Machine Learning for increasingly accurate results. This ought to significantly increase the accessibility of energy supplies and the timely and effective military mobility to all contributing NATO nations in a broad spectrum of operational contexts (Figure B-3).



EWS

Early Warning Systems

Energy Security

IDS/IPS

Cyber Attacks in Smart Grids - Review of Possibilities and Solutions

Enhancing EWS Capabilities - Heterogeneous Information Network

EWS approaches using Bayesian inference

EWS - Distributed Cyber Defense Using DIAMoND (Hive)

DATA SHARING MODEL - Early Warning Systems of Cybersecurity Shared Intelligence

EWS for Industrial Control Systems – Forecasting of abnormalities

EWS Entangled Cyber Space - Multi-Dimensional Structural Data Integration

Gist Features and Deep Neural Networks in Malware Detection

EWS Multi-Stage Attack Detection and Signature Generation with ICS Honeypots

Improving EWS Using Predictive Modeling for Intrusions in Communication Systems

Figure B-3 EWS Emergent Technology Research Directions in the Medium Term by the SAS-163 Scientific Team [58].

B.3.7 Bibliography

Abbaszadeh, M., Mestha, L. and Yan, W. “Forecasting and Early Warning for Adversarial Targeting in Industrial Control Systems.” 2018 IEEE Conference on Decision and Control (CDC).

Arrowsmith, D.K., Mondrag, R. and Woolf, M. “Data Traffic, Topology and Congestion.” Complex Dynamics in Communication Networks. Springer. 2005, 127-157.

Ayoade G., Araujo, F., Al-Naami, K., Hamleen, K.W. et al., “Automating Cyberdeception Evaluation with Deep Learning.” University of Texas at Dallas, IBM Research. Proc. 53rd Hawaii Int. Conf. System Sciences (HICSS). January 2020. https://www.researchgate.net/publication/337287036_Automating_Cyberdeception_Evaluation_with_Deep_Learning

Ayoade, G., Al-Naami, K., Gao, Y., Hamlen, K.W. and Khan, L. “Improving Intrusion Detectors by Crook-Sourcing.” Proceedings of the 35th Annual Computer Security Applications Conference. December 9, 2019. https://www.semanticscholar.org/paper/Improving-intrusion-detectors-by-crook-sourcing-Ayoade-Al-Naami/fef9e447174994c10b359bb1934d19c7c6e4fe9b?p2df

Barnett et al., “19th ICCRTS: C2 Agility : Lessons Learned from Research and Operations Paper 081: Using Causal Models to Manage the Cyber Threat to C2 Agility: Working with the Benefit of Hindsight,” Int. Command Control Res. Technol. Symp., 2014.

Biskup, J, Hömmerli, B., Meier, M., Schmerl, S., Tölle, J. and Vogel, M. “2.08102 Working Group – Early Warning Systems.” Perspectives Workshop: Network Attack Detection and Defence, ser. Dagstuhl Seminar Proceedings, G. Carle, F. Dressler, R.A. Kemmerer, H. König, and C. Kruegel, eds., no. 08102. Dagstuhl, Germany: Schloss Dagstuhl – Leibniz-Zentrum fuer Informatik, Germany, 2008. http://drops.dagstuhl.de/opus/volltexte/2008/1493

Horner, K., “Computer Scientists’ New Tool Fools Hackers into Sharing Keys for Better Cybersecurity.” https://cs.utdallas.edu/cs-new-tool-fools-hackers-cybersecurity/

CORDIS, Worldwide Observatory of Malicious Behaviours and Attack Threats, https://cordis.europa.eu/project/id/216026

Debar, H. “Sticky: March 2008 Archives.” WOMBAT Project. March 19, 2008. https://wombat-project.eu/sticky/2008/03/

Demertzis, K., Tsiknas, K., Takezis, D. 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.” https://arxiv.org/ftp/arxiv/papers/2102/2102.08411.pdf

Dupuy, A., “Energy Security is Critical to NATO’s Black Sea Future.” Atlantic Council. May 12, 2022. https://www.atlanticcouncil.org/blogs/turkeysource/energy-security-is-critical-to-natos-black-sea-future

“FIDeS.” Universität Bremen. https://www.informatik.uni-bremen.de/~sohr/FIDeS/index_e.htm

Raicu, G. and Lohmann, S. “Energy Security in the Era of Hybrid Warfare.” SAS-163 Research Project Annual Workshop, December 2021, Project EWS Concepts, Oberammergau, Germany.

Gao, Y., Li, X., Peng, H., Fang, B., and Yu, P. HinCTI: “A Cyber Threat Intelligence Modelling and Identification System Based on Heterogeneous Information Network,” February 1, 2022, IEEE Xplore, https://ieeexplore.ieee.org/document/9072563

“Gaussian Mixture Models.” Scikit-learn: Machine Learning in Python, Pedregosa et al., JMLR 12, 2825-2830, 2011. https://scikit-learn.org/stable/modules/mixture.html

General Electric Research, “Digital Ghost: Real-Time, Active Cyber Defence”. Digital Ghost: Real-Time, Active Cyber Defence, GE Research.

General Electric Research. “Digital Ghost: Real-Time, Active Cyber Defence.” Digital Ghost: Real-Time, Active Cyber Defence, GE Research.

Golling, M. and Stelte, B. “Requirements for a Future EWS – Cyber Defence in the Internet of the Future.” 3rd International Conference on Cyber Conflict. 2011. https://www.digar.ee/arhiiv/en/download/107746

Gyanfi, E., and Jurcut, A. “Intrusion Detection in Internet of Things Systems: A Review on Design Approaches Leveraging Multi-Access Edge Computing, Machine Learning, and Datasets.” 2022. https://www.mdpi.com/1424-8220/22/10/3744/pdf?version=1652517852

Hwang, K., Kulkareni, S. and Hu, Y. “Cloud Security with Virtualized Defence and Reputation-Based Trust Management.” Dependable, Autonomic and Secure Computing, 2009. DASC ‘09. Eighth IEEE International Conference on, 717-722, Dec 2009.

Ikwu, R. “Multi-Dimensional Structural Data Integration for Proactive Cyber-Defence.” IEEE International Conference on Cyber Situational Awareness, Data Analytics and Assessment, 2017.

Ikwu, R.E. The Entangled Cyberspace: An Integrated Approach for Predicting Cyber-Attacks. [Great Britain]: Brunel University London, 2018.

Korkzy’sky, M., Huh J., Hamieh A. and Holm H. “DIAMoND: Distributed Intrusion/Anomaly Monitoring for Nonparametric Detection.” Research Gate. https://www.researchgate.net/publication/278018275_DIAMoND_Distributed_IntrusionAnomaly_Monitoring_for_Nonparametric_Detection

Kumara H., Shaikh, S., Lee, C. and Sung, F. "Towards an Early Warning System for Network Attacks Using Bayesian inference." 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing, Faculty of Engineering, Environment & Computing Coventry University, United Kingdom. https://ieeexplore.ieee.org/document/7371513

Mann, V., Vishnoi, A. and Bidkar, S. "Living on the Edge: Monitoring Network Flows at the Edge in Cloud Data Centers." IBM Research. https://www.inf.ufpr.br/aldri/disc/artigos/2014/patrick_art2.pdf

Mattioli, R. and Moulinos, K. "Communication Network Interdependencies in Smart Grids." European Union Agency for Network and Information Security (ENISA), 2015. https://Www.Enisa.Europa.Eu/Publications/Communication-Network-Interdependencies-In-Smart-Grids/@@Download/Fullreport

Mazurowski, M.A., Habas, P.A., Zurada, J.M., Lo, J.Y., Baker, J.A. and Tourassi, G.D. "Training Neural Network Classifiers for Medical Decision Making: The Effects of Imbalanced Datasets on Classification Performance." Neural Networks, 21(2-3), 2008, 427-436. ISSN 0893-6080. DOI: 10.1016/j.neunet.2007.12.031.https://doi.org/10.1016/j.neunet.2007.12.031.

Pal, K. "10 Ways Virtualization Can Improve Security." Technopedia. October 22, 2021. https://www.techopedia.com/2/31007/trends/virtualization/10-ways-virtualization-can-improve-security

Raicu, G. and Lohmann, S. "Energy Security in the Era of Hybrid Warfare." SAS-163 Research Project, April 2022, Project EWS Concepts in the Medium Term.

Seker, E. "Use of Artificial Intelligence Techniques/Applications in Cyber Defence." NATO CCD-COE, 2019, https://arxiv.org/pdf/1905.12556

Song, W., Beshley, M., Przystupa, K. et al., "A Software Deep Packet Inspection System for Network Traffic Analysis and Anomaly Detection." 2020. https://www.researchgate.net/publication/340013171_A_Software_Deep_Packet_Inspection_System_for_Network_Traffic_Analysis_and_Anomaly_Detection

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

Abbaszadeh, M., and Mestha, L.K. United States Patent Application 20200067969, "Situation Awareness And Dynamic Ensemble Forecasting of Abnormal Behavior In Cyber-Physical System," General Electric Company, February 27 2020. https://www.freepatentsonline.com/y2020/0067969.html

Vu T., Nguyen, B., Cheng, Z., Chow, M. and Zhang, B. "Cyber-Physical Microgrids: Toward Future Resilient Communities." IEEE Xplore. September 24, 2020. https://ieeexplore.ieee.org/document/9205672

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

"Worldwide Observatory of Malicious Behaviours and Threats." CORDIS. July 15, 2019. https://cordis.europa.eu/project/id/216026/it

Yadav, S., Kumar, S., Sharma, S. and Singh, A. "A Review of Possibilities and Solutions of Cyber Attacks in Smart Grids." 1st International Conference on Innovation and Challenges in Cyber Security. 2016.

B.4 MILITARY INSTALLATIONS AND MICROGRIDS: MOVING TOWARD CYBER-SECURE ENERGY INDEPENDENCE?

Dr. Sarah J. Lohmann

This section discusses the immediate threat to energy security on military installations in Europe posed both by shortages and cyber-attacks 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 back-up capability in the interim.

B.4.1 The Problem

Cyber-attacks 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's 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 Defence on the use of foreign grids for US bases operating OCONUS which "strongly recommended that every U.S. 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" [59]. 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 hacking campaigns in Europe [60], [61], [62]. 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 is largely because cybersecurity applications have not yet been created for the new emerging technology systems being integrated with energy critical 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 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 [63]. It is worth mentioning Germany as a case study in Russia's penetration tactics here, 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 [64]. In addition, there are 173,741 German Bundeswehr soldiers, with all but around 3,000 of those serving in Germany [65], [66]. 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 (https://www.cytomic.ai/alerts/berserk-bear-cyberattacks/) malicious cyber activities, from attacking a number of energy companies and attempting to intrude on Germany's grid (https://intelnews.org/2018/06/21/01-2342/)in 2017, to its long-term efforts (https://www.cyberscoop.com/german-intelligence-memo-berserk-bear-critical-infrastructure/) to compromise the supply chain of critical infrastructure such as energy, water and power sectors up to the present time [67]. Germany's intelligence services have warned that the group's intension was to imbed malware permanently in IT networks, but also to gain access to OT networks. The same group conducted an intelligence gathering campaign on US energy companies, and targets industrial networks [68]. The problem is compounded when a grid is aging or has lack of energy supply, as is the case in several NATO countries, including Germany. Germany's Interior Ministry's Federal Audit found in 2021 that it is at heightened risk of grid black-outs through 2025 [69]. This is due to an aging grid and the energy shortfall as renewables are not producing enough energy to make up for nuclear plants being taken offline and coal needing to be phased out in line with Germany's green energy goals.

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 cyber- attacks against Germany's wind energy companies. This has caused one 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 offline all-together [70], [71].

For US military installations, which depend on Germany's unreliable grid, and which have seen a 30% 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, and how often, and for how long. Back-up 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, which should be prepared for grid black-outs to affect operations in the next 6 months to two years. A recent report by Microsoft's digital Security Unit show that Russia-aligned cyber threat groups were preparing to target organizations allied with Ukraine as early as March of 2021. In fact, 93% 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 [72]. More than 40% of the Russian-backed destructive cyber-attacks were on Ukraine's critical infrastructure sector, including nuclear and transportation [72]. Knowing that 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.

B.4.2 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.

B.4.3 Assessment of Current Military Installation Microgrid Efforts

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, cost-saving, and environmental advantages. In fact, while the US Navy plans for all of its major installations to operate off the grid for two weeks by 2025 due to its microgrid implementation, the US Army just announced a plan in Feb. 2022 for each of its 130 bases worldwide to have a microgrid by 2035 [73]. 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 [74].

However, for the purposes 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, the section begins by examining 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 cyber-secure. To answer this question, several case studies will be examined.

At the Marine Corps Air Station at Miramar in San Diego, 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 black-out, 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 [75]. 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 energy sources, such as wind turbines [76]. It was also supposed to test cyber-secure protection and operation of the grid while islanding. While Otis Air National Guard Base Microgrid was able to establish a cyber-secure 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 the use of only one back-up generator being allowed to be used per building or mission, and the single generators experienced power surges beyond what they could handle [77]. If renewables are unable to be utilized while islanded with its microgrid, and cyber-secure 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.

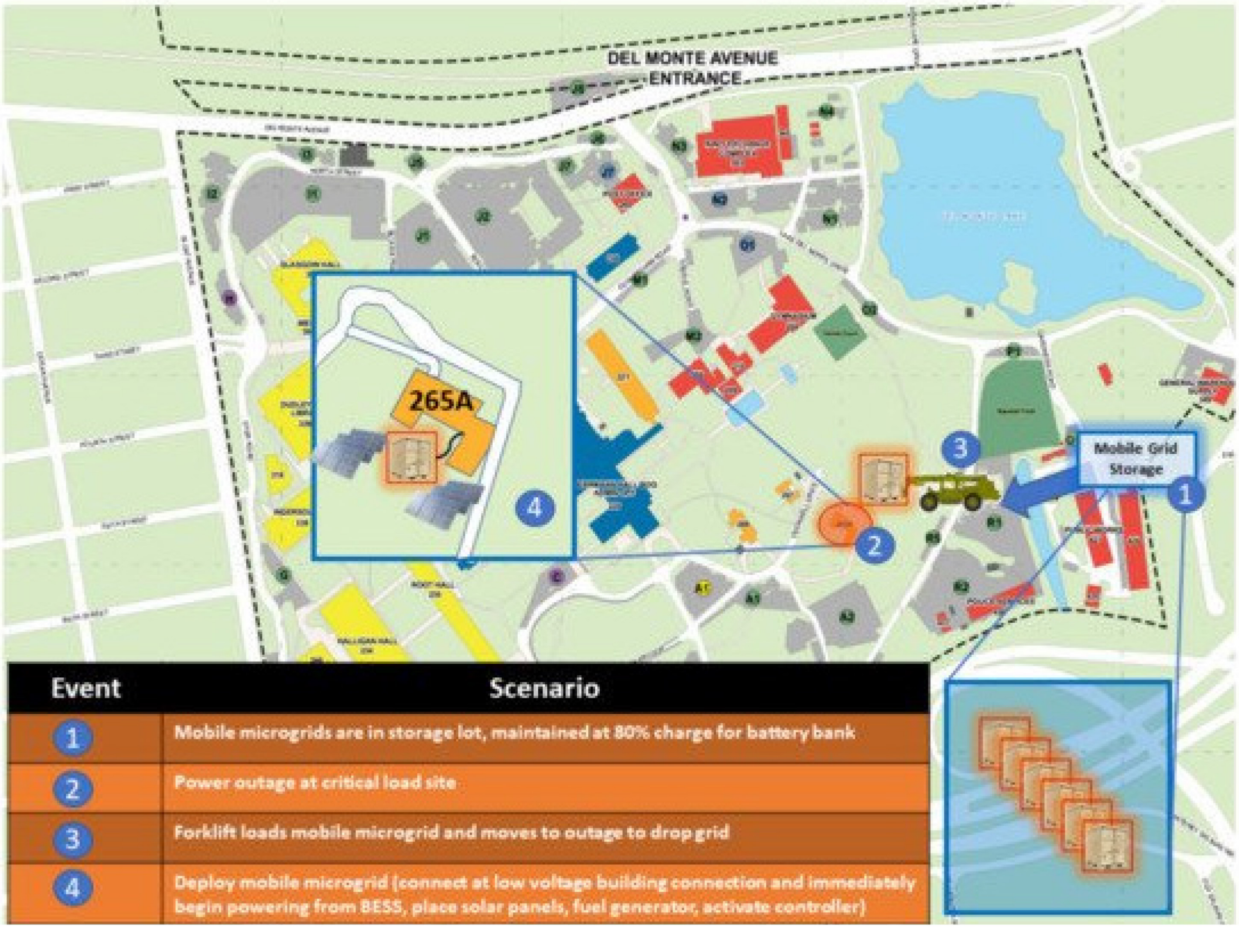
Two other projects are worth briefly mentioning due to their high potential, though their islanding claims have not yet been tested by a natural disaster or cyber-attack. The Parris Island microgrid at the US Marine Corps Recruit Depot has a 5.5 MW of solar photovoltaic power and 4 MW battery-based energy storage system. The grid has its own integrated control system and can conduct islanding and fast load shedding capabilities. The load shedding and islanding is 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" [78], [79]. 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 Army Base 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 hadn't. Not only was it able to island during normal workday 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 [80]. 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-kW mobile diesel generators [80].

In recently published modelling 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 centre, using algorithms to address the energy generation and demand balance and to deal with unexpected contingencies. However, launch campaigns were not possible without the use of dispatchable sources, such as a source of electricity such as a power plant [81].

B.4.4 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 back-up generators and battery storage fit with national security needs, to ensure that renewable technology can contribute power to the microgrid once islanded, and to ensure cybersecurity is included for microgrids even in the test phase (Figure B-4).

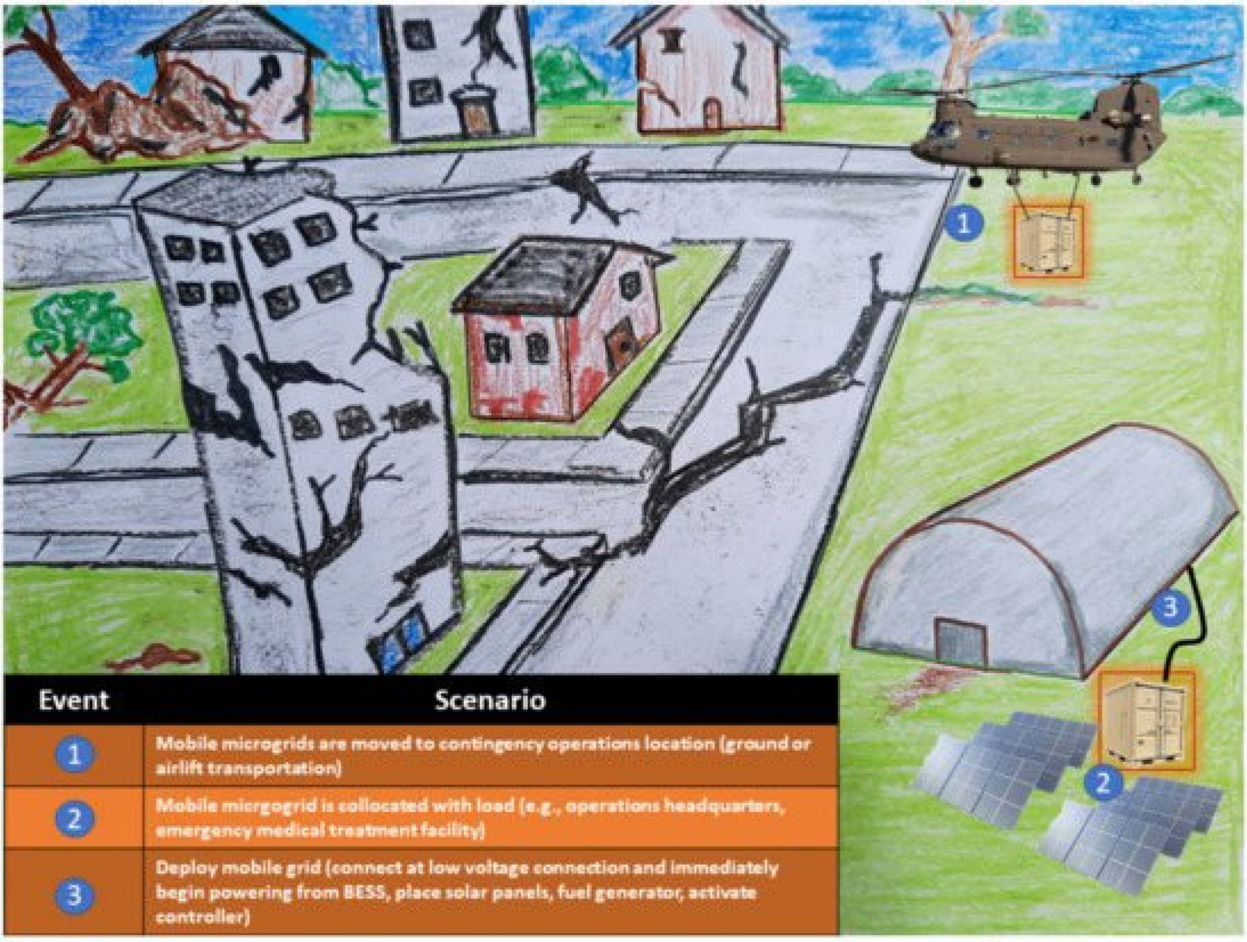


Event	Scenario
1	Mobile microgrids are in storage lot, maintained at 80% charge for battery bank
2	Power outage at critical load site
3	Forklift loads mobile microgrid and moves to outage to drop grid
4	Deploy mobile microgrid (connect at low voltage building connection and immediately begin powering from BESS, place solar panels, fuel generator, activate controller)

Figure B-4: Concept of Operations for Installation of Critical Load Back-Up Power from a Mobile Microgrid. Used with permission of Douglas VanBossuyt, Naval Postgraduate School.

One proposal to address the challenges of the unique energy generation and storage needs of diverse bases is with a mobile microgrid (Figure B-5), which could be stored and used for back-up 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 10kW load and that could be transported in an International Standards Organization Triple container that is 8 ft. x 6ft. 5 inches by 8 ft. and is not more than 10,000 lbs. The design was modelled 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 [82].

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 centre. When the operations centre 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 [82].



Event	Scenario
1	Mobile microgrids are moved to contingency operations location (ground or airlift transportation)
2	Mobile micrgogrid is collocated with load (e.g., operations headquarters, emergency medical treatment facility)
3	Deploy mobile grid (connect at low voltage connection and immediately begin powering from BESS, place solar panels, fuel generator, activate controller)

Figure B-5: Mobile Microgrid is Airlifted to Contingency Operations Location and can be Powered There. Used with permission of Douglas VanBossuyt, Naval Postgraduate School. Graphic originally published in: Varley et al., 2022. "Feasibility Analysis of a Mobile Microgrid Design to Support DoD Energy Resilience Goals." Systems 10, no. 3: 74. https://doi.org/10.3390/systems10030074.

While the system modelled did reduce reliance on the generator by 37%, and the study concluded that a standardized mobile microgrid has advantages that a customized single load microgrid doesn't, the assumptions made in the study call for field testing before the mobile microgrids are used in combat.

First, while both winter and summer data were used for the PV in the modelling 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-kW load that the microgrid can handle is on the low end for what DoD installations need to carry [82]. However, the modelling 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.

Before these lessons learned can be transferred to other 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 completely island from the host nation grid; and 3) Ensuring that cybersecurity is built into the process from the beginning.

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's 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 [83]. This 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.

However, recent recognition of the regulation challenge 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 [84]. 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 soon must calculate the long wait times for the multi-level 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 [85].

Beyond ensuring energy independence in the future, back-up 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. However, current policy only allows the back-up 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 [86]. Preparedness will mean assessing whether each base has enough back-up generators on hand to provide secure protection for the coming black-out seasons for the next four winters, and that they also have provided for the diesel and natural gas which 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" [87]. 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 Center of Excellence found that European militaries' prototype systems for mobile military camps often lacked cybersecurity considerations [88].

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 Defence 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 [88]. But without cybersecurity built in on the front end, a cyber-attack 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" [88].

B.4.5 Conclusion

Tests and modelling of microgrids on and for military installations in both 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 cyber-attacks. However, microgrids themselves 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 that 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 can work toward decreasing this regulatory inhibitor, microgrids can be in place sooner to power NATO's missions going forward.

B.4.6 Bibliography

Altman, D.H. "Hybrid Micro-Grid with High Penetration Wind for Islanding and High Value Grid Services." ESTCP Project EW-201606, Raytheon Integrated Defence Systems, vii. https://www.dvidshub.net/video/620985/otis-microgrid-leads-dod-energy-resiliency

Associated Press. "Russian Officials Charged in Years-Old Energy Sector Hacks." US News, March 25, 2022. https://www.usnews.com/news/business/articles/2022-03-24/russian-officials-charged-in-years-old-energy-sector-hacks?msclkid=5fbb7759b8ee11ecb9487d9555eadb7f

Butrimas, V. "Assessment Study of Cybersecurity of Smart-Grid Technologies Employed in Operational Camps." Energy Security Center 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

Castelo Branco, C.A.S., Moraes, F.P., Oliveira, H.A., Neto, P.B.L., Saavedra, O.R., de Matos, J.G., Oliveira, C.B.M., Ribeiro, L.A.d.S., Oliveira, A.C., Júnior, M.F.A. et al., "Mission Critical Microgrids: The Case of the Alcântara Space Center." Energies 2022, 15, 3-4, 22-24, 3226.

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

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

Guidance for DOD Utilization of Host Nation Power, Lexington, MA: MIT Lincoln Laboratory. October 2015. www.dtic.Mil/get-tr-doc/pd-f?AD=AD1034495

Henry, J. "Europe Cyberattack Results to Massive Internet Outage; About 5,800 Wind Turbines Went Offline.". Tech Times, March 5, 2022. (ampproject.org)

Lindsey, N. Russia and China Can Cripple Critical Infrastructure in the United States. CPO Magazine, Feb. 12, 2019. https://www.cpomagazine.com/cyber-security/russia-and-china-can-cripple-critical-infrastructure-in-united-states/

Lyngaas, S. "German Intelligence Agencies Warn of Russian Hacking Threats to Critical Infrastructure." CyberScoop, May 26, 2020. https://www.cyberscoop.com/german-intelligence-memo-berserk-bear-critical-infrastructure/

Marine Corps Recruit Depot Parris, U.S. Department of Energy Southeast CHP TAP. July 2021. Island https://chptap.ornl.gov/profile/121/MCRDParrisIsland-Project_Profile.pdf

Marqusee, Jeffrey, Craig Schultz, and Dorothy Robyn. "Power Begins at Home: Assured Energy for U.S. Military Bases." Noblis, The Pew Charitable Trusts, Jan. 12, 2017. https://www.pewtrusts.org/~/media/assets/2017/01/ce_power_begins_at_home_assured_energy_for_us_military_bases.pdf

Maxim, T, "China Accused of Hacking Ukraine Days before Russian Invasion." The Times, April 1, 2022. https://www.thetimes.co.uk/article/china-cyberattack-ukraine-z9gfkbmgf

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

"Microgrids for Commercial and Industrial Companies." World Business Council for Sustainable Development, p. 22-23, Nov. 2017. https://docs.wbcsd.org/2017/11/WBCSD_microgrid_INTERACTIVE. pdf

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

Peterson, C.J., Van Bossuyt, D.L., Giachetti, R.E. and Oriti, G. "Analyzing Mission Impact of Military Installations Microgrid for Resilience." Systems 9(3), 69, 2021. DOI: /10.3390/systems9030069

Renahan, T. "Realizing Energy Independence on U.S. Military Bases." JFQ 103, 4th Quarter 2021.

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

"Special Report: Ukraine. An Overview of Russia's Cyberattack Activity in Ukraine." Microsoft, Digital Security Unit, April 27, 2022.

Stockton, P.N. "Strengthening Mission Assurance Against Emerging Threats: Critical Gaps and Opportunities." JFQ 95, 4th Quarter 2019. https://paulnstockton.com/wp-content/uploads/2021/04/strengthening-mission-assurance-against-emerging-threats-critical-gaps-and-opportunities-for-progress.pdf

Stoltenberg, J. "NATO Secretary General's Report: Climate Change &Security Impact Assessment." NATO, 2022, p. 9. https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/280622-climate-impact-assessment.pdf

Stupp, C. "European Wind Energy Sector Hit in Wave of Attacks" The Wall Street Journal, April 25, 2022. European Wind-Energy Sector Hit in Wave of Hacks – WSJ

Varley, D.W., Van Bossuyt, D.L. and Pollman, A. 2022. "Feasibility Analysis of a Mobile Microgrid Design to Support DoD Energy Resilience Goals." Systems 10, no. 3: 74. DOI: 10.3390/systems10030074.

Wacket, M. "Germany's Energy Drive Criticized Over Expense, Risk." Reuters. March 30, 2021. https://www.reuters.com/article/germany-energy-audit-idUSL8N2LS2RC

Wood, E. "Army to Equip All Bases with Microgrids by 2035 as Part of Carbon-Free Electricity Goal." Microgrid Knowledge. Feb. 9, 2002. https://microgridknowledge.com/army-microgrid-climate/

Wood, E. "Military Microgrids: Four Examples of Innovation." Microgrid Knowledge. December 3, 2019, https://microgridknowledge.com/military-microgrids-four-examples/

B.5 CONCLUSION

"*Just as there is a hybrid war, there will be hybrid peace.*"

Ukrainian President Volodymyr Zelensky [89]

As of this writing, Russia's hybrid war against the Ukraine and its allies in NATO continues. Any lessons that Ukraine has taught NATO may be preliminary, but patterns have already started to emerge.

1) **The emerging technology environment creates additional vulnerabilities to energy critical infrastructure during hybrid war.** As Section B.1 demonstrated, malicious cyber actors, whether nation states or cyber criminals, are taking advantage of the vulnerabilities created by an Internet of Things environment, where Smart Grids, 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 the 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 [90]. In addition, Russian FSB officials have previously carried out cyber-attacks against energy critical infrastructure in the United States, including oil and gas, energy, nuclear power plant and utilities companies, giving Moscow the ability to cause disruption on a massive scale now [91].

2) **Russia is targeting energy security through cyber means in tandem with kinetic attacks.** As the Microsoft Digital Security Unit's report on Russia's cyber-attacks on Ukraine mentioned in Section B.2 shows, the current hybrid war 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 cyber-attacks on critical infrastructure, both in Ukraine, and in partner NATO member states.

   While stating that Ukraine's cyber security teams are not afraid of Russian attacks on their power grids and nuclear sites, Ukraine's cyber authority, Viktor Zhora 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.*" [92]

3) **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. This has 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, its hybrid war is being fought with the support of China. China has helped materially to soften the impact of economic sanctions on Russia, helped Russia to track Chinese-made drones being used on the battlefield in the Ukraine, and exerted its own control over the critical infrastructure and supply chain of NATO member states.

B.5.1 A Look Ahead

It is clear from lessons one and two that today's hybrid warfare will continue to target energy critical infrastructure. This study also found that the cybersecurity in place on energy critical infrastructure is not sufficient to protect NATO member states from attacks. This was true whether examining traditional infrastructure such as gas pumps and electric grids, or renewable infrastructure such as wind turbines or microgrids.

It is therefore highly recommended that NATO member states prioritize investing in research and development on Cyber Early Warning Systems (CEWS) that include virtual modelling of energy critical infrastructure for early mitigation of malicious intrusions. As demonstrated in Section B.3, 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 cyber-attacks. By using the virtual model of a natural gas pipeline and combining it with machine learning, cyber-attacks can be identified early and mitigated. Threat intelligence modelling and identification systems, based on heterogeneous information networks that use cyber entanglement capabilities are also helpful in this effort. The modelling 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 implementation of successful prototypes, grids, gas pipelines and other energy sources can be more adequately protected from cyber-attacks. 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. Indeed, strides are being made to improve mobile microgrids. However, there is still field testing and research to be done to ensure that microgrids can use both 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 that 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.

B.6 CYBER ATTACK VECTORS IN THE ENERGY SECTOR

Dr. Casey Dye

This reviews four major cyber-attacks on energy infrastructure in Eastern Europe between 2014 and 2018. It describes common attack vectors, highlights systemic weaknesses, discusses attack severity, and provides potential solutions. Additionally, NATO should consider the possibility of an Allied Nations' Early Warning System to provide the greatest universal defence against cyber-attacks to critical infrastructure.

Part of establishing requirements for the energy sector is understanding its weaknesses. In this section, a sampling of the most prominent cyber-attacks against energy systems or infrastructure in Eastern Europe are analysed for their severity, exploited weaknesses, and attack vectors. Each attack referenced includes a summary, a severity rating (see severity scale for reference), a list of perceived weaknesses exploited by the attackers, and recommendations for improving said weaknesses.

While these attacks do not illustrate the full breadth of attempted annual cyber-attacks there are several common factors which tie these and other cyber-attacks together. Most of this is seeded in the human element and while hardware would have certainly helped stop or deter the attackers, the result likely would have been the same. This summary will show how supply chain and spear phishing were used to circumvent the network perimeter if one existed.

These attacks could have been avoided by configuring a system to properly handle sensitive information. Every system is different and is reliant on external contributors for patches and support systems. Even the best systems surely have weaknesses which have not been discovered yet. To this end, collaboration and sharing of information is important. Early Warning Systems (EWS) are a promising innovation in the field of cyber security. These systems should help to eliminate human error by collecting massive amounts of information from a shared network, warning a system and its owners of an intrusion before damage is done.

B.6.1 Most Common Attack Vectors

The following list describes the most common ways threat actors gain access to a network.

B.6.1.1 Phishing/Spear Phishing

Almost every attack included a payload delivery via email. Though some of these instances only used phishing for the reconnaissance phase, its common success generates concern for how business systems are connected to operational systems, and the limited effectiveness and utility of currently implemented email security and firewalls (boundary defence).

Companies must strengthen their architecture (segmented business and operational networks), include more aggressive firewall/ESA rules, and create more effective employee training/policies to better defend against these attacks.

B.6.1.2 Poor Cyber Policy

Policies such as disabling delinquent accounts or setting secure passwords may seem like common knowledge, but it can often be overlooked. Employees may find it easier to have a common utility account for repairs. These service accounts sometimes do not expire since they are convenient. This can be a massive security risk because a disgruntled employee or someone who gains access to an old password list may be able to gain access to this account. Another often overlooked policy is disabling old accounts. The Colonial Pipeline was completely shut down because a ransomware attack gained access to the network through an account that should have been disabled.

B.6.1.3 Supply Chain Infiltration

Two of the below attacks included potent exploits that took advantage of poor supply chain management. these examples involved an attacker not directly exploiting the energy system, but instead exploiting software or hardware provided to it by a third party. These methods of attack indicate a need to refine how new software (patches, updates, etc.) or hardware (network devices, ICS devices, etc.) is introduced to the boundary.

Institutions need hash verification of patches, strengthened architecture (DMZ, sandbox environment, packet inspection) to accommodate foreign software downloads, scans of incoming devices, and a decreased reliance on third-party services like Internal Certificate Authority (ICA) to avoid similar vulnerabilities.

B.6.2 Most Common Solutions

The following list provides solutions to the aforementioned problems.

B.6.2.1 Cyber Architecture

Entities must better understand the "position" of devices on the network. Sensitive or critical systems should be physically or logically separated from business or common systems. In context, the volatility of the phishing exploits outlined in this section, begs the question why hosts used to check user emails have access to operational systems or networks. Well-constructed networks should have segmented devices. With competent policy and network division, unrelated devices and users should not have access to devices which they do not have permission to use.

B.6.2.2 Boundary Defence

Ideally, a good boundary defence consists of:

1) A solution capable of packet intrusion, detection, and prevention,
2) Some amount of anomaly detection, and
3) The ability to manage and scan emails, downloads, etc.

The idea is to only allow safe, necessary traffic in or out of the system. In the context of this study, phishing can be severely mitigated with solid system architecture. A payload can be delivered via the email itself, or via a malicious link (requiring a user to click said link). With a strong boundary defence, malicious attachments are stripped (or the email disposed of entirely) and bad links are blocked by the firewall. Further, a capable boundary defence system may even be capable of preventing a successfully delivered payload from communicating with its command and control (C&C) server. This solution must be in place to restrict access to and from the system's perimeter.

B.6.2.3 Supply Chain Management

In the context of cyber security, supply chain management involves exercising security controls that ensure the integrity of the resources accrued from vendors and other outside sources. These controls may be exercising hash validation against software downloads, sandbox environments to inspect downloaded software, scans of firmware existing on incoming hardware, and insourcing as to gain positive control of as many possible factors being introduced to the boundary. By applying a mistrust to any software or hardware incoming to the system, and minimizing reliance on foreign resources, an organization limits the attack surface present in the supply chain.

B.6.3 Severity Scale

The following scale (Table B-1) was used to rate each attack summary so as to quantify attack impacts in order to compare them against one another and, in future sections, to other analysed attacks (real or theoretical).

Please note: these ratings were assigned based off of each attack's potential. In other words, if an attack's impact was minimal for no other reason than because of the attacker's intent or 'happen-stance,' its severity was instead based on the attack's potential impact.

Table B-1: Severity Scale of Cyber-Attacks Based on Potential Impact. (Graphic by Casey Dye).

LOW	MEDIUM	HIGH	CRITICAL
Little to no effect on system or subsystem functionality. No loss of sensitive data. Minimal social impact, resulting in no policy changes.	Some recoverable effect on system or subsystem functionality. Loss of sensitive data in the form of network architecture information. Some social impact noticed by officials and citizens, but little to no change to policy.	Major impact to system functionality with inhibited ability to recover. Loss of important data such as patch information, network architecture information, and credentials. Noticeable social impact to include effects noticed by average citizens, and policy changes affecting alliances or strategy.	Dramatic impact to system functionality with no clear means to recover. Loss of critical information such as personal identifiable information or classified information carrying the potential to subvert significant nation-state infrastructure. Dramatic social impact to include some amount of fear or unrest spread to average citizens, and major changes to policy, strategy, and alliances.

B.6.4 Attacks in Review

Ukraine/Poland

GreyEnergy [93]

2015 – 2018

SEVERITY: Medium

SUMMARY: The Black Energy subgroup known as Grey Energy developed a specific form of malware known as '*GreyEnergy*' that was tested multiple times on both Poland and Ukraine between 2015 and 2018. The attacks demonstrated the ability of the group to steal valid digital certificates, implying the infiltration of the energy sector's supply chain (reminiscent of Stuxnet) (Table B-2). One associated attack also remotely accessed the automated control system and deleted information on servers and workstations (akin to KillDisk). Often, the malware was delivered via illegitimate emails (phishing).

Table B-2: Attack Summary of GreyEnergy. (Graphic by Casey Dye).

WEAKNESS	RESPONSE
The relationship between devices and certificates, specifically how they are produced and managed.	Certificate management (ICA), or some other solution).
The infiltration of attacks via email (phishing, spearfishing) highlights weaknesses in ESA, firewall, and employee training.	Strengthening of email security and firewall rules, to hamper the ability for malware to be delivered via email. Improved employee training regarding phishing.

WEAKNESS	RESPONSE
How the purchasing of Industrial Control System (ICS) equipment works in the energy sector including a look at supply chain management.	Validation of incoming equipment (supply chain management).
Issues with Permissions. The malware was consistently able to clear files, directories, and important software as it traversed the network. This suggests the malware either gained admin access, or the network was not correctly utilizing the concept of least privilege. The malware's ability to delete important objects may also/instead imply a successful privilege escalation attack.	Changes to user account configuration and group policy to implement the principle of least privilege -- denying any permissions not explicitly required by user duty.
Network architecture is currently too easy to pivot around. Some of these operations should be performed on utterly independent networks, or at least independent VLAN's.	Potential segmentation of "Business Network" from "Operational Network".
Recovery and Redundancy. When a critical system or subsystem was wiped, there was no means of recovery without physical access. Ideally, a system is resilient enough to have multiple ways to recover from failures and attacks with a greater degree of efficiency than this.	Failover server or some other management device able to quickly restore a compromised device, as well as some deep freeze ability for critical devices. Alternate, reliable way to continue to manage a device that has been compromised.

Poland, Germany, Italy, France, Spain, United States, Turkey

Dragonfly, Energetic Bear [94]

2011 – 2015

SEVERITY: High

SUMMARY: Dragonfly (also known as Energetic Bear) refers to a cyber campaign against power supply networks. Dating back to 2011, these attacks have had one of two purposes: 1) Trying to collect data from power grid networks or 2) Causing damage to the power distribution systems (Table B-3). While these attacks were originally directed at the United States, the focus shifted to Europe in early 2013. Significant damage has not been publicly documented. Attackers delivered two payloads through remote access trojans (RAT). (RAT) '*Trojan.karagany*' was meant to damage system functionality. The other RAT, '*Backdoor.Oldrea'* was used to collect system information and upload this information to the attackers' network. In this way, its role was a more passive one, meant to complement that of '*Trojan.karagany*.' Initially, access was gained to power grid networks via phishing attacks, but subsequent waves of attacks used the watering hole method and even compromised vendor websites (used for updates to power grid components). By compromising the I ICS vendor websites, users intending to download legitimate updates would instead download the malicious payload. Software from the vendors required administrative permissions to be installed. When run, they would install themselves in the '%ALLUSERAPPDATA%' directory. Because of this, non-administrative users were able to activate the trojan, as this directory is not a restricted one. Furthermore, a key was added to the registry causing it to run on reboot.

Table B-3: Attack Summary of Dragonfly/Energetic Bear. (Graphic by Casey Dye).

WEAKNESS	RESPONSE
Firewall rules were not in place to stop users from being redirected to the malicious websites due to the wateringhole attack (block by rule, allow by exception). Further, any normal browser should have detected the bad certificate offered by the malicious website. Employees should have been prevented from continuing to the site under these conditions.	Certificate management, either on the part of the third-party site, or on the part of the firewall's enforcement. Strengthening of firewall rules, to disallow the visiting of unknown/malicious sites (block by rule, allow by exception).
Image baseline not in place. Systems could be compromised by modification of startup programs, registry keys, and other computer resources which should be managed by group policy.	Image management, used in order to manage what programs are run at startup (deep freeze, host-based intrusion detection services, etc.).
Infiltration via email (phishing, spearfishing): This implies weaknesses in ESA, Firewall, and employee training.	Strengthening of email security and firewall rules, to hamper the ability for malware to be delivered via email. Improved employee training regarding phishing.
Vendor Downloads. Improper supply chain management regarding updates. No mechanism to detect whether update files have been modified.	Establish hash and download verification for all external/third-party downloads (supply chain management). Segmentation of download endpoint from rest of network (Quarantine, DMZ, etc.).
The targeted drivers and updates that infected the network were for cameras and other network devices. Network architecture is currently too easy to pivot around. Some of these operations should be performed on utterly independent networks, or at least independent VLAN's.	**Potential Segmentation of networks.** The infiltration of one network should not necessarily mean the infiltration of others, and devices should be associated with networks based on function and necessity.

Ukraine

BlackEnergy3 [95]

2014 – 2015

SEVERITY: Critical

SUMMARY: As early as May of 2014, phishing emails containing malware for the purpose of reconnaissance and initial "staging" were sent to Ukrainian power plants. When the email attachments were opened, malicious actors began harvesting the credentials for the Virtual Private Networks (VPN) that allowed users remote access to control centres. In this time, information regarding the control system's architecture and function was continuously collected. The '*BlackEnergy3*' malware was likely already installed on the system six months before the attack.

In 2015, the BlackEnergy3 malware allowed attackers to gain control of SCADA devices in the control system and overwrite their firmware, preventing any further remote control by legitimate operators. Supplemented by the KillDisk payload, this attack also erased and crashed infected computers, requiring re-imaging, as all data was unrecoverable. This attack shut down power for several hours, but (speculatively) at the discretion of the attackers had the potential to do far worse (Table B-4).

Table B-4: Attack Summary of BlackEnergy3. (Graphic by Casey Dye).

WEAKNESS	RESPONSE
The infiltration of attacks via email (phishing, spearfishing) highlights weaknesses in ESA, firewall, and employee training.	Strengthening of email security and firewall rules, to hamper the ability for malware to be delivered via email. Improved employee training regarding phishing.
The ability for VPN credentials to be harvested implies (potentially) single-factor authentication use for VPN sign-in, or non-encrypted sign-in communications.	Stronger sign-on requirements and protections for the VPN, to include multi-factor authentication, sufficiently encrypted communications and public key infrastructure, and device authentication.
The "persistence" of this access implies a weak IDS (anomaly detection), and potentially weak firewall configuration.	Strengthened firewall rules and IDS to better detect and tear down communication between and infected device and its C&C server.
The ability for baseline configuration to be so drastically changed remotely in the manner it was. The ability to change the firmware of a device locally from an arbitrary remote connection should be impossible.	Potential application account, as well as a critical device specifically responsible for baseline changes such as updates to firmware. This account should be unused by any normal user, making it more difficult for the associated credentials to be stolen. Any change to a device's baseline should require authority from this "patch repository authority" device.
The targeted drivers and updates that infected the network were for cameras and other network devices. Network architecture is currently too easy to pivot around. Some of these operations should be performed on utterly independent networks, or at least independent VLAN's.	**Potential Segmentation of networks.** The infiltration of one network should not necessarily mean the infiltration of others, and devices should be associated with networks based on function and necessity.
Issues with Permissions. The malware was consistently able to clear files, directories, and important software as it traversed the network. This suggests the malware either gained admin access, or the network was not correctly utilizing the concept of least privilege. The malware's ability to delete important objects may also/instead imply a successful privilege escalation attack.	Changes to user account configuration and group policy to implement the principle of least privilege -- denying any permissions not explicitly required by user duty.
Recovery and Redundancy. When a critical system or subsystem was wiped, there was no means of recovery without physical access. Ideally, a system is resilient enough to have multiple ways to recover from failures and attacks with a greater degree of efficiency than this.	Failover server or some other management device able to quickly restore a compromised device, as well as some deep freeze ability for critical devices.
Network architecture is currently too easy to pivot around. Some of these operations should be performed on utterly independent networks, or at least independent VLANs.	Potential segmentation of "Business Network" from "Operational Network".

Ukraine

Industroyer/Crashoverride [96]

2016

SEVERITY: Critical

SUMMARY: In December of 2016, part of Kyiv, the capital of Ukraine, lost power for approximately one hour when the power substation Pivnichna was attacked by the malware, *'Industroyer*', attributed to the hacking group, Sandworm. *Industroyer* is unique in that it appears to be engineered specifically to target energy sector systems and can take control of subsystems. Industroyer had multiple modules each with a specific task. The first module enumerated and scouted the network. The second module performed the Denial of Service (DOS) attack against the Network Interface Card (NIC). The third module ran commands to override system processes. And the fourth and final module deleted system files. Logs indicate that initial access to the system was likely gained through a phishing campaign which dates as far back as January 2016 (Table B-5).

From the public-facing side, the attackers were able to gain access to the management network for the power grid. Account permissions were modified by the attackers on December 1st, 16 days before the attack. *Industroyer* could cause substantially more damage than it did. The vulnerability exploited in this attack was caused by an **NIC** firmware issue for Siemens devices. Malicious packets could be sent to port 50000/UDP to cause a DOS state which could only be resolved with a restart. Once a host was restarted, *Industroyer* malware would move into the next stage, during which it would take over the system. From this point, *Industroyer* was able to erase system files and execute commands with administrator privileges or even under the guise of a legitimate user's account. In the 2016 attack, system processes were overridden and control was taken by the malware but system files were not deleted. Power was lost for only an hour and no permanent damage was done, however *Industroyer* could perform longer lasting damage because of its depth in the system.

Table B-5: Attack Summary of Industroyer. (Graphic by Casey Dye).

WEAKNESS	RESPONSE
Patch Management. The exploited vulnerability was a known issue which had already been patched by Siemens systems in a June 2016 update, nearly six months prior to the attack.	Patch maintenance, in the form of a repository, if necessary.
The infiltration of attacks via email (phishing, spearfishing) highlights weaknesses in ESA, firewall, and employee training.	Strengthening of email security and firewall rules, to hamper the ability for malware to be delivered via email. Improved employee training regarding phishing.
Network architecture is currently too easy to pivot around. Some of these operations should be performed on utterly independent networks, or at least independent VLAN's.	**Potential segmentation of networks.** The infiltration of one network should not necessarily mean the infiltration of others, and devices should be associated with networks based on function and necessity.

WEAKNESS	RESPONSE
Issues with Permissions. The malware was consistently able to clear files, directories, and important software as it traversed the network. This suggests the malware either gained admin access, or the network was not correctly utilizing the concept of least privilege. The malware's ability to delete important objects may also/instead imply a successful privilege escalation attack.	Changes to user account configuration and group policy to implement the principle of least privilege -- denying any permissions not explicitly required by user duty.
Boundary security system robust enough to detect and prevent the malicious packets being sent to port 50000/UDP.	Implement a strong perimeter firewall and IDS or IPS to prevent access to network devices.

B.7 EARLY WARNING SYSTEM (EWS)

B.7.1 Prologue

Each of the above recommendations are industry standard mitigations, focused on reactive controls. In other words, these recommendations only begin affecting an attack once the attack has already begun. That said, no matter how robust these controls become, there is no such thing as an "unhackable" system. Once an attack has started, either a system is prepared, or it isn't. In the case of a zero-day attack, more often than not, a system is not prepared.

The most powerful supplement to cyber defence is information about successful attacks against other systems, developing malware on the dark web, and new offensive techniques and strategies. This kind of knowledge leads to software patches, signature updates, and new standard practices, all of which may thwart future attacks that use similar attack vectors.

Conversely, this is also what makes zero-day attacks so powerful: they deny security personnel access to this kind of information by virtue of being new. Zero-day attacks, theoretically, can only be zero-day attacks once. After the attack has been used against some entity, its most powerful tool, obscurity, is gone. Unfortunately, in practice, this is only true if information about the attack is available. Otherwise, the attack may succeed on a new target, still obscure from its next victim. A major goal for security personnel then, must be striving to effectively disseminate knowledge from attacks as quickly as possible.

B.7.2 What is an EWS

As quoted from Early Warning Systems for Cyber Defence, an EWS "is an emerging area of research which aims at alerting an attack attempt in its nascent stages." The word "early" here and henceforth will be used to refer to any time before a threat reaches its target system, and begins its impact. This can be during the attack's development lifecycle, during the attack's transit across infrastructure not directly related to is target (i.e., ISP infrastructure, etc.), or in the wake of the attack impacting a different target.

An important point to make is the difference between an EWS and typical IDS/IPS systems as referenced in previous recommendations. Unlike an EWS, IDS/IPS systems "attempt to detect attack(s) using known indications of attack patterns (these can be either signatures or anomalies) instead of using generic preliminary indications." EWS do not rely on the type of information zero-day attacks deny a system. Instead, they both gather that information and have a unique way of obtaining it. The advantage ends up being that an attack loses its obscurity before it ever impacts its target and, in doing so, hardens the target in question. Though effective in practice, this type of system relies on a more complex infrastructure than typical solutions. EWS still largely depend on their ability to collect evidence of an attack. Obstacles to this data collection could be availability (i.e., a victim unwilling to share information), and the ability to collect it in the first place (i.e., the ability to mount sensors on key infrastructure points). This type of system would require massive inter-entity cooperation. It is no small undertaking, but it is not unheard of as shown in the example below [97].

B.7.3 The Great Firewall of China

The Great Firewall of China refers to an initiative started by the Chinese government to control what information its citizens can see on the internet. This amount of authority over the private sector is effectively the opposite extreme of the United States' relationship with its own private sector. The Great Firewall grants the Chinese government near-total control over what data is allowed in and out of its perimeter through the use of packet filtering, and extensive IP blacklists/whitelists [98].

For every comment that can be made against the extremity of China's measure, there are two more that can be made regarding its effectiveness. A report done by the Harvard Kennedy Institute indicates that China has the highest ranked Cyber Power Score in the defence category. More importantly, their infrastructure is an ideal environment to mount the sort of sensors that an EWS would rely on. Not only would it provide uninhibited access to information entering their boundary (whatever boundary that may be), but it would have the advantage of being privy to any incoming attack before it hits its eventual target (likely deeper in the boundary) [99].

That said, this paper certainly is not proposing an initiative as extreme as the Great Firewall, but instead uses it as a point of reference. Rather than creating such a totalitarian system, Allied Countries should create a similar border based on inter-entity cooperation. Allied energy sectors alone could create a cooperative boundary across countries that would afford access to significant early warning data. Taking this cooperation any further only strengthens the effectiveness of EWS.

B.7.4 The Challenge

This paper does not attempt to address the logistics and analysis that goes into EWS. Machine learning/artificial intelligence is most certainly required for the kind of analysis necessary to differentiate it from IDS/IPS systems. This sort of analysis is hardly unheard of and is being developed every day. Acquiring access to the information required to make this sort of system work is the greater challenge. This kind of security, like many security systems, walks the line between security and privacy. Inter-country cooperation aside, countries like the United States face the obstacle of a public sector resistant to government cooperation.

According to IC3 director, Donna Gregory, 88-90% of cybercrimes go unreported in the United States because entities are unwilling to admit an attack happened, let alone share the details about it. Because important data that goes into an early warning system will require victims sharing information about a zero-day, lacking access to it will severely hamper an EWS's effectiveness. Further, a similar sort of cooperation is going to be required to mount sensors in meaningful network locations, and in cases like the United States, many of these locations are privately owned.

The United States federal government owns less than 16% of the shares in the energy sector [100]. Almost the entire energy grid complex, consisting of 7,300 power plants is privately owned [100]. Further, ISPs are private entities as well, and will undoubtedly own choke points for network traffic.

If companies were forthcoming with their information, it runs the risk of being exposed in an attack similar to the Solarwinds attack. Solarwinds was the backbone for many international organizations. We may not know the repercussions of that attack for years to come. All the information for an EWS would have to be delivered through a collection channel. If a malicious actor were to get hold of the information, multiple systems would be at risk instead of just a single system and the risk increases as multiple allied nations become involved. Not only would this larger collection of data be the target of external attacks, but it would also be subject to changing alliances between included nation states. Espionage becomes substantially easier when you are freely given access to a nation's vulnerabilities. To that end, careful selection of who is contributing and participating is imperative. It may ultimately be impossible for such a system to work on a multi-nation scale.

B.7.5 Recommendation

An EWS system absolutely offers the kind of advantage the energy sector needs to remain resilient against threats as noted in the above analysis. In order to create an environment in which this sort of system can exist, an initiative needs to be started at a governmental level calling for inter-entity cooperation. This initiative needs to outline not only the sharing of attack and network data between allied countries, but also between the private and public sector. Further, creating an "out of band" network to share this kind of information between key entities would ensure that as the EWS detected a potential threat, the information could be efficiently disseminated, ensuring updates hit potential victims before the attack does.

While an EWS among allied nations might be impossible, there is still the ability to share information among allies. Several nations have already started sharing their cyber information. The United States, Japan, and much of Europe share common cyber vulnerability information. Untrusted nations are not given this information. While far from an EWS, it could still be the groundwork for more advanced information sharing in the future.

B.7.6 Glossary

Admin Access Also called "root permission" or "admin permission." Describes a user account with a permission level that has little to no restrictions on creation, modification, or deletion of any files, directories, or settings across the network. Its name comes from the only kind of legitimate users who should have these permissions -- administrators.

Boundary Where a network environment ends and another begins. All the devices within one subnet or network area. Generally speaking, the place where information would leave one network and go to another. In cyber security, a boundary is a grouping of network appliances and devices with a similar overarching policy or security level.

C&C Server Host controlled by an attacker used to send commands or updates to a device infected by associated malware. A connection from the compromised host to this device is often required for an attack's goal to be met

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. This allows a reliable means of identifying a host or user.

ICA Internal Certificate Authority. A server internal to a network responsible for managing, generating, and issuing digital certificates.

IDS Intrusion Detection System. A device which monitors a network for malicious activity. When suspicious activity is detected, it is logged and sent to an administrator or stored on a logging server.

IPS Intrusion Prevention System. A device which monitors a network for malicious activity. When suspicious activity is detected, it will deny it access or move it to quarantine for evaluation.

Least Privilege A common security practice in which users and application accounts are allowed the minimum permissions necessary to complete their job. A typical plant operator, for example, would have no legitimate need of the ability to delete restricted files.

NIC Network Interface Card. The device in computer systems responsible for communicating between the network and that device.

Phishing Using a vague, fraudulent email to steal information or gain unauthorized access to a network. Designed to trick a user into executing malicious code, or responding with information.

Privilege Escalation A method by which a user or application gains access to a group or user with less restrictions or greater privileges than was previously had. When being attacked, this is one of the primary goals of an attacker, as greater privileges also mean more power to execute malicious processes. When an attacker obtains this, it is typically via a means not intended by the system administrator.

Public-Facing Describes an interface or "side" of a network the public can access. For example, when visiting 'Google.com,' a user is visiting a public-facing server hosted by Google.

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.

RAT Remote Access Trojan. A piece of malware which gives an attacker a backdoor into a system. Usually allowing them to gain complete administrative control.

SIEM Security Information and Event Management. A server which stores and manipulates logs from network devices. Allows for system administrators to view events on the network from a centralized location.

SIEMENS A large German based manufacturer for Industry, Energy, Healthcare, and Infrastructure.

Spearphishing Using a targeted, fraudulent email under the guise of legitimate personal circumstances to steal information or gain unauthorized access to a network. Designed to trick a user into executing malicious code, or responding with information.

Wateringhole A cyber-attack where the attacker infects a website often visited by the victim. Either by redirecting to a fraudulent weblink or manipulating the webpages at the infected website.

B.7.7 Bibliography

Danyk, Y., Briggs, C., and Maliarchuk, T. (n.d.). Features of Ensuring Cybersecurity of the Critical Infrastructure of the State. Retrieved December 16, 2020, from http://tacs.ipt.kpi.ua/article/view/209484/209553

Langill, J.T. "Defending Against the Dragonfly Cyber Security Attacks." September 15, 2014. Retrieved December 16, 2020, from https://www.docdroid.net/hmws/belden-white-paper-dragonfly-cyber-security-attacks-pdf

Baezner, M. "Cyber and Information Warfare in the Ukrainian Conflict," October 01, 2018. Retrieved December 16, 2020, from https://www.research-collection.ethz.ch/handle/20.500.11850/321570

Slowik, J. “Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE.” October 12, 2018. Retrieved December 16, 2020, from https://www.bgp4.com/wp-content/uploads/2018/10/CRASHOVERRIDE2018.pdf

Kalutarage H., Shaikh S., Lee B.S., Lee C., and Kiat Y.C. “Early Warning Systems for Cyber Defence.” In: Camenisch J., Kesdoğan D. (eds) Open Problems in Network Security. iNetSec 2015. Lecture Notes in Computer Science, vol 9591. Springer, Cham, 2016. DOI: 10.1007/978-3-319-39028-4_3.

Chan, C., Dao, A., Hou, J., Jin, T. and Tuong, C. “Free Speech vs Maintaining Social Cohesion.” cs.stanford.edu. 2011 https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreeExpressionVsSocialCohesion/china_policy.html

Voo, J., Hemani, I., Jones, S., DeSombre, W., Cassidy, D., and Schwarzenbach, A. “National Cyber Power Index 2020: Methodology and Analytical Considerations.” Harvard Kennedy: Belfer Center, 2020. https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf

U.S. Energy Information Administration. “Electricity Explained.” 2020. Retrieved from eia.gov: https://www.eia.gov/energyexplained/electricity/electricity-in-the-us-generation-capacity-and-sales.php

Anthropocene Institute. “How the Grid Works.” (n.d.). Retrieved from Anthropocene Institute, 2021. .https://www.anthropoceneinstitute.com/science/grid/

B.8 REFERENCES

[1] Lee, A. “War in Ukraine: Russia Attacks Nation Looking to Renewables and EU Grid for Energy Freedom,” February 24, 2022.

[2] NATO, “NATO’s Response to Hybrid Threats,” June 7, 2022. https://www.nato.int/cps/en/natohq/topics_156338.htm

[3] International Energy Agency, “Energy Security: Ensuring the Uninterrupted Availability of Energy Sources at an Affordable Price,” December 2, 2019. https://www.iea.org/areas-of-work/ensuring-energy-security.

[4] NATO, “NATO’s Role in Energy Security,” June 23, 2021. https://www.nato.int/cps/en/natohq/topics_49208.htm

[5] “Special Report: Ukraine. An overview of Russia’s cyberattack activity in Ukraine,” Microsoft, Digital Security Unit, April 27, 2022.

[6] Joseph, H. “Europe Cyberattack Results to Massive Internet Outage; About 5,800 Wind Turbines Went Offline,” Tech Times, 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

[7] Stupp, C. “European Wind Energy Sector Hit in Wave of Attacks,” The Wall Street Journal, 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

[8] Butrimas, V. “Assessment Study of Cybersecurity of Smart-Grid Technologies Employed in Operational Camps,” Energy Security Center 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

[9] Cyber Peace Institute, “Attack Details,” September 28, 2022. https://cyberconflicts.cyberpeaceinstitute.org/threats/attack-details

[10] Lohmann, S. What Ukraine Taught NATO About Hybrid Warfare, United States Army War College Press, 2022.

[11] Rühle, M. and Roberts, C. “Enlarging NATO’s Toolbox to Counter Hybrid Threats,” NATO Review, March 19, 2021. https://www.nato.int/docu/review/articles/2021/03/19/enlarging-natos-toolbox-to-counter-hybrid-threats/index.html

[12] U.S. Department of State, Office of the Spokesperson, “Russia’s Top Five Persistent Disinformation Narratives,” Januarys 20, 2022. https://www.state.gov/russias-top-five-persistent-disinformation-narratives/

[13] Cockrell, C.D. “Russian Actions and Methods Against the United States and NATO,” US Army University Press, Military Review, September 27, 2017. https://www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2017-Online-Exclusive-Articles/Russian-Actions-and-Methods/

[14] Gigitashvili, G. “Cyber-Enabled Information Operations Targets Poland with Radiological Leak Hoax,” Atlantic Council Digital Forensic Lab, April 2, 2021, accessed May 14, 2021. https://medium.com/dfrlab/cyber-enabled-information-operation-targets-poland-with-radiological-leak-hoax-28a5b1fb6776

[15] Higgins, A. “Russian Money Suspected Behind Fracking Protests,” The New York Times, November 30, 2014.

[16] World Nuclear News, “Teaming Agreement siged for Romanian SMR deployent,” Nov. 5, 2021. https://www.world-nuclear-news.org/Articles/Teaming-agreement-signed-for-Romanian-SMR-deployme

[17] Wood, E. “Military Microgrids: Four Examples of Innovation,” Microgrid Knowledge, Dec. 3, 2019. https://microgridknowledge.com/military-microgrids-four-examples/

[18] Butrimas, V. “Assessment Study of Cybersecurity of Smart Grid Technologies Employed in Operational Camps,” NATO Energy Security Center of Excellence, Aug. 11, 2021. https://enseccoe.org/data/public/uploads/2021/11/vb-cyber-asses-study-v1dot2dot3-oct-1-2021-cyber-sg-for-mil-camps.pdf

[19] Colomina, C., Margalef, H.S., and Youngs, R. “The Impact of Disinformation on Democratic Processes and Human Rights in the World,” Apr 2021, 48. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653635/EXPO_STU(2021)653635_EN.pdf

[20] Giannopoulos, G., Smith, H., and Theocharidu, M., “The Landscape of Hybrid Threats: A Conceptual Model,” 2021, 13.

[21] DoD Dictionary of Military and Associated Terms, August 2021.

[22] European Commission, “Tackling Disinformation Online,” February 23, 2022. https://digital-strategy.ec.europa.eu/en/policies/online-disinformation

[23] Baca-Pogorzelska, K. “How Chernobyl Fake News Poisons Nuclear Energy Debate in Poland,” Notes from Poland, 25 April 2020. https://notesfrompoland.com/2020/04/25/how-chernobyl-fake-news-poisons-nuclear-energy-debate-in-poland/

[24] Krol, A. “Information Warfare Against Strategic Investments in the Baltic States and Poland,” The Warsaw Institute Review, 19 July 2017. https://warsawinstitute.org/information-warfare-strategic-investments-baltic-states-poland/

[25] Scott, M. “As War in Ukraine Evolves, So Do Disinformation Tactics,” Politico, 10 March 2022. https://www.politico.eu/article/ukraine-russia-disinformation-propaganda/

[26] Ukrinform, “A Digest of Russia Propaganda for May 31,” Center for Strategic Communications – Ministry of Culture and Information Policy of Ukraine, June 1, 2022.

[27] Scott, M. “As War in Ukraine Evolves, So Do Disinformation Tactics,” Politico, 10 March 2022. https://www.politico.eu/article/ukraine-russia-disinformation-propaganda/

[28] Reuters, “Fearing Martial Law or Conscription, Some Russians Try to Flee Abroad.” 3 March 2022. https://www.reuters.com/world/europe/fearing-martial-law-or-conscription-some-russians-try-flee-abroad-2022-03-03/

[29] Scott, M. “As War in Ukraine Evolves, So Do Disinformation Tactics,” Politico.

[30] Hybrid CoE, “Countering Disinformation: News Media and Legal Resilience,” Apr 2019.

[31] West, D.M. “How to Combat Fake News and Disinformation,” Brookings Institution, 18 December 2017. https://www.brookings.edu/research/how-to-combat-fake-news-and-disinformation/

[32] Dupuy, A. “Energy Security is Critical to NATO’s Black Sea Future,” Atlantic Council, May 12, 2022. https://www.atlanticcouncil.org/blogs/turkeysource/energy-security-is-critical-to-natos-black-sea-future

[33] Hwang, K., Kulkareni, S. and Hu, Y. “Cloud Security with Virtualized Defense and Reputation-Based Trust Management,” Dependable, Autonomic and Secure Computing, 2009. DASC ‘09. Eighth IEEE International Conference on, 717 – 722, Dec 2009.

[34] Demertzis, K., Tsiknas, K., Takezis, D. 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.” https://arxiv.org/ftp/arxiv/papers/2102/2102.08411.pdf

[35] Song, W., Beshley, M., Przystupa, K. et al., “A Software Deep Packet Inspection System for Network Traffic Analysis and Anomaly Detection,” 2020. https://www.researchgate.net/publication/340013171_A_Software_Deep_Packet_Inspection_System_for_Network_Traffic_Analysis_and_Anomaly_Detection

[36] Mann, V., Vishnoi, A. and Bidkar, S. “Living on the Edge: Monitoring Network Flows at the Edge in Cloud Data Centers,” IBM Research. https://www.inf.ufpr.br/aldri/disc/artigos/2014/patrick_art2.pdf

[37] Gyanfi, E. and Jurcut, A. “Intrusion Detection in Internet of Things Systems: A Review on Design Approaches Leveraging Multi-Access Edge Computing, Machine Learning, and Datasets,” 2022. https://www.mdpi.com/1424-8220/22/10/3744/pdf?version=1652517852

[38] Maciej, A., Mazurowski, P.A., Habas, J.M., Zurada, J.Y., Lo, J.A., and Tourassi Baker, G.D. "Training Neural Network Classifiers for Medical Decision Making: The Effects of Imbalanced Datasets on Classification Performance," Neural Networks, 21(2-3), 2008, 427-436. ISSN 0893-6080, DOI: 10.1016/j.neunet.2007.12.031.

[39] William, D. "How AI Can Help Improve Intrusion Detection Systems," GCN, April 15, 2020. https://gcn.com/cybersecurity/2020/04/how-ai-can-help-improve-intrusion-detection-systems/291266/

[40] Ayoade, G., Al-Naami, K., Gao, Y., Hamlen, K.W., and Khan, L. "Improving Intrusion Detectors by Crook-Sourcing," Proceedings of the 35th Annual Computer Security Applications Conference, December 9, 2019. https://www.semanticscholar.org/paper/Improving-intrusion-detectors-by-crook-sourcing-Ayoade-Al-Naami/fef9e447174994c10b359bb1934d19c7c6e4fe9b?p2df

[41] Horner, K. "Computer Scientists' New Tool Fools Hackers into Sharing Keys for Better Cybersecurity," https://cs.utdallas.edu/cs-new-tool-fools-hackers-cybersecurity/

[42] Ayoade, G., Araujo, F., Al-Naami, K., Hamleen, K.W. et al., "Automating Cyberdeception Evaluation with Deep Learning," University of Texas at Dallas, IBM Research, January 2020, Proc. 53rd Hawaii Int. Conf. System Sciences (HICSS). https://www.researchgate.net/publication/337287036_Automating_Cyberdeception_Evaluation_with_Deep_Learning

[43] Pal, K., "10 Ways Virtualization Can Improve Security," Technopedia, October 22, 2021. https://www.techopedia.com/2/31007/trends/virtualization/10-ways-virtualization-can-improve-security

[44] Golling, M. and Stelte, B. "Requirements for a Future EWS – Cyber Defence in the Internet of the Future," 3rd International Conference on Cyber Conflict, 2011. https://www.digar.ee/arhiiv/en/download/107746

[45] Raicu, G. and Lohmann, S. "Energy Security in the Era of Hybrid Warfare," SAS-163 Research Project Annual Workshop, December 2021, Project EWS Concepts, Oberammergau, Germany.

[46] Yadav, S., Kumar, S., Sharma, S. and Singh, A. "A Review of Possibilities and Solutions of Cyber Attacks in Smart Grids," 2016, 1st International Conference on Innovation and Challenges in Cyber Security.

[47] Mattioli, R. and Moulinos, K. "Communication Network Interdependencies in Smart Grids," ENISA, n.d. https://www.enisa.europa.eu/publications/communication-network-interdependencies-in-smart-grids/@@download/fullReport

[48] Abbaszadeh, M., and Mestha, L.K. United States Patent Application 20200067969, "Situation Awareness And Dynamic Ensemble Forecasting of Abnormal Behavior In Cyber-Physical System," General Electric Company, February 27 2020. https://www.freepatentsonline.com/y2020/0067969.html

[49] Abbaszadeh, M., Mestha, L. and Yan, W. "Forecasting and Early Warning for Adversarial Targeting in Industrial Control Systems," 2018 IEEE Conference on Decision and Control (CDC).

[50] Pedregosa et al., "Gaussian Mixture Models," in: Scikit-learn: Machine Learning in Python, JMLR 12, 2825-2830, 2011. https://scikit-learn.org/stable/modules/mixture.html

[51] Kleeman, L. "Understanding and Applying Kalman Filtering," Monash University, Clayton, https://www.cs.cmu.edu/~motionplanning/papers/sbp_papers/kalman/kleeman_understanding_kalman.pdf

[52] General Electric Research, “Digital Ghost: Real-Time, Active Cyber Defense,” Digital Ghost: Real-Time, Active Cyber Defense, GE Research.

[53] Korkzy’sky, M., Huh, J., Hamieh, A. and Holm, H. “DIAMoND: Distributed Intrusion/Anomaly Monitoring for Nonparametric Detection,” ICCCN Conference, August 2015. https://www.researchgate.net/publication/278018275_DIAMoND_Distributed_IntrusionAnomaly_Monitoring_for_Nonparametric_Detection

[54] Ikwu, R. “Multi-Dimensional Structural Data Integration for Proactive Cyber-Defense,” published in the IEEE International Conference on Cyber Situational Awareness, Data Analytics and Assessment, 2017.

[55] Ikwu, R.E. “The Entangled Cyberspace: An Integrated Approach for Predicting Cyber-attacks,” [Great Britain]: Brunel University London, 2018.

[56] Barnett et al., “19th ICCRTS: C2 Agility: Lessons Learned from Research and Operations Paper 081: Using Causal Models to Manage the Cyber Threat to C2 Agility : Working with the Benefit of Hindsight,” Int. Command Control Res. Technol. Symp., 2014.

[57] Gao, Y., Li, X., Peng, H., Fang, B. and Yu, P. “HinCTI: A Cyber Threat Intelligence Modelling and Identification System Based on Heterogeneous Information Network,” IEEE Xplore, February 1, 2022. https://ieeexplore.ieee.org/document/9072563

[58] Raicu, G. and Lohmann, S. “Energy Security in the Era of Hybrid Warfare,” SAS-163 Research Project, April 2022, Project EWS Concepts in the Medium Term.

[59] Guidance for DOD Utilization of Host Nation Power, Lexington, MA: MIT Lincoln Laboratory, October 2015. www.dtic.Mil/get-tr-doc/pd-f?AD=AD1034495

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

[61] Lindsey, N. Russia and China can Cripple Critical Infrastructure in the United States. CPO Magazine, Feb. 12, 2019. https://www.cpomagazine.com/cyber-security/russia-and-china-can-cripple-critical-infrastructure-in-united-states/

[62] Maxim, T. “China Accused of Hacking Ukraine Days before Russian Invasion,” The Times, April 1, 2022. https://www.thetimes.co.uk/article/china-cyberattack-ukraine-z9gfkbmgf

[63] Associated Press, “Russian Officials Charged in Years-Old Energy Sector Hacks,” US News, March 25, 2022. https://www.usnews.com/news/business/articles/2022-03-24/russian-officials-charged-in-years-old-energy-sector-hacks?msclkid=5fbb7759b8ee11ecb9487d9555eadb7f

[64] “Number of Active-Duty United States Military Personnel in Europe in 2022, by Country,” Statista, Feb. 4, 2022. https://www.statista.com/statistics/1294271/us-troops-europe-country/

[65] “Anzahl der Soldaten und Soldatinnen bei der Bundeswehr von 2000 bis 2022,” June 2022. https://de.statista.com/statistik/daten/studie/38401/umfrage/personalbestand-der-bundeswehr-seit-2000/

[66] “Anzahl der an internationalen Einsätzen beteiligten deutschen Soldaten der Bundeswehr,” Statista, May 30, 2022. https://de.statista.com/statistik/daten/studie/72703/umfrage/anzahl-der-soldaten-der-bundeswehr-im-ausland/

[67] "German Intelligence Sees Russia Behind Hack of Energy firms," Reuters, June 20, 2018. https://www.reuters.com/article/us-germany-cyber-russia-idUSKBN1JG2X2

[68] Lyngaas, S. "German Intelligence Agencies Warn of Russian Hacking Threats to Critical Infrastructure," CyberScoop, May 26, 2020. https://www.cyberscoop.com/german-intelligence-memo-berserk-bear-critical-infrastructure/

[69] Wacket, M. "Germany's Energy Drive Criticized Over Expense, Risk," Reuters, March 30, 2021. https://www.reuters.com/article/germany-energy-audit-idUSL8N2LS2RC

[70] Henry, J. "Europe Cyberattack Results to Massive Internet Outage; About 5,800 Wind Turbines Went Offline," Tech Times, March 5, 2022. ampproject.org.

[71] Stupp, C. "European Wind Energy Sector Hit in Wave of Attacks" Wall Street Journal, April 25, 2022.

[72] "Special Report: Ukraine. An Overview of Russia's Cyberattack Activity in Ukraine," Microsoft, Digital Security Unit, April 27, 2022.

[73] Wood, E., "Army to Equip All Bases with Microgrids by 2035 as Part of Carbon-Free Electricity Goal," Microgrid Knowledge, Feb. 9, 2002. https://microgridknowledge.com/army-microgrid-climate/

[74] Stoltenberg, J. "NATO Secretary General's Report: Climate Change & Security Impact Assessment," NATO, 2022, p. 9. https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/280622-climate-impact-assessment.pdf

[75] "Microgrid at Marine Corps Air Station Miramar," Marine Corps Installations Command, MCICOM, June 30, 2021. https://www.marines.mil/News/News-Display/Article/2677033/microgrid-at-marine-corps-air-station-miramar /

[76] Roege, P. "4 Lessons Learned from the Otis Microgrid Project," Typhoon HIL, Inc., June 8, 2021. https://info.typhoon-hil.com/blog/4-lessons-learned-from-the-raytheon-technologies-otis-microgrid-project

[77] Altman, D.H. "Hybrid Micro-Grid with High Penetration Wind for Islanding and High Value Grid Services," ESTCP Project EW-201606, Raytheon Integrated Defense Systems, vii. https://www.dvidshub.net/video/620985/otis-microgrid-leads-dod-energy-resiliency

[78] Wood, E. "Military Microgrids: Four Examples of Innovation," Microgrid Knowledge, December 3, 2019. https://microgridknowledge.com/military-microgrids-four-examples/

[79] Marine Corps Recruit Depot Parris, U.S. Department of Energy Southeast CHP TAP, July 2021. https://chptap.ornl.gov/profile/121/MCRDParrisIsland-Project_Profile.pdf

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

[81] Castelo Branco, C.A.S., Moraes, F.P., Oliveira, H.A., Neto, P.B.L., Saavedra, O.R., de Matos, J.G., Oliveira, C.B.M., Ribeiro, L.A.d.S., Oliveira, A.C., Júnior, M.F.A., Pinheiro, L.d.P.A., and Cazo, R.M. "Mission Critical Microgrids: The Case of the Alcântara Space Center." Energies 2022, 15, 3-4, 22-24, 3226.

[82] Varley, D.W., Van Bossuyt, D.L. and Pollman, A. 2022. “Feasibility Analysis of a Mobile Microgrid Design to Support DoD Energy Resilience Goals” Systems 10, no. 3: 74. DOI: 10.3390/systems10030074.

[83] Cho, R. “Microgrids: Taking Steps Toward the 21st Century Smart Grid,” Columbia Climate School, April 18, 2017. https://news.climate.columbia.edu/2017/04/18/microgrids-taking-steps-toward-the-21st-century-smart-grid/

[84] “Microgrids for Commercial and Industrial Companies,” World Business Council for Sustainable Development, 22-23, Nov. 2017. https://docs.wbcsd.org/2017/11/WBCSD_microgrid_INTERACTIVE.pdf

[85] Renahan, T. “Realizing Energy Independence on U.S. Military Bases,” JFQ 103, 4th Quarter 2021.

[86] Marqusee, J., Schultz, C., and Robyn, D. “Power Begins at Home: Assured Energy for U.S. Military Bases,” Noblis, The Pew Charitable Trusts, Jan. 12, 2017. https://www.pewtrusts.org/~/media/assets/2017/01/ce_power_begins_at_home_assured_energy_for_us_military_bases.pdf

[87] Peterson, C.J., Van Bossuyt, D.L., Giachetti, R.E. and Oriti. 2021, G. “Analyzing Mission Impact of Military Installations Microgrid for Resilience” Systems 9, no. 3: 69. DOI: 10.3390/systems9030069.

[88] Butrimas, V. “Assessment study of cybersecurity of smart-grid technologies employed in operational camps,” 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

[89] Ukrinform, “Purpose of Meeting with Putin Depends on When Such Talks to Take Place,” 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

[90] Lyngaas, S. “Russian Hackers Allegedly Target Ukraine’s Biggest Private Energy firm,” CNN, July 1, 2022.

[91] Benner, K. and Conger, K. “U.S. Accuses 4 Russians of Hacking Infrastructure, Including Nuclear Plant,” New York Times, March 24, 2022. https://www.nytimes.com/2022/03/24/us/politics/russians-cyberattacks-infrastructure-nuclear-plant.html

[92] Tidy, J. “Ukraine Says it is Fighting First ‘Hybrid War’,” BBC News, March 4, 2022. https://www.bbc.com/news/technology-60622977

[93] Danyk, Y., Briggs, C., and Maliarchuk, T. (n.d.). “Features of Ensuring Cybersecurity of the Critical Infrastructure of the State.” Retrieved December 16, 2020, from http://tacs.ipt.kpi.ua/article/view/209484/209553

[94] Langill, J.T. “Defending Against the Dragonfly Cyber Security Attacks,” September 15, 2014. Retrieved December 16, 2020, from https://www.docdroid.net/hmws/belden-white-paper-dragonfly-cyber-security-attacks-pdf

[95] Baezner, M. “Cyber and Information Warfare in the Ukrainian Conflict,” October 01, 2018. Retrieved December 16, 2020, from https://www.research-collection.ethz.ch/handle/20.500.11850/321570

[96] Slowik, J. “Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE,” October 12, 2018. Retrieved December 16, 2020, from https://www.bgp4.com/wp-content/uploads/2018/10/CRASHOVERRIDE2018.pdf

[97] Kalutarage, H., Shaikh S., Lee B.S., Lee C., and Kiat Y.C. “Early Warning Systems for Cyber Defence,” in: Camenisch J., Kesdoğan D. (eds) Open Problems in Network Security. iNetSec 2015. Lecture Notes in Computer Science, vol 9591. Springer, Cham, 2016. DOI: 10.1007/978-3-319-39028-4_3.

[98] Chan, C., Dao, A., Hou, J., Jin, T. and Tuong, C. “Free Speech vs Maintaining Social Cohesion,” cs.stanford.edu. 2011 https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreeExpressionVsSocialCohesion/china_policy.html

[99] Voo, J., Hemani, I., Jones, S., DeSombre, W., Cassidy, D., and Schwarzenbach, A. “National Cyber Power Index 2020: Methodology and Analytical Considerations,” Harvard Kennedy: Belfer Center, 2020. https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf

[100] U.S. Energy Information Administration. “Electricity Explained,” 2020. Retrieved from eia.gov: https://www.eia.gov/energyexplained/electricity/electricity-in-the-us-generation-capacity-and-sales.php

[101] Anthropocene Institute. “How the Grid Works,” (n.d.). Retrieved from Anthropocene Institute, 2021.https://www.anthropoceneinstitute.com/science/grid/

Annex C – LITERATURE REVIEW

Peter Burgherr
Paul Scherrer Institut (PSI)
SWITZERLAND

C.1 INTRODUCTION

The Systems Analysis and Studies RTG SAS-163 “Energy Security in the Era of Hybrid Warfare” focuses on two main elements as already exemplified in its title. The scope of the literature review is bounded by these two key concepts, while it also investigates their interdependencies and relationships to other overarching concepts.

A main motivation for this study is that the past decade has seen an unprecedented increase of hybrid threats worldwide, and it is a major and growing challenge for individual countries and supranational entities such as the European Union (EU) or the North Atlantic Treaty Alliance (NATO) (Dupuy et al. 2021). Furthermore, cyber as a hybrid threat has the capability and capacity to directly impact NATO’s operational energy security (Dupuy et al. 2020).

A recent Google Scholar Advanced Search for the terms “Hybrid Threats” and “Hybrid Warfare” yielded a total of about 15,700 results, of which about 14,000 since 2014. This is a significant increase to the number of almost 10,000 hits given in a report published in 2020 by the European Commission’s Joint Research Centre (JRC) (Giannopoulos, Smith, and Theocharidou 2020). Overall, this confirms and highlights the importance of the topic on the global agenda and in different spheres, including politics and military, academia and private research and consulting, and the media and public at large. The specific methodological process used for the literature review is described in Section C.2.

The main elements and contents of the literature review are briefly introduced in the following two sections, whereas a detailed presentation of the findings and insights is given in Section C.3 and C.4, and Section C.5 provides a summary of recent developments and concluding remarks.

C.1.1 Definitions and Conceptual Developments

The term hybrid warfare appeared in the defence community with an article published in the US Naval Institute Magazine in 2005 (Mattis and Hoffman 2005). In the following years, Hoffman further developed the concept and defined hybrid threats as “a full range of different modes of warfare including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder” (Hoffman 2009; 2007; 2010) but see also (Qureshi 2020).

These recent conceptual developments were complemented by the recognition that hybrid and cyber threats are part of a megatrend that describes the increasing influence of new governing systems (Cagnin et al. 2021). Despite this fact hybrid warfare is nothing new, but as old as the Trojan Horse (Ducaru 2016). Numerous other examples have been stated, including the French Revolution and Napoleonic Wars, the Second World War, the Soviets in the Cold War, the Israel-Hezbollah War, the Israeli- Palestinian conflict, the Russian-Ukrainian conflict in Crimea and Eastern Ukraine, China’s island building in the South China Sea, etc. (Caliskan and Liégeois 2021). At the same time, it should not be considered old wine in new bottles because there are some new twists. Particularly in the cyber domain and the increasing threat of ambiguous cyber-attacks (Mazeikis et al. 2017). Furthermore, in a recent study that interviewed NATO officials most of them confirmed that hybrid warfare is not a new concept, broad and ambiguous, useful as a strategic communications tool, but of limited operational value (Caliskan and Liégeois 2021).

The roots of the concepts of hybrid warfare and threats are predominantly in the defence sector (e.g., operational and technological aspects) and linked to the geopolitical environment as well as socio-economic / political / cultural trends (Mälksoo 2018; Cohen, Han, and Rhoades 2020; Giannopoulos, Smith, and Theocharidou 2020). Generally, methodological frameworks and techniques for risk and resilience assessment and management form an essential base for quantitative evaluations, modeling and scenario analysis. Furthermore, the performance of systems exposed to threats can be assessed in many ways that are based on different conceptual foundations. Therefore, a better understanding of the commonalities and distinctions as well as trade-offs and synergies between concepts is needed (Galaitsi et al. 2021; Galaitsi, Kurth, and Linkov 2021).

Chapter C.3 is organized in three parts. It starts with an overview of the history, definitions and conceptual developments related to hybrid warfare and threats. The next section presents a discussion of the main implications concerning the concept's operational value and use for policy and strategy development. Finally, the relationships with related and overarching concepts are explored.

C.1.2 Hybrid Threat Assessment

The statement "data is the new oil" has been first made by Clive Humby and has since then been repeated regularly (Palmer 2006). This analogy is often used in positive context, but it can also create significant negative impacts in the sense that data breach and leak incidents are the "oil spills" in the digital information economy (Neto et al. 2021; Hirsch 2014). Incident and accident data for critical infrastructure and the energy sector in particular are systematically collected and available from numerous data providers either publicly or by subscription (Kim et al. 2018). In contrast, there are fewer information sources and databases for cyber incidents, and there are issues with regard to lack of standardized reporting, difficulty in consistently mapping security indicators, etc., which makes it difficult to judge the completeness of this data (Neto et al. 2021; Romanosky 2016). Specifically for hybrid threats, the situation is even less comfortable in terms of incident data, although it is generally recognized that that there is an increasing trend, which is often exemplified by activities in Ukraine (Butrimas et al. 2020; Dupuy et al. 2021; Thiele 2020). Independent from availability and quality of data, it is of crucial importance that the applied analytical methods and modeling frameworks are adequate, transparent, reproducible and appropriate for a study's scope and objectives because otherwise it is simply "garbage in – garbage out". Consequently, a diverse portfolio of approaches and methods have been proposed for analyzing hybrid threats and applying them to real-world problems (Guikema and Aven 2010; Nadolski and Fairbanks 2019; Balaban and Mielniciczek 2018).

Therefore, Section C.4 is split in three main parts. First, an exemplarily overview of existing and proposed approaches and modeling frameworks for hybrid threat assessment is given. This also includes consideration of their relevance for critical infrastructure protection and operation, policy and strategy development, and testing of emergency plans and procedures, etc. Second, an excursus on the role of insurance is presented, and how it can support and stimulate the deterrence and defence against hybrid threats. Third, this literature review also resulted in some spin-off research activities at the Paul Scherrer Institute (PSI), which are briefly described and presented.

Finally, Section C.5 provides a concise summary of the recent developments to provide an explicit connection to the geopolitical developments since the Russian invasion in Ukraine in February 2022, and some overarching conclusions and recommendations are presented.

C.2 LITERATURE SURVEY AND ASSESSMENT METHODOLOGY

Generally, the goal of the literature review was not to establish just another bibliography with relevant publications covering the topics of hybrid threats and energy security, but to explicitly allow incorporating additional concepts taking an integrated nexus perspective. Having such a broad scope, the review can serve different purposes. On the one hand, it provides an overview of the current state-of-the-art. On the other hand, it can be used to identify lessons learnt as well as to derive recommendations for future research directions, and to support complex decision-making by policy makers and other stakeholders, which needs to be informed by risks (and opportunities) in its broadest sense. Particularly, it enables a systematic and comprehensive analysis of trade-offs and synergies, which is a necessary prerequisite to 1) Reconcile diverging stakeholder preferences; 2) Cope with uncertainties; and 3) Identify and prioritize robust solutions with broad acceptance. This far reaching aspiration led to a literature database that has a much broader coverage than typical review articles that deal with the topics of hybrid warfare and hybrid threats in a narrower scope.

The individual steps of the applied literature review process are explained in the following. As a starting point, several recent publications on the topic by NATO, European Union and the Centre of Excellence for Countering Hybrid Threats (Hybrid COE) were chosen. In a second step, a keyword search was carried out in Google Scholar and Web of Science. Complementary searches were conducted in the OECD iLibrary, NATO's Science and Technology (STO) database, IEEE Explore, and Nexis Uni to ensure no key publications were omitted. The list of keywords included "Hybrid Threats", "Hybrid Warfare", "Energy Security", "Risk, and "Resilience", and was kept rather general and short on purpose. In this way, the initial set of publications was not yet constrained and reduced by a too restrictive search strategy. Next, a relevance judgment and refinement was undertaken, based on title, abstract and keywords, and if necessary, a full text screening to exclude publications that were not within the scope of this review. The final set of publications was then entered in the Mendeley reference manager that helps users to store, organize, annotate, share and cite references. For this purpose, a dedicated bibliography group entitled "Hybrid Threats" was created, and for each entry either the source file (e.g., pdf) or a DOI (Digital Object Identifier) /URL (Unique Resource Locator) was added to ensure that the original resource can be accessed.

The complete literature database consists of more than 300 documents. It includes a broad range of publication types such as journal articles, books, encyclopedias, handbooks, research reports, conference proceedings, dissertations and student theses, newspapers and magazines articles, and official publications. This literature review is organized by topics and thus only contains a selection of the most relevant references for each of them. However, the complete bibliography can be requested by the author of this contribution. Access to the Mendeley database is possible by registration, but the number of subscriptions is limited due to maximum number of users in a group. Alternatively, the database content is available in pdf format through the ResearchGate profile of the author.

C.3 EVOLUTION OF THE HYBRID THREAT CONCEPT

There is no unique or commonly agreed definition of the term hybrid threat. However, this does not point to an urgent need for action, and it is not an atypical situation as confirmed by the following examples from different but linked domains.

The concept of risk and risk assessment has a long history (Aven 2016), and already over 2400 years ago the Athenians assessed the risks before taking a decision (Bernstein 1996). In modern times, the Society for Risk Analysis (SRA) as one of its first actions in the 1990s established a committee that was supposed to define the word "risk". It gave up after four years and stated in its final report that maybe it is better not to define risk: "Let each author define it in his own way, only please each should explain clearly what way that is" (Kaplan 1997). Despite this inability to arrive at a common and broadly accepted definition of risk, the quantitative definition of risk is often based on the idea of a set of triplets. Fundamentally, it aims at answering three questions: 1) What can happen (or go wrong)? 2) What is the likelihood that it will happen? and 3) If it happens, what are the consequences? (Kaplan and Garrick 1981). To answer these questions, one has to establish a list of scenarios, and then to calculate a probability and consequence (extent of damage) for each of them. More recently, the concept of risk has also been extended to better incorporate aspects of uncertainty, knowledge, vulnerability and resilience to name a few (Aven 2011b; Aven and Kristensen 2019).

Energy security is another example of a complex concept that involves many disciplines, including 1) Engineering responsible for technical safety and sufficient capacity; 2) Economy concerned about functioning energy markets; and 3) Political sciences analyzing geopolitical security threats, among others. Thus, it is not surprising that there is no univocal and uncontested definition that grasps all aspects (Cherp and Jewell 2011; Ang, Choong, and Ng 2015). On the other hand, common elements in many definitions include 1) Physical availability and accessibility of supply sources, 2) Economic affordability, and 3) Long-term environmental sustainability (International Energy Agency 2007; European Commission 2000; APERC 2007).

In summary, the lessons learned from the still ongoing discussions about the definitions and concepts of risk and energy security apply to hybrid threats as well. This implies that we should not just aim for a clear, concise and complete definition, but it also has to fit the context, scope and objectives of a study, so that it can be applied and operationalized.

C.3.1 One Concept with Many Meanings

The first use of the term hybrid warfare is usually assigned to the book of Mockaitis entitled "British Counterinsurgency in the Post-imperial Era" (Mockaitis 1995). It took another decade until hybrid warfare received broader recognition, but it was still more a description of its characteristics than a formal definition (Mattis and Hoffman 2005). A next milestone was the publication of the seminal monograph by Hoffmann that on the one hand provided a detailed definition, and on the other hand led to a wide recognition and popularization among academics and military practitioners (Hoffman 2007). In this monograph, hybrid warfare is defined as:

> *Hybrid Wars incorporate a range of different modes of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder.*

In the years after, two main schools of thoughts further developed the original formulation of the concept by Hoffman. The first research stream stresses the coordinated and combined use of regular and irregular forces under a unified strategic direction as major element of hybrid warfare. In this respect, the book edited by Murray and Mansoor provides a major milestone and highly cited work (Murray and Mansoor 2012). It starts with making the argument that hybrid warfare is a normal part of warfare in general since ancient times, then presents in detail nine case studies, and concludes with the key lessons learned. These insights are not completely new, but also confirm and reinforce findings of previous studies or general quotes like Sun Tzu's guidance of knowing the enemy. The same approach to hybrid warfare gained additional support in subsequent studies (Deep 2015; Boot 2020).

Proponents of the second research stream suggest modifying and broadening the scope of the concept to include non-kinetic elements and techniques (Burbridge 2013; McCuen 2008; Glenn 2009). For example, the hybrid threat definition by Glenn (Glenn 2009) proposes that an adversary combines the following elements in a simultaneous and adaptive manner: On the one hand, political, military, economic, social, and information means, and on the other hand, conventional, irregular, catastrophic, terrorism, and disruptive/criminal warfare methods. They major conceptual difference of this definition of hybrid threats is that it equally builds upon military and non-military instruments.

The 2014 annexation of Crimea showed that the activities of Russia in Ukraine did not fit that well with previous conceptualizations of hybrid warfare because one of its main constituting elements was covert action and deception, i.e., to create ambiguity and to enable plausible deniability (Solmaz 2022). This perspective is very much in line with the so-called Gerasimov doctrine that advocates a mix of military and non-military means to achieve political goals and aims to intentionally blur the line between war and peace (Thiele 2016; Cederberg and Eronen 2015; Jones 2014). Consequently, subsequent publications of leading Western institutions stressed the aspects of below threshold activities in connection with kinetic and non-kinetic methods to characterize hybrid warfare (NATO 2014; 2021; European Commission 2016; European Centre of Excellence for Countering Hybrid Threats (Hybrid COE) n.d.). The concept of hybrid warfare has continued to evolve and adapt to date, referring to cyber-attacks, economic coercion, disinformation campaign, election meddling, outlaw motorcycle gangs, and migrants as a political weapon, among others (Kuczynski 2019; Harris 2020; Deni 2017; Shedd and Stradner 2020; BBC 2021). A recent article by Jacobs and Kitzen from 2021 provides an excellent overview of the discussions about hybrid warfare in the last two decades (Jacobs and Kitzen 2021).

In conclusion, defining hybrid warfare is not an easy task and more than an intellectual or academic exercise because the operationalization and application of the concept in a real-world concept is of crucial importance. Therefore, this section ends with an overview of definitions ranging from a pure battlefield perspective to achieving political objectives or just referring to non-kinetic destabilization operations.

On the one hand, the US Army has adopted in many of its official documents either Hoffman's original definition of hybrid warfare or some modified variants of it (Solmaz 2022). On the other hand, the United States Global Accountability Office (US GAO) clearly stated in a report published in 2010 that the US Department of Defence (DoD) has not officially defined hybrid warfare and at this time has no intention to do so (US GAO 2010). Another study concluded that the US has formally identified hybrid threats, and that the multitude of descriptions and definitions focus on the concepts form and function of a hybrid threat, but do not sufficiently address logic (McCulloh 2012). While earlier definitions were mostly battlefield-centered, more recently non-kinetic means have come into consideration, defining hybrid warfare as "the use of political, social, criminal, and other non-kinetic means employed to overcome military limitations" (TRADOC G-2 2015).

In contrast, NATO and the EU characterize hybrid warfare as a means to achieve political objectives by using both kinetic and non-kinetic methods, but activities remain below the threshold of traditional war.

NATO provides the following definition on its website (NATO 2021):

> *Hybrid threats combine military and non-military as well as covert and overt means, including disinformation, cyber-attacks, economic pressure, deployment of irregular armed groups and use of regular forces. Hybrid methods are used to blur the lines between war and peace and attempt to sow doubt in the minds of target populations. They aim to destabilise and undermine societies.*

Along the same lines, the European Union's (EU) Joint Framework on countering hybrid threats defines hybrid threat as (European Commission 2016):

> *The concept of hybrid threats aims to capture the mixture of conventional and unconventional, military and non-military, overt and covert actions that can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare.*

The definition of the European Centre of Excellence for Countering Hybrid Threats is rather similar to those of NATO and EU (European Centre of Excellence for Countering Hybrid Threats (Hybrid COE) n.d.):

> *The term hybrid threat refers to an action conducted by state or non-state actors, whose goal is to undermine or harm a target by influencing its decision-making at the local, regional, state or institutional level. Such actions are coordinated and synchronized and deliberately target democratic states' and institutions' vulnerabilities. Activities can take place, for example, in the political, economic, military, civil or information domains. They are conducted using a wide range of means and designed to remain below the threshold of detection and attribution.*

Similar discussions are going on in other regions of the world such as the Asia-Pacific. For example, the Singaporean defence minister gave the following hybrid threat definition (I. Li 2020):

> *Hybrid warfare is 'an orchestrated campaign to fracture the solidarity of the target nation through undermining its defences in civil, economic, social, psychological and military spheres.*

The concerns about hybrid threats in Singapore are mostly related to the fact that the country is surrounded by water on all sides with no natural resources and strongly depending on maritime trading, which provides a low-cost high-impact threat (B.C.H. Ang 2018).

Despite the general lack of a common and universally accepted definition of the concept of hybrid warfare as well as hybrid threat, a number of main characteristics and key aspects can be established that allow deriving specific implications to make the concept applicable in an operational, real-world context.

C.3.2 Operational Value and Strategy Development

The previous discussion about the definition of hybrid warfare and hybrid threats clearly highlighted that there is a grey zone between war and peace. Almäng proposed to tackle this vagueness from a philosophical perspective (Almäng 2019) along an ontological and epistemological dimension (Almäng 2019). The former refers to the question if a conflict classifies as war or not, described by the attributes vague and non-vague. The latter concerns uncertainty where one or both of the parties to the conflict lack knowledge of the relevant contextual parameters of the conflict. The corresponding categories are transparent when both parties know all relevant institutional facts and opaque when it is not the case. Combining both dimensions leads to four different types of conflict, but only a non-vague and transparent conflict qualifies as a normal war, whereas the other three combinations are examples of hybrid wars. A conflict can also move from one category to another. For example, during the initial phase of the invasion in Crimea 2014, the Ukrainian government considered the "little green men" as unidentified people, but later on the Russian involvement in the attack became clear, meaning that the conflict was still vague, but no longer opaque.

Similarly, NATO's Allied Joint Doctrine demonstrates the evolution of hybrid war from a narrow definition under other threats in 2010, to a much more exhaustive definition under its own heading in 2017 (NATO 2017; 2010). However, adding more details and nuances, also introduces a higher degree of vagueness as described before. Furthermore, the grey zone in hybrid conflicts can be exploited in different ways. The geostrategic momentum utilized by China can be attributed to so-called "offensive hybridism", whereas Russia's actions are associated with "hybridism in retreat" (Belo 2020). Finally, modern hybrid warfare provides a wide range of applications that can affect almost all areas of activity of a nation, and thus lead to harmful consequences in civil society and the military environment (Barbu 2020). In summary, hybrid threats and conflicts should not be viewed as a homogenous phenomenon, but rather require a deep understanding to identify the distinct tools and combination of techniques used by the attacker, so that it can be counteracted with diverse, tailored approaches linked as well to crisis management.

Defence and security are areas in which there is an increasing need for action both at a regional and global level. The constantly evolving nature of internal and external security threats results in more complex, multi-faceted, hybrid and cross-border activities, which are also influenced by technological advances and digitalization in particular (Dokos 2019). For example, the Global Risks Report of the World Economic

Forum as well as opinion polls like the Eurobarometer show a broad range of themes about which both experts and the public are increasingly concerned, including economic security, social cohesion, political radicalization and physical security (World Economic Forum 2021; European Commission 2022; European Political Strategy Centre 2019). In the last four Eurobarometer surveys, 77 – 78 % of Europeans expressed their support for a common defence and security policy among EU Member States. The various threat assessments and surveys mentioned above show a rather good agreement on the types of security threats and risks at different scales (i.e., global, European, national), although the actual likelihoods and impacts may differ The main categories are (Dokos 2019):

- External threats (e.g., great-power competition, regional conflicts).
- Damage to critical infrastructure.
- Pandemics.
- Population movements.
- Terrorism.
- Natural and man-made disasters.
- Organized crime.
- Cyber threats.
- Hybrid threats.

A key aspect of hybrid threats is that they can be applied to a broad range of targets, such as cyber-attacks on critical information systems, the disruption of critical services (e.g., energy supplies, financial services), undermining of public trust in government institutions or the deepening of social divisions. Another aggravating factor is that hybrid threats often occur at the energy security nexus with many controversial issues. This includes reduction of foreign dependencies through diversified options like new pipelines, US shale gas, Liquefied Natural Gas LNG) imports or increased storage capacity. Furthermore, the global energy transition and the race to Net Zero will produce winners and losers at the global and regional level. In this context, key challenges for the future include the emerging technological dependency and know-how, control and availability of so-called rare, raw materials (cobalt, lithium, etc.), and increased (cyber) vulnerabilities due to digitalization and decentralization of the energy system and interconnected systems and services. For a more detailed discussion compare (Dokos 2019).

The ongoing evolution of the energy sector with the energy transition and the digitalization of the whole infrastructure as the major trends has led to an increase and diversification of cyber threats due to the pervasive use of Information and Communication Technologies (ICT) and new data interfaces (European Cyber Security Organisation 2018). This makes the energy sector one of the three most affected sectors together with finance and ICT.

In the context of hybrid threats, Industrial Control Systems (ICS) due to their nature and function are critical infrastructure themselves and need to be protected from both physical and cyber threats. Especially cyber threats have the potential to modify and disrupt their mode of operation, take the role of an information extraction vehicle, and ultimately turn against itself (Beretas 2020). Therefore, security policies need to be designed and implemented that not just protect against cyber threat, but also enable system recovery without compromising operation and reliability of often interconnected systems as otherwise cascading effects may occur. The portfolio of methods and tools that can be applied is broad and many already exist. Security assessment is essential, but it is recommended to complement it by safety assessment because both are different sides of the same coin and should not be treated in isolation. Assessments are also not a one-time activity in the sense that the Chief Security Officer (CSO) once per year reports to the board of directors, and then the subject is checked off. It is rather an iterative and repeated process that needs to be carefully designed and becomes part of the DNA of a company, organization, authority, country, etc. In other words, it requires strong internal and external support from decision and policy makers and should be formalized as part of a comprehensive risk governance process. In particular, this calls for an integrated methodological framework that is not just focused on technical features, but also considers organizational aspects and supports a systemic and transdisciplinary approach, which allows identifying risk governance deficits and addressing them from a technical, human factor, legal and regulatory perspective (Aven 2011a; Renn et al. 2020; Renn 2021; Sidortsov, Ivanova, and Stammler 2016).

Hybrid threats are a continuous, evolving challenge, calling for societal resilience and a whole-of-government approach. They pose a major concern to NATO and many European countries since the start of Russia's conventional and unconventional war in Ukraine in 2014 (Bajarūnas 2020) that also systematically targeted critical energy infrastructure (Butrimas et al. 2020). This is even more prominent since Russia started a full-scale invasion of the country on 24 February 2022 (Andrew 2022).

Specific strategies and counter measures have been proposed to recover from hybrid threat events and crises in general (Wigell, Mikkola, and Juntunen 2021). On the one hand, risk mitigation involves the use of processes and policies to reduce the overall risk or impact of hybrid threats, which comprises three elements, namely prevention, detection and remediation (Steingartner, Galinec, and Kozina 2021). Similarly, the strategy of NATO to counter hybrid warfare is based on the three pillars prepare, deter and defend, which also applies to the cyber domain. Furthermore, a pragmatic approach is advocated, based on a comprehensive description and analysis of the phenomenon, followed by its operationalization through the development of a relevant strategy, instead of scholastic and conceptual efforts aiming at a unique definition (Ducaru 2016). On the other hand, resilience is understood as a complex process of adaptation and change (Wigell, Mikkola, and Juntunen 2021). In an operational context, resilience incudes both systemic resistance and general adaptive capacities (Tierney 2014). Furthermore, resistance can be categorized into physical or mental robustness and systemic redundance, whereas adaptive capacities refer to resourcefulness of society as a whole (Juntunen and Hyvönen 2014). Consequently, a whole-of-society approach to identify hybrid activity and to respond to hybrid attacks is definitively a meaningful and comprehensive approach, but also complex because a significant amount of coordination is needed between many stakeholders and decision makers (Giles 2019). Already a whole-of-government approach that "only" requires coordination between government agencies is a challenging endeavor, for which Singapore is one of few successful examples (Ho 2018). Similarly, smaller countries like Sweden or Finland apply a total defence concept, while large organizations such as NATO have developed specific mechanisms for this purpose, for example the Very High Readiness Joint Task Force (VJTF) (Giles 2019). Finally, yet importantly, it is important to understand and acknowledge that the evolving cyber threat environment and Cyber Threat Intelligence (CTI) should support comprehensive strategic-political decision-making (Ertan et al. 2020).

C.3.3 Relationships with Related and Overarching Concepts

In this section, hybrid threats and warfare are put in the broader context by looking at their connection to and integration with related and overarching concepts. Although security is of paramount importance for every country and its people, there are other challenges, which modern society faces and that need to be coordinated. This of course also implies that there is no single optimal and broadly accepted solution, taking into account all societal needs and concerns equally and at once, calling for trade-offs and compromises. In other words, the phrase "the best of all possible worlds" coined by the German Enlightenment philosopher Gottfried Leibnitz does not apply to our complex and intertwined socio-technical systems. Inherently, such a broad stance cannot be discussed in all of its facets in this literature review, which is why the focus is on few selected topical areas.

C.3.3.1 Energy Transition Between the Poles of Climate Change Impacts and Net Zero Targets

The concept of the energy trilemma has been introduced by the World Energy Council (WEC) in 2010, and since then the associated, annual report has provided an independent and objective rating of a country's energy policy and performance (WEC 2020). The Energy Trilemma Index uses and indicator-based methodology to assess the three dimensions of environmental sustainability, economic competitiveness and energy security, and to evaluate and balance potential trade-offs and conflicts. Environmental sustainability is usually placed first because of the imminent and global threat that climate change poses to humankind and our planet. However, it is often defined solely as reaching net zero in terms of Greenhous Gas (GHG) emissions, which neglects other important issues such as for example critical materials, waste, biodiversity, toxicity, etc. Furthermore, future scenarios based on energy system models are looking for the optimal, least-cost pathways to net zero. Energy security was usually ranked on a distant third place, but since the start of the Russia's war against Ukraine, it has climbed to the top on national and international political agendas as well as media and public interest. To put it simple, energy security is about "keeping the lights on". Following the WEC's definition, it aims to meet current and future energy demand reliably, withstand and bounce back swiftly from system shocks with minimal disruption to supplies.

The energy sector and its transition to net zero with low-carbon technologies is facing additional challenges. First, it experiences unprecedented shifts in supply and demand, which are further accelerated by the geopolitical developments in the last few months. Second, the transition is shaped by the digitalization of the industry, which is both an enabler of resilience, but also a threat. In particular, a digital energy sector is exposed to various factors that can increase vulnerability to digital disruption and cyber threats. This includes:

1) A rapid pace of innovation;
2) Technological complexity;
3) Data sharing and interconnectivity;
4) Rising cyberattack sophistication; and
5) The sector's attractiveness as a cyber target (WEC 2019).

Within a defence and military perspective, it has been recognized that climate change can increase pressure on the military sector to contribute more significantly to greenhouse gas emissions reductions, but there are also additional concerns that have emerged recently.

For example:

1) Effects of climate change impacts on societal resilience;
2) Information warfare discrediting climate change research; and
3) Lack of legal and regulatory frameworks for risk-informed governance of geoengineering technologies potentially deployed in the future by different actors (Briggs 2020).

Furthermore, the case of so-called hybrid or "unnatural" disasters has been discussed that can be triggered by sabotage or military actions (e.g., intentional breaching of dykes by the Dutch Army and targeting dams during WWII, the Korean war, and most recently in Ukraine). Similarly, deliberate environmental interventions (e.g., herbicides, forest fires) to reduce the opponents "natural" advantages (Briggs and Matejova 2019). Despite this well-known history, the capabilities available already today and potentially in the future for manipulations of the environment and energy systems are unprecedented both in terms of variety and impact. Finally, there is also a growing relationship between energy issues and defence planning, and how this affects convergence of security, economic and environmental decision-making (Samaras, Nuttall, and Bazilian 2019; Kerber et al. 2021), which links back to the initial presentation of the energy trilemma.

C.3.3.2 Energy Security, Resilience and Hybrid Threat Nexus

Modern society relies upon complex and interconnected systems that are often described with attributes such as socio-technical, cyber-physical, etc. These systems are exposed to a variety of hazards and threats, challenges and disruptive events that can affect their performance. However, the measurement of what is a "good", or sufficient, acceptable, required performance is not straightforward, and can be characterized by many concepts, but the relationships, synergies and trade-offs between these are often not systematically addressed (Galaitsi et al. 2021; Liu et al. 2018; Fiksel 2006; Keskinen, Sojamo, and Varis 2019).

Historically, critical infrastructure protection relies on a risk model that defines risk as the triplet of threat, vulnerability and consequence (US Department of Homeland Security (DHS) 2013; Moteff and Parfomak 2004). On the one hand, it builds on earlier work by the Sandia National Laboratory on adversarial infrastructure risk (Baker et al. 2002). On the other hand, it is an extension and variation of the traditional risk model that represents risk as the product of likelihood (or probability) and consequence (Kaplan and Garrick 1981; Haimes 2009). Despite its broad acceptance and wide use in practical applications by authorities, businesses and many organizations, this tripartite risk approach for critical infrastructure protection has received some criticism. This includes issues to account for correlations among its components, non-additivity of risks, potential lack of optimal resource allocation, and elements of subjectivity and ambiguity (L.A.T. Cox 2008). Furthermore, national risk assessments for critical infrastructure often use risk matrices because they provide a simple tool for assessment of the level of risk, priority setting and management action, although they can suffer from several shortcomings when not applied with caution (L.A. Cox 2008; Duijm 2015). Lastly, another recent study investigated how well ISO Standards are aligned with current state-of-the-art approaches and methods in the scientific risk management literature. The authors concluded that industrial standards 1) Suffer from a lack of guidance on how to perform risk analysis, 2) Are not properly taking into account properly the scientific state of knowledge, and 3) Are not appropriate to manage risks of complex socio-technical systems (Björnsdóttir et al. 2021). Consequently, this highlights that the assessment of critical infrastructure disruption and subsequent crisis management is a challenging and complex process that involves many stakeholders, especially leaders from the public, private, military and non-profit sectors. It is crucial to widen the often-applied technical approaches to crisis management of disruptions towards a holistic perspective, including: 1) The institutional, economic and social context; 2) New and rapidly evolving challenges such as cybersecurity and malign influence; and 3) Establish a framework for core crisis management tasks and leadership (Stern and Nussbaum 2022).

In recent years, resilience has been extensively analyzed often as an extension of classical risk assessment to achieve a better representation of both the pre-event (e.g., prepare, absorb) and post-event (e.g., recover, reconfigure) phases (Gasser et al. 2019). However, most applications are related to physical infrastructures, while the cyber domain is lacking behind (Hausken 2020). Consequently, cyber resilience requires a comprehensive and inter-disciplinary approach because it concerns a broad range of thematic areas and domains, e.g., infrastructure, management, policy, economics, insurance, and the internet of things (Hausken 2020). The authors propose that a comprehensive approach to cyber resilience should address seven focus points, namely:

- Technical focus on controls, measures and recovery mechanisms.
- Organizational aspects.
- Human behavioral patterns.
- Policy and regulation.
- Learning from the past, but also adapting to the present and evolving into the future.
- Collect and compile historical data of cyber incidents and their causes and consequences.
- Advantages of cyber resilient actors.

Based on the above discourse, it becomes evident that the energy dimension poses a significant challenge in the assessment and management of hybrid threats and warfare, requiring adaptation and resilience building in specific areas. This includes:

1) Intelligence sharing and strategic analysis;
2) Political dialogue on energy developments;
3) Training and exercises;
4) Strategic communication;
5) Involvement of the private sector rand energy organizations; and
6) Close relationship between NATO and EU (Rühle and Grubliauskas 2015).

The year 2014 marked an "inflection point" in the sense that NATO started to use the term "Hybrid Warfare" to make sense of new security challenges, and as a response NATO has referred to the concept of resilience as a countermeasure (Hartmann 2017).

In a security and policy context, resilience has initially been viewed as an ambiguous term and a concept difficult to transform into practice (Hanisch 2016). In contrast, the focus in in disaster and community resilience was originally on technical aspects, which is sometimes also called resilience engineering (Gasser et al. 2019). These contradictory positions can be reconciled by applying a holistic resilience framework that does not just rely on technological and financial aspects, but also considers strategic, organizational and operational aspects as core resilience areas (Natale, Poppensieker, and Thun 2022).

Coming back to hybrid threats in the context of NATO, the Alliance's future strategic concept should be based on resilience as a guiding principle and a key element, which additionally can serve as first line of defence in an increasingly complex security environment (Hartmann 2017). For example, Russia's hybrid warfare efforts are based on strategic thinking and several principles, including among others:

1) Identify and exploit vulnerabilities using scientific methods;
2) Apply unpredictable and opportunistic strategies;
3) Implement hybrid threats over extended periods; and
4) Conduct disinformation and fake news campaigns (Hartmann 2017).

The same study also proposes resilience as a countermeasure that must comprise the capability to be prepared and to absorb shocks, recover fast to counteract and learn from experience.

The past years have also shown that adversaries have actively targeted critical infrastructure of the USA, European Union and NATO, particularly focusing on energy, transportation, information and communications sectors to impact the defence industry and to undermine military capability and readiness (Evans 2020). The ongoing Russian war in Ukraine also demonstrates the pervasive use of computational propaganda by using algorithms, automation and big data as well as social engineering and its impact on critical infrastructure (Bradshaw and Howard 2019; 2017; Pollack and Ranganathan, n.d.).

Moreover, current geopolitical developments highlight as well that energy security concerns are not limited to oil, but also concerns natural gas and nuclear energy, and even renewable energy sources have more or less critical geopolitical aspects (Hafner and Tagliapietra 2020). Its effects are broadly recognized with regard to the global energy transition and its relevance for topics such as security of supply, import dependence and resilient national energy systems. However, there are also clear and manifold implications in the context of hybrid threats and warfare. Furthermore, geo-economics is an aspect of globalization that is of outmost importance, while at the same time I strongly dependent on infrastructure, and in turn infrastructure is often spatially linked to multiple state- and non-state interests (Strobl and Borchert 2022). Last but not least, this also includes supply chain resilience, since it is a key aspect in the increasingly complex and interconnected global context in which countries, businesses and other entities operate, and which ultimately affects society as a whole. A recent study demonstrated this for the COVID-19 pandemic, but its key findings can also be considered relevant for hybrid threats (Golan, Jernegan, and Linkov 2020). Similarly, other studies have analyzed resilience of critical infrastructure in the context of stress testing and compound threats (Wells et al. 2022; Linkov et al. 2022).

In summary, a comprehensive framework to strengthen resilience for countering hybrid threats needs exceptional efforts and international coordination to develop and implement a more specific set of measures and policies, which are then also effectively put into action. Best practices and a model of preparedness based on the concepts of whole-of-government, whole-of-society, and strategic, operational and societal resilience can play a key role in such initiatives (Wigell, Mikkola, and Juntunen 2021).

C.4 APPROACHES FOR HYBRID THREAT ASSESSMENT

The operationalization of the hybrid threat concept requires that transparent and consistent analytical approaches and methods are developed, tested, and applied in a real-world environment to support strategic decision. A comprehensive overview of methodological approaches and modeling frameworks is outside the scope of this conceptual review on the thematic complex of hybrid threats. Nevertheless, the following sections provide a concise overview of current state-of-the-art frameworks and methodological approaches, and the references cited can be used as a starting point for more detailed information on this thematic area.

C.4.1 Approaches and Modeling Frameworks

Recently, the Joint Research Centre (JRC) of the European Commission (EC) and the European Centre of Excellence for Countering Hybrid Threats (Hybrid COE) have jointly developed a conceptual model for characterizing Hybrid Threats, and subsequently analyze them by means of a methodological framework (Giannopoulos, Smith, and Theocharidou 2020). The model combines a narrative and visual representation, which builds upon four main pillars. These are actors, domains, tools and phases, and additionally links between them are identified. Overall, it provides a flexible framework or blueprint that can be adapted to the requirements of individual EU and/or NATO member states. Lastly, the associated methodological framework has been applied to a number of case studies to assess its analytical value and usability under real-world conditions. This conceptual model has also been used as a starting point to develop an indicator-based approach to assess the resilience of the European natural gas network against hybrid threats (see Section C.4.3).

In the USA, the Department of Homeland Security (DHS) has been established as a direct consequence of the 9/11 attacks, and is responsible for critical infrastructure protection, covering aspects of risk, security and more recently resilience (Doty 2015). In 2018, the Cybersecurity and Infrastructure Security Agency (CISA) was created to lead the cybersecurity and infrastructure security programs, operations, and policy through its key mission areas, namely cybersecurity, infrastructure security, and emergency communications (CISA 2021). Similarly, NATO has founded several Centres of Excellence (COE) that address and analyze topics related to the nexus of energy security, cybersecurity and hybrid threats. This includes the NATO Energy Security Centre of Excellence (ENSEC COE) (Butrimas 2021), the European Centre of Excellence Countering Hybrid Threats (Hybrid COE) (Mumford 2020) the NATO Strategic Communications Centre of Excellence (NATO Stratcom COE 2020), and the NATO accredited Cooperative Cyber Defence Centre of Excellence (CCDCOE) (Štrucl 2021). More recently, an Indo-Pacific hybrid threat center has been proposed (Seebeck, Williams, and Wallis 2022).

In the context of hybrid threats, specific areas have become a major concern for governments, authorities, and the military, but also received increased attention by the media and public in the past years. Few selected examples include the following:

- Information warfare or malign influence, which through disinformation, cognitive hacking and other social engineering techniques aimed at creating uncertainty, ambiguity and fear that in turn foster destabilization and influencing democracies (Dowse and Bachmann 2022).
- In the past years, the Arctic security environment has seen “a return to great-power competition” due to geostrategic interests, potential vast deposits of mineral resources and raw materials, but also discussions around the themes of hybrid threats or grey-zone warfare (Grätz 2012; Alessa et al. 2021; Østhagen 2019).
- The Black Sea region is another area where the competition of Russia and the West about the future of Europe takes place. The Russian strategy is a perfect example for a hybrid approach by employing a variety of non-military and military instruments to advance its goals, which requires a sustainable Western strategy to counter Russian aggression, protect common interests, and foster regional stability (Flanagan et al. 2020).
- Another area of active development concerns cyber information sharing models and information management frameworks to identify crucial factors, which support the establishment of early warning systems (Simola 2021; Cullen and Wegge 2022).
- Last but not least, preparation for, identification of and response to hybrid threats from state actors pose a major challenge because both the number of activities as well as their level sophistication have substantially increased over the last years, and the likely sabotage attacks that caused the North Stream gas leaks are just the most recent and prominent example for this trend (Speranza 2020; Siddi 2020; Plucinska 2022).

Concerning cybersecurity, a study by Homeland Security Systems Engineering and Development Institute carried out a survey and comparative assessment of cyber threat modeling frameworks and extended an existing framework to serve as a basis for cyber threat modeling for a variety of purposes (Bodeau, McCollum, and Fox 2018). In particular, the comparison included threat modeling frameworks (NIST, CBEST, COBIT-5), threat modeling approaches (STRIDE, DREAD, OCTAVE, TARA), specific threat models such as enterprise-neutral (ATT&CK, CAPEC) and enterprise-oriented (TARA, NSCSAR). Lastly, this study proposed an initial framework and high-level model, tailored from NIST SP 800-30R1 and drawing from numerous other surveyed sources, for use by the Next Generation Cyber Infrastructure (NGCI) Apex program.

Other notable model developments in the cybersecurity domain include the following examples.

- The threat Operating Model (TOM) that applies data analytic approaches to facilitate automated risk assessment, and hence achieve the early warning of likely cyber-attacks. (Bo et al. 2019).
- Defending a cyber-system and especially the effect of an early warning mechanism on the system reliability has become of vital importance because of the increasing reliance on networks (Chen, Xu, and Shi 2018).
- The reliable functioning of a country’s critical infrastructure has led to numerous sectoral cybersecurity models, e.g., for oil and natural gas (DOE 2014).
- The European Network of Transmission System Operators for Electricity and Gas (ENTSO-E and ENTSO-G) regularly publish a joint scenario report for the whole energy system that provides an assessment of the infrastructure from an integrated systems perspective (ENTSO-E and ENTSO-G 2022).
- The Monetary Authority of Singapore (MAS) has proposed a selection of key indicators for the financial that can be collected and tracked through time (Goh et al. 2020). These include event studies, Value-at-Risk (VaR), custom surveys, structured presentation via a cyber-RAM (Risk Assessment Matrix) and financial-cyber network maps. Some of them could also be adapted so that they can be applied to hybrid threat assessment.

Although, the development of sophisticated, state-of-the-art frameworks and methodological approaches is a crucial part to deter and counter hybrid threats, it needs to be embedded in a broader portfolio of operational, strategic and policy measures. The European Union has designed a portfolio of countermeasures against hybrid threats that includes both an external view on ongoing crises at its Eastern and Southern neighborhoods, and inward focused measures to secure the EU's borders, critical infrastructure and information environment, which is vital for Europe's digital economy, as well as its cyber, maritime, space and energy domains (Fiott and Parkes 2019). Another important pillar concerns the understanding and processing of social media data that is of high strategic importance for security applications (Dragos, Forrester, and Rein 2020). The extremely voluminous and noisy data together with fast changes in topics pose a tremendous challenge to mining of social streams and analyzing its dynamics, but this study describes three main approaches, namely 1) Machine learning techniques; 2) Semantic-driven algorithms; and 3) Indicators from sociology, linguistics and authority-provided inputs. Most commonly supervised machine learning is used to perform text analysis. However, the disconnected use of machine learning models and semantic-driven approaches has several weaknesses, including the utility and accuracy of methods and techniques applied.

Finally, all of these analytical activities need to be transferred to a real-world context. This need to train decision makers has been recognized for long time, for example for emergency management of natural disasters, large-scale industrial accidents and malicious activities (Crichton, Flin, and Rattray 2000). There are diverse approaches and methods, including for example:

1) Tactical Decision Games (TDG) to practice non-technical skills relevant in an emergency situation, but they are not script-driven, i.e., no limits exist with regard to the decisions that can be made.
2) Table-top exercises (TTX) involve key personnel / teams that in an informal, discussion-based setting discuss their roles and responses during an emergency using one or more simulated example scenarios to assess plans, policies and procedures.
3) Full-Scale Exercises (FSE) are at the other end of the spectrum and comprise a multi-agency, multi-jurisdictional and multi-disciplinary exercise that involve both functional (e.g., joint field office, emergency operation centers, etc.) and "boots on the ground" response (e.g., firefighters decontaminating mock victims).

A more detailed overview and description of the different types of discussion-based and operations-based exercises can be found in the following DHS publication (DHS 2007).

C.4.2 Role and Contribution of Insurance

At a first glance, insurance may not seem to be connected to cybersecurity and hybrid threats, but it can play a crucial role in the mitigation of direct and indirect financial impacts, promote increased preparedness, and similar to academia provide cross-fertilization to develop better analytical models for the assessment of hybrid threats. Therefore, this section offers a short introduction on ongoing activities and trends in this sector.

Modern society becomes increasingly dependent on both information technology (IT; data and flow of digital information) and operational technology (OT; operation of physical processes and the machinery used) and related services. Therefore, the risk management of cyber incidents is of pivotal importance, and cyber insurance is one tool among others (Franke and Draeger 2019). The authors of this study propose two simple models, i.e., one that looks at the impact on aggregated claims cost (insurers perspective) and one that considers the impacts of limited incident management capacity (insured's perspective). Furthermore, various methods and key performance indicators from the financial sector (e.g., Value-at-Risk) have been proposed and applied within a cyber-risk context. On the one hand, they can be helpful to improve cyber management strategies, and on the other hand, they provide instruments for insurance companies to price cyber insurance contracts, and to set minimum capital requirements defined by the regulators.

In a broader context, cyber risks are of critical importance because the online connection and (inter)dependencies of infrastructure and services is increasing at an unprecedented speed. However, the assessment and management of cyber risks poses a very difficult task because data on both near -misses and successful attacks as well as corresponding losses are scarcely disclosed (Giudici and Raffinetti 2021). Furthermore, there are few loss models for cyber data, and none for ordinal cyber-risk data. Therefore, the authors of this study developed a rank-based statistical model that is simple to implement and interpret when applied to real-world conditions. While this approach is feasible if only ordinal severity levels of cyber-attacks are available, efforts within (re)insurance aim at the development of full-scope, quantitative accumulation risk models. While this is well-known and established for natural hazards, it is still at a rather early stage for cyber risks.

Overall, the rapidly changing and evolving cyber landscape and in particular the associated digitalization of modern society has led to a substantially broader range of threats and vulnerabilities (Carter, Pain, and Enoizi 2022). Not surprisingly, ransomware and supply chain attacks in particular have become more frequent during the ongoing COVID-19 pandemic, and with them wider recognition of the potential for large-scale economic disruption from malicious cyber incidents. The report also makes the following statements. First, a dedicated market for cyber insurance has developed, and a wider class of risks is covered, including first- and third-party losses. Second, accumulated losses of some cyber risks caused by malicious cyber activities may go beyond the capacity of the private (re)insurance sector. Third, this raises the question if additional mechanisms involving governments and/or Public-Private-Partnerships (PPP) may be needed to finance extreme cyber risks. Ultimately, some form of government backstop or PPP to finance extreme cyber risks will be needed.

C.4.3 Spin-Off Activities of the Literature Review

Within the Future Resilient Systems (FRS) program of the Singapore ETH Centre (SEC) the Technology Assessment Group of the Paul Scherrer Institute (PSI) started to analyze the resilience of the European natural gas network using complex network analysis. This resulted in publications on assessing the performance of the network for selected supply disruption scenarios and the potential role of storage facilities (Lustenberger et al. 2019). Furthermore, a case study of the regional distribution natural gas network for the Greater Leipzig area was carried out to simulate the recovery dynamics after a shock event (e.g., flood) (Kyriakidis et al. 2018).

In the past two years, this analysis of the European natural gas network has been extended to achieve a better understanding of its exposure to hybrid threats, and how potential impacts can be evaluated at the policy level and for individual countries. Conceptually, this research built upon the conceptual framework that has been proposed in a joint report by the European Commission's Joint Research Centre (JRC) and the European Centre of Excellence for Countering Hybrid Threats (Hybrid COE) (Giannopoulos, Smith, and Theocharidou 2020).

Specifically for this study, a comprehensive set of indicators has been established and quantified, categorized into four major resilience dimensions, namely i) Infrastructure; ii) Socio-economic; iii) Political; and iv) External factors. While the infrastructure indicators were making use of the previously described complex network analysis, the indicators for the other dimensions were based on data from trusted, reliable and publicly available sources from international organizations and national authorities. The indicator-based approach has then been complemented with a synergy of Multi-Criteria Decision Analysis (MCDA) methods to assess the resilience and energy security performance in the context of hybrid threats. A unique feature is that it applies a transparent and comprehensive methodological approach, including an interactive and iterative exchange between the analyst and decision maker (Siskos and Tsotsolas 2015; Siskos and Burgherr 2021). The main objectives were threefold:

- Elicitation of preferences from different decision makers.
- Identification of potential changes in preferences due to recent geopolitical events.

- Comparison of 35 European countries with regard to their resilience and energy security performance against hybrid threats.
- Assessment of the robustness of the country ranking.

The main conclusions of this study can be summarized as follows.

- Development and implementation of a transparent and consistent methodological framework that facilitates interaction between analyst and decision maker.
- Consideration of different decision makers, which is essential to account for trade-offs and synergies between indicators, and to assess the robustness of the ranking.
- Overall, preliminary results show that indicators from the infrastructure and socio-economic dimensions are most important, followed by the external factors, whereas the political dimension played a minor role.
- This finding highlights the importance of a combined energy security and cyber-physical systems perspective.
- The composite Hybrid Threat Index (HTR) provides an easy and straightforward measure for the comparative evaluation of the European natural gas network in the context of hybrid threats at the country level.
- Furthermore, it can help to increase understanding and trust among diverse stakeholders (e.g., industry, authorities, political decision makes and the public).
- Ultimately, it contributes to identify areas for improvement at a national level and influence the development of new initiatives and policies.

So far, this research has resulted in two publications. While the first one focused on the methodological framework and the development of the indicator system (Burgherr et al. 2021), the second one presents preliminary results based on inputs from different decision makers (Burgherr et al. 2022). An article in a peer-reviewed scientific journal with extended and final results is expected for 2023.

C.5 RECENT DEVELOPMENTS AND CONCLUDING REMARKS

This literature review has been revisited and expanded over the past months to incorporate aspects that after the Russian invasion in the Ukraine have newly emerged or received greater attention with regard to hybrid threats. Nevertheless, selected topics deserve to be mentioned explicitly in this final section.

- The dependencies on fossil fuel imports and particularly supply chain risks are a major weakness of many European countries (Axon and Darton 2021).
- The Ukraine war has also highlighted the potential collateral damage of cyberwar activities on energy infrastructure (e.g., disruption of communication services for monitoring and controlling) in the short-term (Willhuhn 2022), while its long-term and far-reaching impacts are uncontested, but associated with high uncertainties and great risks (Benton et al. 2022).
- Furthermore, disinformation as a hybrid threat has received even more attention with the war in Ukraine than before (Raemdonck, and Meyer 2022).
- Finally, articles published since the beginning of the war highlight aspects such as a common external energy security policy (Misik 2022), the choice between two contrary strategies of national energy security vs. acceleration of energy transition (Żuk and Żuk 2022), and the threat to European biodiversity due to policy responses focusing on food and energy security (Strange et al. 2022), among others.

In the following, selected conclusions and recommendations are presented as final outcome of this literature review.

The review found and confirmed that hybrid threats are a complex and complicated topical area with a broad scope, diverse and partially controversial objectives, a need for inter- and transdisciplinary assessment, potential impacts in many critical infrastructure domains that are also (partially) interdependent, and involvement of diverse stakeholders and decision makers. Therefore, it is rather clear that no "one-fits-all" approach can be applied, but that an overarching, conceptual framework – such as the one put forward by the EC's JRC and Hybrid COE – needs to be complemented by a tailored methodological approach to account for the specific objectives of case study, and that the results, conclusions and recommendations provide direct value in an operational and tactical systems environment as well as for strategy and policy development and implementation.

Therefore, the following, final statements and recommendations are rather general and are not just applicable in a hybrid threat context, but useful for any activity requiring a holistic and risk and resilience assessment and management process that is part of an overarching conceptual and political governance framework.

- Risk and resilience assessment and management is an iterative and interactive process.
- Risks and uncertainties in the decision-making process need to be addressed systematically, and potential trade-offs, conflicts and synergies identified and evaluated to find robust and broadly accepted solutions, which is not always the optimal solution in a purely operational research perspective.
- Predictions are inherently uncertain and experts tend to overconfidence! This can be nicely illustrated by the following two quotes.

  The average expert was roughly as accurate as a dart-throwing chimpanzee (Tetlock, 2005).

  A fox knows many things, but a hedgehog knows one big thing (Archilochos, 680 BC).
- Unconventional (out-of-the-box) thinking and scenario analysis are central for disruptive changes (e.g., megatrends) and extreme events (e.g., Black Swans).
- Evidence-based analysis plays a crucial role, and there is a broad toolbox, including for example:
  - Classical "Frequentist" statistical analysis that assigns probabilities to data.
  - Bayesian statistical approaches and models that assign probabilities to hypotheses, incorporate prior knowledge into the analysis, and update hypotheses probabilities as more data become available.
  - Multi-Criteria Decision Analysis (MCDA) as a sub-discipline of operations research that aims to structure and evaluate (solve) decision and planning problems involving multiple, (conflicting) criteria.
  - Machine learning algorithms are used nowadays in many fields and applications, and in the context of hybrid threats, they are, for example, considered useful for fake news detection and classification.
- Generally, a trend towards resilience-based approaches can be observed for problems involving complex, interconnected and adaptable systems.
- Ultimately, this means that organizations and other entities need to move from (defensive) risk management to forward-looking, strategic resilience, including improved foresight capabilities (scenarios and stress testing) and risk culture as well strengthen the integration of resilience in the strategy process.

C.6 BIBLIOGRAPHY

Alessa, L., Valentine, J., Moon, S. and Kiliskey, A. 2021. "Asymmetric Competition in the Arctic. Implications for North American Defense and Security." Journal of Indo-Pacific Affairs, Winter 2021: 1-28. https://par.nsf.gov/biblio/10335279

Almäng, J. 2019. "War, Vagueness and Hybrid War." Defence Studies 19(2): 189-204. DOI: 10.1080/14702436.2019.1597631.

Andrew, L. 2022. "War in Ukraine: Russia Attacks Nation Looking to Renewables and EU Grid for Energy Freedom." 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

Ang, B.W., Choong, W.L. and Ng, T.S. 2015. "Energy Security: Definitions, Dimensions and Indexes." Renewable and Sustainable Energy Reviews 42: 1077-93. DOI: 10.1016/j.rser.2014.10.064.

Ang, B.C.H. 2018. "Hybrid Warfare – A Low-Cost, High-Returns Threat to Singapore as a Maritime Nation." Pointer, Journal of the Singapore Armed Forces 44(4): 26-37. https://www.mindef.gov.sg/oms/safti/pointer/documents/pdf/V44N4_Article3.pdf

APERC. 2007. "A Quest for Energy Security in the 21st Century." www.ieej.or.jp/aperc

Aven, T. 2011a. "On Risk Governance Deficits." Safety Science 49(6): 912-19. DOI: 10.1016/j.ssci.2011.02.015.

Aven, T. 2011b. "On Some Recent Definitions and Analysis Frameworks for Risk, Vulnerability, and Resilience." Risk Analysis.

Aven, T. 2016. "Risk Assessment and Risk Management: Review of Recent Advances on Their Foundation." European Journal of Operational Research 253(1): 1-13. DOI: 10.1016/j.ejor.2015.12.023.

Aven, T., and Kristensen, V. 2019. "How the Distinction between General Knowledge and Specific Knowledge Can Improve the Foundation and Practice of Risk Assessment and Risk-Informed Decision-Making." Reliability Engineering and System Safety 191(June): 106553. DOI: 10.1016/j.ress.2019.106553.

Axon, C.J. and Darton, R.C. 2021. "Sustainability and Risk – a Review of Energy Security." Sustainable Production and Consumption 27: 1195-1204. DOI: 10.1016/j.spc.2021.01.018.

Bajarūnas, E. 2020. "Addressing Hybrid Threats: Priorities for the EU in 2020 and Beyond." European View 19(1): 62-70. DOI: 10.1177/1781685820912041.

Baker, A.B, Eagan, R.J., Falcone, P.K., Harris, J.M., Herrera, G.V., Hines, W.C., Hutchinson, R.L., et al. 2002. "A Scalable Systems Approach for Critical Infrastructure Security," no. April.

Balaban, M. and Mielniciczek, P. 2018. "Hybrid Conflict Modeling." In Proceedings of the 2018 Winter Simulation Conference, edited by M. Rabe, A.A. Juan, N. Mustafee, A. Skoogh, S. Jain, and B. Johansson, 1:3709-20. Gothenborg, Sweden: IEEE Press. DOI: 10.5555/3320516.3320960.

Barbu, V. 2020. "A Euro-Atlantic Perspective on Counteracting the Hybrid Threat." In Proceedings of the 16th International Scientific Conference "Strategis XXI". Strategic Changes in Security and International Relations, edited by Dorin Corneliu Plescan, Ion Puricel, Daniel Ghiba, Lucian Dragos Popescu, Ioana Enache, and Tudorel Lehaci, 88-100. Bucharest, Romania: Pro Quest.

BBC. 2021. “Poland Border Crisis: EU to Widen Belarus Sanctions as Row Intensifies.” 2021. https://www.bbc.co.uk/news/world-europe-59289998

Belo, D. 2020. “Conflict in the Absence of War: A Comparative Analysis of China and Russia Engagement in Gray Zone Conflicts.” Canadian Foreign Policy Journal 26(1): 73-91. DOI: 10.1080/11926422.2019.1644358.

Benton, T.G, Froggatt, A., Wellesley, L., Grafham, O., King, R., Morisetti, N., Nixey, J. and Schröder, P. 2022. “The Ukraine War and Threats to Food and Energy Security. Cascading Risks from Prices and Supply Disruptions.” London, UK. https://www.chathamhouse.org/sites/default/files/2022-04/2022-04-12-ukraine-war-threats-food-energy-security-benton-et-al_0.pdf

Beretas, C.P. 2020. “Industrial Control Systems: The Biggest Cyber Threat.” Annals of Civil and Environmental Engineering 4(1): 044-046. DOI: 10.29328/journal.acee.1001026.

Bernstein, P.L. 1996. Against the Gods – the Remarkable Story of Risk. Chichester, USA: John Wiley & Sons Inc.

Björnsdóttir, S.H., Jensson, P., de Boer, R.J. and Thorsteinsson, S.E. 2022. “The Importance of Risk Management: What Is Missing in ISO Standards?” Risk Analysis 42(4), 659-691. DOI: 10.1111/risa.13803.

Bo, T., Chen, Y., Wang, C., Zhao, Y., Lam, K.-Y., Chi, C.-H. and Tian, H. 2019. “TOM: A Threat Operating Model for Early Warning of Cyber Security Threats.” In International Conference on Advanced Data Mining and Applications (ADMA) 2019, edited by Jianxin Li, Sen Wang, Shaowen Qin, Xue Li, and Shuliang Wang, 696-711. Cham, Switzerland: Springer International Publishing. DOI: 10.1007/978-3-030-35231-8_51.

Bodeau, D.J, McCollum, C.D. and Fox, D.B. 2018. “Cyber Threat Modeling: Assessment, and Representative Framework Authors : Homeland Security Systems Engineering & Development Institute.” The Homeland Security Systems Engineering and Development Institute (HSSEDI). Washington DC (USA). https://www.mitre.org/sites/default/files/publications/pr_18-1174-ngci-cyber-threat-modeling.pdf

Boot, M. 2020. “The Changing Character of Conflict. Countering Hybrid Warfare.” In The IISS Armed Conflict Survey 2015, edited by Nigel Inkster, 11-20. London, UK: Routledge. DOI: 10.4324/9780429333620.

Bradshaw, S., and Howard, P.N. 2017. “Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation.” Oxford, UK. DOI: 10.1016/S0140-6736(59)90596-3.

Bradshaw, S., and Howard, P.N. 2019. “The Global Disinformation Order 2019 Global Inventory of Organised Social Media Manipulation.” University of Oxford. Oxford, UK. https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf

Briggs, C.M. 2020. “Climate Change and Hybrid Warfare Strategies.” Journal of Strategic Security 13(4): 45-57. DOI: 10.5038/1944-0472.13.4.1864.

Briggs, C.M., and Matejova, M. 2019. “Hybrid Disasters and Security.” In Disaster Security: Using Intelligence and Military Planning for Energy and Environmental Risks, edited by Chad M. Briggs and Miriam Matejova, 41:137-60. Cambridge, United Kingdom and New York, NY, USA: Cambridge University Press. DOI: 10.1017/9781108560023.008.

Burbridge, D.A., Col. 2013. "Employing U.S. Information Operations Against Hybrid Warfare Threats." Carlisle Barracks, PA, USA. https://apps.dtic.mil/sti/pdfs/ADA589058.pdf

Burgherr, P., Siskos, E., Spada, M., Lustenberger, P. and Dupuy, A.C. 2021. "Resilience of the European Natural Gas Network to Hybrid Threats." In Proceedings of the 31st European Safety and Reliability Conference (ESREL 2021), edited by Bruno Castanier, Marko Cepin, David Bigaud, and Christophe Berenguer, 3238-44. Singapore, SG: Research Publishing. DOI: 10.3850/978-981-18-2016-8_628-cd.

Burgherr, P., Siskos, E., Spada, M., Lustenberger, P. and Dupuy, A.C. 2022. "Energy Security in the Context of Hybrid Threats: The Case of the European Natural Gas Network." In Critical Information Infrastructures Security, edited by Bernhard Hämmerli, Udo Helmbrecht, Wolfgang Hommel, Stefan Pickl, and Leonhard Kunczik, 10. Zug, Switzerland: Springer Nature.

Butrimas, V. 2021. "Assessment Study of Cybersecurity of Smart-Grid Technologies Employed in Operational Camps." Vilnius, Lithuania. https://enseccoe.org/data/public/uploads/2021/11/vb-cyber-asses-study-v1dot2dot3-oct-1-2021-cyber-sg-for-mil-camps.pdf

Butrimas, V., Hajek, J., Sukhodolia, O., Dmytro, B. and Karasov, S. 2020. "Energy Security: Operational Highlights. Hybrid Warfare against Critical Energy Infrastructure: The Case of Ukraine." Vilnius, Lithuania. https://www.enseccoe.org/data/public/uploads/2020/11/hybrid-warfare-against-critical-energy-infrastructure-the-case-of-ukraine.pdf

Cagnin, C., Muench, S., Scapolo, F., Störmer, E. and Vesnic-Alujevic, L. 2021. "Shaping and Securing the EU's Open Strategic Autonomy by 2040 and Beyond." Luxembourg. DOI: 10.2760/414963.

Caliskan, M., and Liégeois, M. 2021. "The Concept of 'Hybrid Warfare' Undermines NATO's Strategic Thinking: Insights from Interviews with NATO Officials." Small Wars & Insurgencies 32(2): 295-319. DOI: 10.1080/09592318.2020.1860374.

Carter, R.A., Pain, D. and Enoizi, J. 2022. "Insuring Hostile Cyber Activity: In Search of Sustainable Solutions." Geneva (Switzerland). https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/cybersolutions_web.pdf

Cederberg, A. and Eronen, P. 2015. "How Can Societies Be Defended against Hybrid Threats?" Strategic Security Analysis. Geneva, Switzerland. https://css.ethz.ch/en/services/digital-library/articles/article.html/194510

Chen, D., Xu, M. and Shi, W. 2018. "Defending a Cyber System with Early Warning Mechanism." Reliability Engineering and System Safety 169: 224-34. DOI: 10.1016/j.ress.2017.08.021.

Cherp, A. and Jewell, J. 2011. "The Three Perspectives on Energy Security: Intellectual History, Disciplinary Roots and the Potential for Integration." Current Opinion in Environmental Sustainability 3(4): 202-12. DOI: 10.1016/j.cosust.2011.07.001.

CISA. 2021. "CISA Global." Washington DC, USA.

Cohen, R.S, Han, E. and Rhoades, A.L. 2020. "Geopolitical Trends and the Future of Warfare." Santa Monica, CA, USA. https://www.rand.org/content/dam/rand/pubs/research_reports/RR2800/RR2849z2/RAND_RR2849z2.pdf

Cox, L.A. 2008. "What's Wrong with Risk Matrices?" 28(2): 497-512. DOI: 10.1111/j.1539-6924.2008.01030.x.

Cox, L.A.T. 2008. “Some Limitations of ‘Risk = Threat x Vulnerability x Consequence’ for Risk Analysis of Terrorist Attacks.” Risk Analysis: An Official Publication of the Society for Risk Analysis 28(6): 1749-61. DOI: 10.1111/j.1539-6924.2008.01142.x.

Crichton, M.T., Flin, R. and Rattray, W.A.R. 2000. “Training Decision Makers – Tactical Decision Games.” Journal of Contingencies and Crisis Management 8(4): 208-17. DOI: 10.1111/1468-5973.00141.

Cullen, P., and Wegge, N. 2022. “Warning of Hybrid Threats.” In Intelligence Analysis in the Digital Age, edited by Stig Stenslie, Lars Haugom, and Brigt Harr Vaage, 85-103. London, UK: Routledge. DOI: 0.4324/9781003168157-7.

Deep, M. 2015. “Hybrid War: Old Concept, New Techniques.” Small Wars Journal, 1-4. https://smallwarsjournal.com/jrnl/art/hybrid-war-old-concept-new-techniques

Deni, J.R. 2017. “More of the Same in Response to Russia?” Carnegie Europe.” 2017. https://carnegieeurope.eu/strategiceurope/74811

DHS. 2007. “Homeland Security Exercise and Evaluation Program Volume I: HSEEP Overview and Exercise Program Management.” Washington DC, USA. https://www.hsdl.org/?view&did=470611

DOE. 2014. “Oil and Natural Gas Subsector – Cybersecurity Capability Maturity Model Version 1.1.” Washington DC (USA).

Dokos, T. 2019. “Threats and Challenges to European Security and the Need for Well-Informed Parliamentarians.” Berlin, Germany. https://www.mercatoreuropeandialogue.org/download-file/983/

Doty, P. 2015. “U.S. Homeland Security and Risk Assessment.” Government Information Quarterly 32(3): 342-52. DOI: 10.1016/j.giq.2015.04.008.

Dowse, A. and Bachmann, S.D. 2023. “Information Warfare: Methods to Counter Disinformation.” Defense and Security Analysis 38(4): 453-469. DOI: 10.1080/14751798.2022.2117285.

Dragos, V., Forrester, B. and Rein, K. 2020. “Is Hybrid AI Suited for Hybrid Threats? Insights from Social Media Analysis.” In Proceedings of 2020 23rd International Conference on Information Fusion, FUSION 2020. Virtual Conference. DOI: 10.23919/FUSION45008.2020.9190465.

Ducaru, S.D. 2016. “The Cyber Dimension of Modern Hybrid Warfare and Its Relevance for NATO.” Europolity: Continuity and Change in European Governance 10(1): 7-23. http://europolity.eu/wp-content/uploads/2016/07/Vol.-10.-No.-1.-2016-editat.7-23.pdf

Duijm, N.J. 2015. “Recommendations on the Use and Design of Risk Matrices Recommendations on the Use and Design of Risk Matrices.” Safety Science 76: 21-31. DOI: 10.1016/j.ssci.2015.02.014.

Dupuy, A.C., Iftimie, I., Nussbaum, D. and Pickl, S. 2020. “Cyber as a Hybrid Threat to NATO’s Operational Energy Security.” In 20th European Conference on Cyber Warfare and Security (ECCWS 2020), 98. Reading, UK: Academic Conferences and Publishing Limited. DOI: 10.34190/EWS.20.044.

Dupuy, A.C., Nussbaum, D., Butrimas, V. and Granitsas, A. 2021. “Energy Security in the Era of Hybrid Warfare.” NATO Review, 1-5. https://www.nato.int/docu/review/articles/2021/01/13/energy-security-in-the-era-of-hybrid-warfare/index.html

ENTSO-E, and ENTSO-G. 2022. “TYNDP 2022 Scenario Report.” Brussels, Belgium. https://2022.entsos-tyndp-scenarios.eu/wp-content/uploads/2022/04/TYNDP2022_Joint_Scenario_Full-Report-April-2022.pdf

Ertan, A, Floyd, K., Pernik, P. and Stevens, T. 2020. Cyber Threats and NATO 2030: Horizon Scanning and Analysis. Cyber Threats and NATO 2030: Horizon Scanning and Analysis. Tallinn, Estonia: NATO CCDCOE Publications. www.ccdcoe.org

European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE). n.d. "Hybrid Threats as a Concept." Accessed April 12, 2022. https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/

European Commission. 2000. "Towards a European Strategy for the Security of Energy Supply." Brussels, Belgium. https://op.europa.eu/en/publication-detail/-/publication/0ef8d03f-7c54-41b6-ab89-6b93e61fd37c/language-en.

European Commission. 2016. "Fact Sheet FAQ: Joint Framework on Countering Hybrid Threats." Brussels, Belgium. https://ec.europa.eu/commission/presscorner/detail/en/MEMO_16_1250

European Commission. 2022. "Standard Eurobarometer 96 Winter 2021-2022. Public Opinion in the European Union." Brussels, Belgium. https://europa.eu/eurobarometer/api/deliverable/download/file?deliverableId=81214

European Cyber Security Organisation. 2018. "Energy Networks and Smart Grids. Cyber Security for the Energy Sector. WG3 Sectoral Demand." Brussels, Belgium.

European Political Strategy Centre. 2019. "10 Trends Shaping Democracy in a Volatile World." Brussels, Belgium. https://op.europa.eu/en/publication-detail/-/publication/c2a3e6d5-10ce-11ea-8c1f-01aa75ed71a1/language-en

Evans, C.V. 2020. "Future Warfare: Weaponizing Critical Infrastructure." Parameters 50(2): 35-42. https://press.armywarcollege.edu/parameters/vol50/iss2/6%0AThis

Fiksel, J. 2006. "Sustainability and Resilience: Toward a Systems Approach." Sustainability: Science, Practice and Policy 2(2): 14-21. DOI: 10.1080/15487733.2006.11907980.

Flanagan, S.J, Binnendijk, A., Chindea, I.A., Costello, K., Kirkwood, G., Massicot, D. and Reach, C. 2020. "Russia, NATO, and Black Sea Security." Santa Monica, CA, USA. https://www.rand.org/pubs/research_reports/RRA357-1.html

Franke, U. and Draeger, J. 2019. "Two Simple Models of Business Interruption Accumulation Risk in Cyber Insurance." In 2019 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, Cyber SA 2019, 1-7. Oxford, UK: IEEE. DOI: 10.1109/CyberSA.2019.8899678.

Galaitsi, S.E., Keisler, J.M., Trump, B.D. and Linkov, I. 2021. "The Need to Reconcile Concepts that Characterize Systems Facing Threats." Risk Analysis 41(1): 3-15. DOI: 10.1111/risa.13577.

Galaitsi, S.E., Kurth, M. and Linkov, I. 2021. "Resilience: Directions for an Uncertain Future Following the COVID-19 Pandemic." GeoHealth. DOI: 10.1029/2021gh000447.

Gasser, P., Lustenberger, P., Cinelli, M., Kim, W., Spada, M., Burgherr, P., Hirschberg, S., Stojadinovic, B. and Sun, T.Y. 2021. "A Review on Resilience Assessment of Energy Systems." Sustainable and Resilient Infrastructure 6(5): 273-299. DOI: 10.1080/23789689.2019.1610600.

Giannopoulos, G., Smith, H. and Theocharidou, M. 2020. "The Landscape of Hybrid Threats: A Conceptual Model (Public Version)." Ispra, Italy: European Commission (EC), Joint Research Centre (JRC). https://euhybnet.eu/wp-content/uploads/2021/01/Conceptual-Framework-Hybrid-Threats-HCoE-JRC.pdf

Giles, K. 2019. "'Hybrid Threats': What Can We Learn From Russia?" Federal Academy for Security Policy Security Policy Working Paper. Berlin, Germany.

Giudici, P. and Raffinetti, E. 2021. "Cyber Risk Ordering with Rank-Based Statistical Models." AStA Advances in Statistical Analysis 105(3): 469-84. DOI: 10.1007/s10182-020-00387-0.

Glenn, R.W. 2009. "Thoughts on 'Hybrid' Conflict." Small Wars Journal, 1-8. https://smallwarsjournal.com/blog/journal/docs-temp/188-glenn.pdf

Golan, M.S., Jernegan, L.H. and Linkov, I. 2020. "Trends and Applications of Resilience Analytics in Supply Chain Modeling: Systematic Literature Review in the Context of the COVID-19 Pandemic." Environment Systems and Decisions 40(2): 222-43. DOI:10.1007/s10669-020-09777-w.

Grätz, J. 2012. "The Arctic: Thaw with Conflict Potential." Zurich (Switzerland).

Guikema, S.D. and Aven, T. 2010. "Assessing Risk from Intelligent Attacks: A Perspective on Approaches." Reliability Engineering and System Safety 95(5): 478-83. DOI: 10.1016/j.ress.2009.12.001.

Hafner, M. and Tagliapietra, S. 2020. The Geopolitics of the Global Energy Transition. Lecture Notes in Energy. Vol. 73. Cham, Switzerland: Springer. DOI:10.1007/978-3-030-39066-2.

Haimes, Y.Y. 2009. "On the Complex Definition of Risk: A Systems-Based Approach." Risk Analysis.

Hanisch, M. 2016. "What Is Resilience? Ambiguities of a Key Term." Federal Academy for Security Policy, no. 19: 1-4. http://www.jstor.com/stable/resrep22143%0AJSTOR

Harris, K. 2020. "A Hybrid Threat: The Night Wolves Motorcycle Club." Studies in Conflict and Terrorism, 1-29. DOI: 10.1080/1057610X.2020.1862752.

Hartmann, U. 2017. "The Evolution of the Hybrid Threat, and Resilience as a Countermeasure." NATO Research Paper 19(139): 1-8. https://www.ndc.nato.int/download/downloads. php?icode=527

Hausken, K. 2020. "Cyber Resilience in Firms, Organizations and Societies." Internet of Things 11: 100204. DOI: 10.1016/j.iot.2020.100204.

Hirsch, D.D. 2014. "The Glass House Effect: Big Data, the New Oil and the Power of Analogy." Maine Law Review. https://ssrn.com/abstract=2393792

Ho, P. 2018. The Challenges of Governance in a Complex World. The Challenges of Governance in a Complex World. Singapore, SG: World Scientific Publishing Co. Pte. Ltd. DOI: 10.1142/9789813231832.

Hoffman, F.G. 2007. "Conflict in the 21st Century: The Rise of Hybrid Wars." Arlington, Virginia, USA. DOI: 10.20542/0131-2227-2019-63-12-56-66.

Hoffman, F.G. 2009. "Hybrid Warfare and Challenges." Joint Force Quarterly 52(1): 34-39. https://ndupress.ndu.edu/portals/68/Documents/jfq/jfq-52.pdf

Hoffman, F.G. 2010. "'Hybrid Threats': Neither Omnipotent nor Unbeatable." Orbis 54(3): 441-55. DOI: 10.1016/j.orbis.2010.04.009.

International Energy Agency. 2007. "Energy Supply Security: Emergency Response of IEA Countries 2014." Oil Supply Security: Emergency Response of IEA Countries 2007. Paris (France). DOI: 10.1787/9789264040045-en.

Jacobs, J.G.L.J., and Kitzen, M.W.M. 2021. “Hybrid Warfare.” In Oxford Bibliographies. Oxford University Press. DOI: 10.1093/OBO/9780199743292-0260.

Jones, S. 2014. “Ukraine: Russia’s New Art of War.” Financial Times, August 27, 2014. http://www.ft.com/intl/cms/s/2/ea5e82fa-2e0c-11e4-b760-00144feabdc0.html

Juntunen, T. and Hyvönen, A.-E. 2014. “Resilience, Security and the Politics of Processes.” Resilience 2(3): 195-209. DOI: 10.1080/21693293.2014.948323.

Kaplan, S. 1997. “The Words of Risk Analysis.” Risk Analysis 17(4): 407-17. DOI: 10.1111/j.1539-6924.1997.tb00881.x.

Kaplan, S. and Garrick, B.J. 1981. “On The Quantitative Definition of Risk.” Risk Analysis 1(1): 11-27. DOI: 10.1111/j.1539-6924.1981.tb01350.x.

Kerber, S.W., Gilbert, A.Q., Deinert, M.R. and Bazilian, M.D. 2021. “Understanding the Nexus of Energy, Environment and Conflict: An Overview.” Renewable and Sustainable Energy Reviews 151(July): 111473. DOI: 10.1016/j.rser.2021.111473.

Keskinen, M., Sojamo, S. and Varis, O. 2019. “Enhancing Security, Sustainability and Resilience in Energy, Food and Water.” Sustainability 11(24): 7244. DOI: 10.3390/SU11247244.

Kim, Wansub, Peter Burgherr, Matteo Spada, Peter Lustenberger, Anna Kalinina, and Stefan Hirschberg. 2018. “Energy-Related Severe Accident Database (ENSAD): Cloud-Based Geospatial Platform.” Big Earth Data 2(4): 368-94. https://doi.org/10.1080/20964471.2019.1586276.

Kuczynski, G. 2019. “Russia’s Hybrid Warfare in the Western Balkans.” Warsaw, Poland. https://warsawinstitute.org/russias-hybrid-warfare-western-balkans/

Kyriakidis, M., Lustenberger, P., Burgherr, P. and Dang, V.N. 2018. “Quantifying Energy Systems Resilience – A Simulation Approach to Assess Recovery.” Energy Technology 6(9): 1700-1706. DOI: 10.1002/ente.201700841.

Li, I. 2020. “Sound the Clarion! Hybrid Warfare Has Arrived in the Asia-Pacific.” Small Wars & Insurgencies, 1-3.

Linkov, I., Trump, B.D., Trump, J. and Pescaroli, G. 2022. “Resilience Stress Testing for Critical Infrastructure.” International Journal of Disaster Risk Reduction 82(May): 103323. DOI: 10.1016/j.ijdrr.2022.103323.

Liu, J., Hull, V., Godfray, H.C.J., Tilman, D., Gleick, P., Hoff, H., Pahl-Wostl, C., et al. 2018. “Nexus Approaches to Global Sustainable Development.” Nature Sustainability 1(9): 466-76. DOI: 10.1038/s41893-018-0135-8.

Lustenberger, P., Schumacher, F., Spada, M., Burgherr, P., and Stojadinovic, B. 2019. “Assessing the Performance of the European Natural Gas Network for Selected Supply Disruption Scenarios Using Open-Source Information.” Energies 12(24): 1-30. DOI: 10.3390/en12244685.

Mälksoo, M. 2018. “Countering Hybrid Warfare as Ontological Security Management: The Emerging Practices of the EU and NATO.” European Security 27(3): 374-92. DOI: 10.1080/09662839.2018.1497984.

Mattis, J.N., and Hoffman, F. 2005. “Future Warfare: The Rise of Hybrid Wars.” U.S. Naval Institute Proceedings 131(11): 18-19. http://www.dtic.mil/dtic/aulimp/citations/gsa/2005_118877/123268.html

Mazeikis, E., Jaeski, A., Meyer, H., Paillard, C.-A., Bartuska, V., Gonchar, M., Chubyk, A., Sukhodolia, O., and Vizbaras, K. 2017. "Hybrid Threats : Overcoming Ambiguity , Building Resilience." Vilnius, Lithuania. https://enseccoe.org/data/public/uploads/2017/03/zurnalas_no11_sp_176x250mm_3mm_2.pdf

McCuen, J.J. 2008. "Merging Three Battlegrounds and Two Wars." Military Review, no. March-April: 107-13. https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20080430_art017.pdf

McCulloh, T.B. 2012. "The Inadequacy of Definition and the Utility of a Theory of Hybrid Conflict: Is the 'Hybrid Threat' New?" Fort Leavenworth, Kansas, USA. https://www.hsdl.org/?view&did=758318

Misik, M. 2022. "The EU Needs to Improve Its External Energy Security." Energy Policy 165(March): 112930. DOI: 10.1016/j.enpol.2022.112930.

Mockaitis, T.R. 1995. British Counterinsurgency in the Post-Imperial Era Manchester: Manchester University Press; Distributed by St. Martin's Press, New York, N.Y. xvi, 165. ISBN 0-7190-3919-3. Manchester, UK: Manchester University Press.

Moteff, J., and Parfomak, P. 2004. "CRS Report for Congress Received through the CRS Web Critical Infrastructure and Key Assets."

Mumford, A. 2020. "Ambiguity in Hybrid Warfare. Hybrid CoE Strategic Analysis / 24." Helsinki, Finland. https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-24-ambiguity-in-hybrid-warfare/

Murray, W., and Mansoor, P.R. 2012. Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present. New York, USA: Cambridge University Press.

Nadolski, M., and Fairbanks, J. 2019. "Complex Systems Analysis of Hybrid Warfare." Procedia Computer Science 153: 210-17. DOI: 10.1016/j.procs.2019.05.072.

Natale, A., Poppensieker, T. and Thun, M. 2022. "From Risk Management to Resilience Management." McKinsey & Co. Insights & Publications, March. https://www.e-elgar.com/shop/handbook-on-resilience-of-socio-technical-systems

NATO. 2010. "AJP-01(D) Allied Joint Doctrine, December 2010." Brussels, Belgium. https://www.cmdrcoe.org/download.cgf.php?id=13

NATO. 2014. "Wales Summit Declaration." Press Release (2014) 120. 2014. https://www.nato.int/cps/ic/natohq/official_texts_112964.htm

NATO. 2017. "AJP-01 Allied Joint Doctrine Edition E, Version 1, February 2017." Brussels, Belgium.

NATO. 2021. "NATO's Response to Hybrid Threats." 2021. https://www.nato.int/cps/en/natohq/topics_156338.htm

NATO Stratcom COE. 2020. "Hybrid Threats. A Strategic Communications Perspective." DOI: 10.1007/978-3-319-15347-6_300702.

Neto, N.N., Madnick, S. Anchises Moraes, P. and Malara Borges, N. 2021. "Developing a Global Data Breach Database and the Challenges Encountered." Journal of Data and Information Quality 13(1): 1-33. DOI: 10.1145/3439873.

Østhagen, A. 2019. “The New Geopolitics of the Arctic : Russia , China and the EU.” Brussels, Belgium. https://euagenda.eu/upload/publications/untitled-212267-ea.pdf

Palmer, M. 2006. “Data Is the New Oil (Blog Post).” 2006.

Plucinska, J. 2022. “Nord Stream Gas ‘Sabotage’: Who’s Being Blamed and Why?” Reuters, 2022. https://www.reuters.com/world/europe/qa-nord-stream-gas-sabotage-whos-being-blamed-why-2022-09-30/

Pollack, J., and Ranganathan, P. n.d. “Social Engineering and Its Impacts on Critical Infrastructure: A Comprehensive Survey.” In International Conference on Security and Management SAM’18, 122-28. Las Vegas, USA.

Qureshi, W.A. 2020. “The Rise of Hybrid Warfare.” Notre Dame Journal of International & Comparative Law 10(2): 173.

Van Raemdonck, N. and Meyer, T. 2022. “Why Disinformation Is Here to Stay. A Socio-Technical Analysis of Disinformation as a Hybrid Threat.” In Addressing Hybrid Threats: European Law and Policies Publication, edited by Luigi Lonardo, 18. Cheltenham Glos, UK: Edward Elgar.

Renn, O. 2021. “Transdisciplinarity : Synthesis Towards a Modular Approach.” Futures 130(March): 102744. DOI: 10.1016/j.futures.2021.102744.

Renn, O., Laubichler, M., Lucas, K., Kröger, W., Schanze, J., Scholz, R.W. and Schweizer, P.J. 2020. “Systemic Risks from Different Perspectives.” Risk Analysis, 1-19. DOI: 10.1111/risa.13657.

Romanosky, S. 2016. “Examining the Costs and Causes of Cyber Incidents.” Journal of Cybersecurity 2(2): 121-35. DOI: 10.1093/cybsec/tyw001.

Rühle, M., and Grubliauskas, J. 2015. “Energy as a Tool of Hybrid Warfare.” NATO Research Paper, no. 113: 8. https://www.ndc.nato.int/download/downloads.php?icode=451

Samaras, C., Nuttall, W.J. and Bazilian, M. 2019. “Energy and the Military: Convergence of Security, Economic, and Environmental Decision-Making.” Energy Strategy Reviews 26(January): 100409. DOI: 10.1016/j.esr.2019.100409.

Seebeck, L., Williams, E. and Wallis, J. 2022. “Countering the Hydra. A Proposal for an Indo-Pacific Hybrid Threat Centre. Policy Brief Report No. 60/2022.” Barton, Australia. https://www.aspi.org.au/report/countering-hydra

Shedd, D.R., and Stradner, I. 2020. “Putin Is Winning Russia’s Hybrid War against America.” National Review, 2020. https://www.nationalreview.com/2020/12/putin-is-winning-russias-hybrid-war-against-america/

Siddi, M. 2020. “Theorising Conflict and Cooperation in EU-Russia Energy Relations : Ideas , Identities and Material Factors in the Nord Stream 2 Debate.” East European Politics 36(4): 544-63. DOI: 10.1080/21599165.2019.1700955.

Sidortsov, R., Ivanova, A. and Stammler, F. 2016. “Localizing Governance of Systemic Risks: A Case Study of the Power of Siberia Pipeline in Russia.” Chemical Physics Letters. DOI: 10.1016/j.erss.2016.03.021.

Simola, J. 2021. Comparing Cybersecurity Information Exchange Models and Standards for the Common Secure Information Management Framework. Studies in Big Data. Vol. 84. Springer International Publishing. DOI: 10.1007/978-3-030-65722-2_9.

Siskos, E., and Burgherr, P. 2021. "Multicriteria Decision Support for the Evaluation of Electricity Supply Resilience: Exploration of Interacting Criteria." European Journal of Operational Research 298(2): 611-26. DOI: 10.1016/j.ejor.2021.07.026.

Siskos, E., and Tsotsolas, N. 2015. "Elicitation of Criteria Importance Weights through the Simos Method: A Robustness Concern." European Journal of Operational Research 246(2): 543-53. DOI: 10.1016/j.ejor.2015.04.037.

Solmaz, T. 2022. "Hybrid Warfare: One Term, Many Meanings." Small Wars Journal, 1-12. https://smallwarsjournal.com/jrnl/art/hybrid-warfare-one-term-many-meanings

Speranza, L. 2020. "A Strategic Concept for Countering Russian and Chinese Hybrid Threats." Washington DC, USA. https://www.atlanticcouncil.org/wp-content/uploads/2020/07/Strategic-Concept-for-Countering-Russian-and-Chinese-Hybrid-Threats-Web.pdf

Steingartner, W., Galinec, D., and Kozina, A. 2021. "Threat Defense: Cyber Deception Approach and Education for Resilience in Hybrid Threats Model." Symmetry 13(4): 1-25. DOI: 10.3390/sym13040597.

Stern, E. and Nussbaum, B. 2022. Critical Infrastructure Disruption and Crisis Management. Oxford Research Encyclopedia of Politics. https://doi.org/10.1093/acrefore/9780190228637.013.1603.

Strange, N., Geldmann, J., Burgess, N.D. and Bull, J.W. 2022. "Policy Responses to the Ukraine Crisis Threaten European Biodiversity." Nature Ecology and Evolution. DOI: 10.1038/s41559-022-01786-z.

Strobl, J. and Borchert, H. 2022. "Storms Ahead: The Future Geoeconomic World Order." Vienna, Austria. https://www.researchgate.net/publication/358347091_Storms_Ahead_The_Future_Geoeconomic_World_Order

Štrucl, D. 2021. "Comparative Study on the Cyber Defence of NATO Member States." Tallinn, Estonia.

Thiele, R.D. 2016. "Hybrid Threats and How to Counter Them." ISPSW Strategy Series: Focus on Defense and International Security, no. 448: 1-12. http://www.ispsw.com/wp-content/uploads/2016/09/448_Thiele_Oslo.pdf%0Ahttp://www.ispsw.de

Thiele, R.D. 2020. "Over Five Years of Russian Hybrid Warfare against Ukraine Provide Lessons How to Make Ukraine Stronger." ISPSW Strategy Series: Focus on Defense and International Security, no. 662: 1-5. https://ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/ISPSW_662_Thiele.pdf

Tierney, K. 2014. The Social Roots of Risk Producing Disasters, Promoting Resilience. Redwood City, CA, USA: Stanford University Press.

TRADOC G-2. 2015. "Threat Tactics Report Compendium: ISIL, North Korea, Russia, and China." Vol. 1. Fort Leavenworth, Kansas, USA. https://community.apan.org/cfs-file/__key/docpreview-s/00-00-01-79-53/TTR-Comp-Vol-1-Sept-2015.pdf

US Department of Homeland Security (DHS). 2013. "NIPP 2013: Partnering for Critical Infrastructure Security and Resilience." Washington DC, USA. https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf

US GAO. 2010. "GAO-10-1036R Hybrid Warfare." Washington DC (USA). https://www.gao.gov/assets/gao-10-1036r.pdf

WEC. 2019. "Cyber Challenges to the Energy Transition." London, UK.

WEC. 2019. 2020. "World Energy Trilemma Index." London, UK. https://www.worldenergy.org/assets/downloads/World_Energy_Trilemma_Index_2020_-_REPORT.pdf? v=1602261628

Wells, E.M., Boden, M., Tseytlin, I. and Linkov, I. 2022. "Modeling Critical Infrastructure Resilience under Compounding Threats: A Systematic Literature Review." Progress in Disaster Science 15(July): 100244. DOI: 10.1016/j.pdisas.2022.100244.

Wigell, M., Mikkola, H. and Juntunen, T. 2021. "Best Practices in the Whole-of-Society Approach in Countering Hybrid Threats." Brussels, Belgium. https://www.europarl.europa.eu/thinktank/en/document/EXPO_STU(2021)653632

Willhuhn, M. 2022. "Satellite Cyber Attack Paralyzes 11 GW of German Wind Turbines." Pv Magazine International, May: 7. https://www.pv-magazine.com/2022/03/01/satellite-cyber-attack-paralyzes-11gw-of-german-wind-turbines/

World Economic Forum. 2021. The Global Risks Report 2021, 16th Edition. Cologny/Geneva, Switzerland: World Economic Forum (WEF). https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf

Żuk, P. and Żuk, P. 2022. "National Energy Security or Acceleration of Transition? Energy Policy after the War in Ukraine." Joule 6(4): 709-12. DOI: 10.1016/j.joule.2022.03.009.

Annex D – GERMAN CASE STUDY

John R. Deni, David Dorondo, and Elvira Loredo

Additional contributions from
Afra Herr and John Tabler

D.1 INTRODUCTION

Germany is a pivotal country in terms of European energy security. Whether viewed as a transit country, as a consumer, or in terms of the shift to renewables, Germany's role in Europe is vital. That role has become increasingly a balancing act, which manifests along several axes – between the fuels of yesterday and the clean energy of tomorrow, between the commitment to allies in Eastern Europe and the desire for partnership with Russia, and between national and private interests on the one hand and collective EU interests on the other.

This annex provides an overview of Germany's efforts to achieve equilibrium across all these competing priorities as the leading economy of Europe and as a lynchpin of transatlantic security and stability. It will begin by providing a historically grounded overview of Germany's approach to energy security, including its efforts to achieve something of a special relationship with Russia. This will lead into a discussion of Germany's efforts to transition from fossil fuels to renewables, including the fateful decision to close all nuclear and coal-fired power plants. Next, the annex briefly highlights some issues regarding national versus regional and public versus private imperatives in Germany's energy sector.

The annex then turns to address the importance of Germany as an energy transit country, including the strategically and operationally important energy infrastructure on German territory. This includes some key data on Germany's resilience against energy supply disruption and how discussion of Germany's energy position affects the fuel requirements of military forces. The annex ends with a brief conclusion, which identifies some of the risks Berlin is likely to face in the coming years as it balances international, national, regional, public, and private interests at the intersection of energy security and hybrid conflict.

D.2 GERMAN PERSPECTIVE ON ENERGY SECURITY

As in most countries, energy security constitutes a critical concern of any German government, regardless of party[1]. Nonetheless, Germany's perspective on energy security is a product of the country's unique characteristics, its history, and its contemporary politics. At 83.1 million, Germany's population makes it the largest of any country in Europe after Russia and Turkey, respectively [1]. Germany has the largest economy in Europe [2] and the fourth largest in the world [3], one that commands a leading role in cutting-edge technologies, research-and-development, automated manufacturing, and highly intensive agriculture. Inexpensive and reliable energy supplies are essential to maintaining Germany's economic prominence.

At one time or another since the 1860s, Germany fought against most of the countries of Europe, from the United Kingdom to Russia and from Norway to Italy, to include the former East German government's logistical support for the Warsaw Pact's invasion of Czechoslovakia in 1968. These antecedents affect the German government's pursuit of any significant foreign policy initiative in Europe today, and energy security is no exception. Even though Germany's approach to energy security is usually perceived to be based on market dynamics, geopolitical and historical factors play critical roles [4].

[1] The Alternative for Germany, or AfD, party does not support Germany's energy transition and it denies climate change. However, it does not govern at the federal level.

In the post-World War II era, Germany has harbored pronounced environmentalism and anti-nuclear sentiment. Germany's investments in renewable energy have slowly shifted the mix of fuels used to produce electricity, but coal (28.1%) and nuclear (11.9%) together still account for a not insignificant amount, nearly as much as renewables (40.9%) [5]. The embrace of more environmentally friendly policies and an increasingly de-carbonized approach to energy and the economy – including by the mainstream parties – has enabled Germany to pursue a full-scale 'energy transition', or *Energiewende*[2]. The *Energiewende* is a multi-year strategy to achieve a transformation of energy supply in Germany. This transition and its attendant shift to a no-carbon energy footprint by 2050 will have profound societal and economic implications.

D.3 THE GERMAN ENERGY TRANSITION

Although the Germany Energy Transition, or *Energiewende*, has its roots in the anti-nuclear movement of the Cold War era, there are important economic reasons for Germany to transition to a no-carbon energy economy [6]. Germany remains very much a resource-poor country as regards petroleum-based energy. Historically, Germany has therefore relied upon imports. The energy *in*security generated by this reliance was dramatically demonstrated by the Nazi regime's attempts between 1933 and 1945 to both produce synthetic fuel and to control or conquer European oil fields at Lake Balaton in Hungary, around Ploeşti in Romania, and between the Black and Caspian Seas in the Soviet Union.

Since December 2021, the responsibility for continued implementation of the *Energiewende* has fallen to Germany's first-ever national tripartite coalition comprised of Social Democrats, Bündnis 90/Greens, and Free Democrats, led by Chancellor Olaf Scholz. As it was for Scholz's predecessor, Angela Merkel, continued implementation of the *Energiewende* promises to be neither smooth nor necessarily steady [7]. Central to this transition are long-standing policies adopted by the previous government to shut down all of Germany's remaining nuclear power plants as well as all remaining coal mines. It also includes incentives to increase renewable energy sources, such as wind, solar power, and biofuels.

As of this writing, the process of shutting down nuclear power plants continues. In late December 2021, Germany closed nuclear power plants in Brokdorf (Schleswig-Holstein), Grohnde (Lower Saxony), and Unit C at Gundremmingen (Bavaria) [8].[3] This leaves Germany with just three remaining nuclear plants – at Emsland (Lower Saxony), Isar (Bavaria), and Neckarwestheim (Baden-Württemberg) – which are all slated to close by the end of 2022. The ending of coal production is officially slated to be completed no later than 2038, a goal supposedly made more palatable by huge federal subsidies to coal-mining states such as North-Rhine Westphalia, Saxony, and Saxony-Anhalt [9].[4]

While Germany and the European Union have set ambitious goals to reduce the emissions of greenhouse gasses [8][5], they recognize that for the foreseeable future natural gas and oil will continue to provide a significant amount of the energy required by Europe and Germany [10]. At present in Germany, natural gas is more heavily used for heating and power generation, while liquid petroleum is more heavily used for transportation. Both are critically important to the economic stability of Germany and the quality of life of its people.

In 2018, the production of hard coal in Germany was terminated and the domestic production of natural gas, already quite low, continues to sink due to depletion of gas fields. The Ministry of the Environment projects

[2] Energiewende involves a series of policies, laws, and regulations by the German government to achieve a green energy transformation across multiple energy sectors, including power generation, transportation, agriculture, and industry.

[3] Three further nuclear plants remain as of this writing.

[4] The federal structure of Germany adds a further complicating element for any government in Berlin as the sixteen states (*Länder*) can sometimes play an outsized role in national decision-making.

[5] Climate Action Plan 2050 calls for a 62% reduction in CO2 emissions compared to 1990, by 2030.

a 100 percent dependency on primary energy imports for liquid petroleum products, uranium, hard coal, and natural gas [11]. In terms of countries that supply Germany's energy, the main suppliers of natural gas are (in descending order) Russia, Norway, and the Netherlands while the main suppliers of petroleum products are (in descending order) Russia, Norway, the United Kingdom, Kazakhstan, Libya, Nigeria, Iraq, and the United States. Hard coal is imported from the United States, Australia, and Columbia among others [12]. Since at least 2000, Germany has steadily increased its imports of natural gas from its leading supplier, the Russian Federation [13].[6]

D.4 THE GERMAN-RUSSIA ENERGY RELATIONSHIP

Germany's complex historical relationship with Russia has contributed in no small part to the pursuit of an interdependent energy relationship between the two by generations of German politicians [14]. The prospect of rapprochement with Russia has been an important rhetorical and policy element of Germany's efforts to build stability and security across the European landmass [15]. The goal of (West) Germany's '*wandel durch handel*' policy, or change through trade, was to create a high degree of interdependence that would make military confrontation with the West unthinkable in Moscow.

A secondary goal of *wandel durch handel* and the broader *Ostpolitik* of which it was part was to expose those isolated behind the Iron Curtain to Western idea, norms, and standards[7]. At the end of the Cold War, interdependence through trade and its associated dampening of security competition was viewed by many in Germany as a key element in explaining how and why the era of bipolar competition ended peacefully [17]. This guiding principle remained central to German strategy toward Russia through the post-Cold War period as well [18]. It was made manifest through a variety of practical approaches and projects, including and especially in the energy sector. For instance, Germany's major gas and oil refineries and distributors have worked closely with Russian oil and gas producers, sharing technology and receiving favorable pricing and assured supply. In 2011, the Nord Stream 1 gas pipeline connected Russia directly with Germany through the Baltic Sea. In 2015, agreement was reached on construction of another, parallel pipeline – Nord Stream 2 – which would allow Russia to provide even more gas directly to Germany, bypassing other pipelines across Central and Eastern Europe. With the German government's support of the Nord Stream 2 project, and the importance of natural gas as a so-called 'bridging fuel' to more renewable resources, Germany's demand for and reliance on Russian gas looked likely to continue into the foreseeable future.

All of this changed in February 2022 because of Russia's actions in and around Ukraine. Following an announcement by Moscow to recognize two Russian-backed separatist regions of Ukraine as independent, Germany announced the suspension of the process to approve operation of the Nord Stream 2 pipeline. Just days later, following Russia's brutal re-invasion of Ukraine, Berlin went further in the energy sector by announcing the planned construction of two Liquefied Natural Gas (LNG) terminals, one in Brunsbuettel and one in Wilhelmshaven, both along Germany's North Sea coastline, to facilitate the delivery of non-Russian natural gas [19]. The German government also announced it would increase the amount of natural gas held in its storage facilities by 2 billion cubic meters via long-term options and by purchasing additional natural gas on world markets in coordination with the European Union. Finally, the government announced it was weighing whether to extend the lifespan of its three remaining nuclear power plants and to permit coal-fired plants to operate beyond 2030.

Taken together with the dramatic increase in military spending also announced by Scholz in the wake of Russia's attack against Ukraine, these energy security policy changes appeared among the first steps in a complete reversal of Germany's consensus-based, decades-old approach to both Russia and energy [20],

[6] Russian gas imports in 2018 were estimated at 70 bcm, while total imports were 120 bcm.

[7] Ostpolitik – a policy of reconciliation with Germany's eastern neighbors – began in the late 1960s and was driven initially by the SPD while it governed West Germany from 1969 until 1982. Later, it was adopted by the center right parties as well as a core element of West German – and later, German – foreign policy [16].

[21]. With regard to the former, Germany appears to have reached a point of no return regarding *Ostpolitik* and the end of a process of reconsideration that actually began in 2014, when Russia first invaded Ukraine [22]. And on energy security specifically, the invasion has raised questions over whether and how the German energy transition can continue amidst the hostilities and Russia's broader upending of security across the continent [23].

D.5 BALANCING INTERGOVERNMENTAL, NATIONAL, REGIONAL, AND PRIVATE IMPERATIVES

The invasion of Ukraine has also sent shock waves through EU institutions tasked with energy security matters, exposing the risks of relying – as Germany does – on Russia as an energy supplier [24]. This prompted EU officials to fast-track the development of alternative strategies and approaches to energy security across the continent, including by diversifying natural gas supplies and transitioning more quickly to renewables [25]. Nonetheless, even as it tries to reduce reliance on Russian energy sources, the EU has made clear that natural gas in particular remains essential in the short run and most likely even longer. Just two months before the Russian invasion, the EU announced that natural gas would be part of its taxonomy of sustainable energy sources, in part thanks to the firm stance taken by the new German government [26], [27]. While the EU's decision may result in some criticism from those who point out that methane emissions from natural gas are as bad as any other greenhouse gas emission, it is unlikely that the decision will be reversed, and it further bolsters the continued reliance on natural gas as an essential source of fuel for the time being, especially by the EU's leading economy.

Domestically, Germany has a liberalized energy market. Together with the relative strength of German states (or *Länder*) vis-à-vis the federal government, there are a large array of private, public, and mixed businesses active in the energy sector, as city-wide or regional suppliers of electricity, as refineries, or as grid operators [28]. In some cases, German authorities have partially privatized the operation of the energy grid or supplier, which has notably included related information technology infrastructure [29]. The high-voltage network, for example, is divided into four regions, administrated by four individual, nongovernmental providers with ties to other European countries.

Privatization has created some risks in terms of Germany's cyber security in the energy sector. To address perceived problems in the German cyber security realm, in 2015 a law was passed to assure adequate cyber security measures with state-of-the-art information technology introduced by operators of critical infrastructure as well as a mandated linkage between operators and the federal level. Following this, annual information technology security reports by the Ministry of the Interior identified between 20 and 30 individual cyber incidents in the energy sector [30], [31].[8]

D.6 GERMANY'S ENERGY INFRASTRUCTURE

Two main pipelines bring Russian natural gas to Germany – the Yamal, which flows through Belarus and Poland, and the Nord Stream pipelines, which flow directly from Russia under the Baltic Sea and into Germany. Russian gas from these pipelines serves the needs of both Germany and many other countries across Europe, including Belgium, the Netherlands, France, Austria, Italy, and the Czech Republic [32].

Germany therefore plays a critical role as a transit country. Figure D-1 shows the dollar value of exports of natural gas from Germany to other European countries in 2019. This figure demonstrates Germany's central role, not only as a major importer of Russian fuel but as a gas distribution hub for the rest of Europe. Perhaps somewhat intuitively, Germany and its European neighbors have widely divergent susceptibilities to a disruption in gas flow from Russia or to an unexpected demand increase [33]. This is generally though not

[8] This year's report splits the nuclear sector off from the energy sector. In previous years, nuclear did not have a separate section.

entirely based on whether and how a country adheres to its emergency fuel storage plan. In the case of Germany, it is only at risk if its fuel reserves are depleted, which is highly unlikely under most circumstances.

In terms of petroleum products, crude oil can enter Germany through a variety of pipelines. Crude oil imported into Germany is refined into fuel at one of 13 national refineries [34].[9] Germany has 2.1 million barrels a day (b/d) of refining capacity, the largest capacity in Europe [35]. Table D-1 lists the refineries associated with each pipeline and the refining capacity supported by each pipeline. A list of the major refineries in Germany along with their location and refining capacity is shown in Figure D-1. Of note, the refineries in the former West Germany account for approximately 84 percent of the refining capacity in Germany.

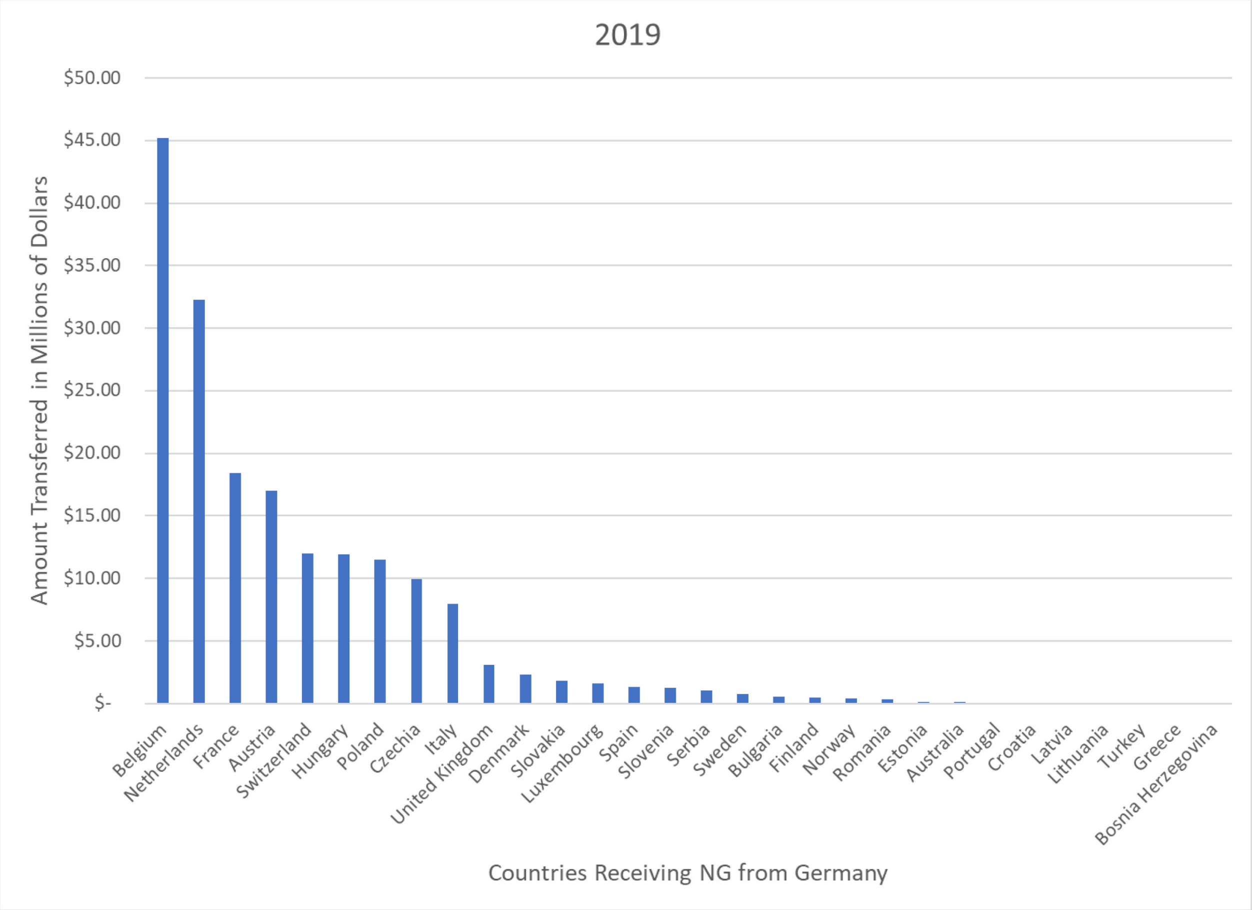


Figure D-1: Natural Gas Transfers from Germany to Other Countries. Source: comtrade.un.org.

In late 2021, the Russian state-owned Rosneft acquired Shell’s minority stake of 230,000 b/d in the PCK Schwedt refinery, increasing its controlling share of that refinery from 54 percent to 92 percent. Overall, Rosneft is now Germany’s second largest refiner, behind Shell. Rosneft controls 344 kbd or 16 percent of Germany’s refining capacity. Rosneft also owns a 24 percent stake in the 310 kbd Miro refinery and a 28.57 percent interest in the 220 kbd Bayernoil plants at Neustadt and Vohburg, both of which are located along the Danube River in Bavaria in southern Germany [36].

[9] Of the 13 refineries, 2 refine crude primarily for chemical production. Fuel is effectively produced by 11 of the 13 refineries listed in the table.

Pipelines and refineries have a direct impact not merely on domestic energy security broadly speaking but also on military operational energy security. Figure D-2 shows the country-level jet fuel domestic production and consumption as well as imports of jet fuel for Europe. The data indicates that some of the biggest producers of jet fuel (red bars) are at the same time the biggest net importers (green bar). As the figure indicates, most of the larger economies in Europe, including Germany's, do not refine enough jet fuel to meet their demand (blue bar) and must import jet fuel.

According to the IEA (2020) World Energy Outlook [13], jet fuel accounts for only 5 percent of the output of German refineries. Because Germany does not refine enough jet fuel for its own uses – or of any fuels – it must import to meet its domestic demands.

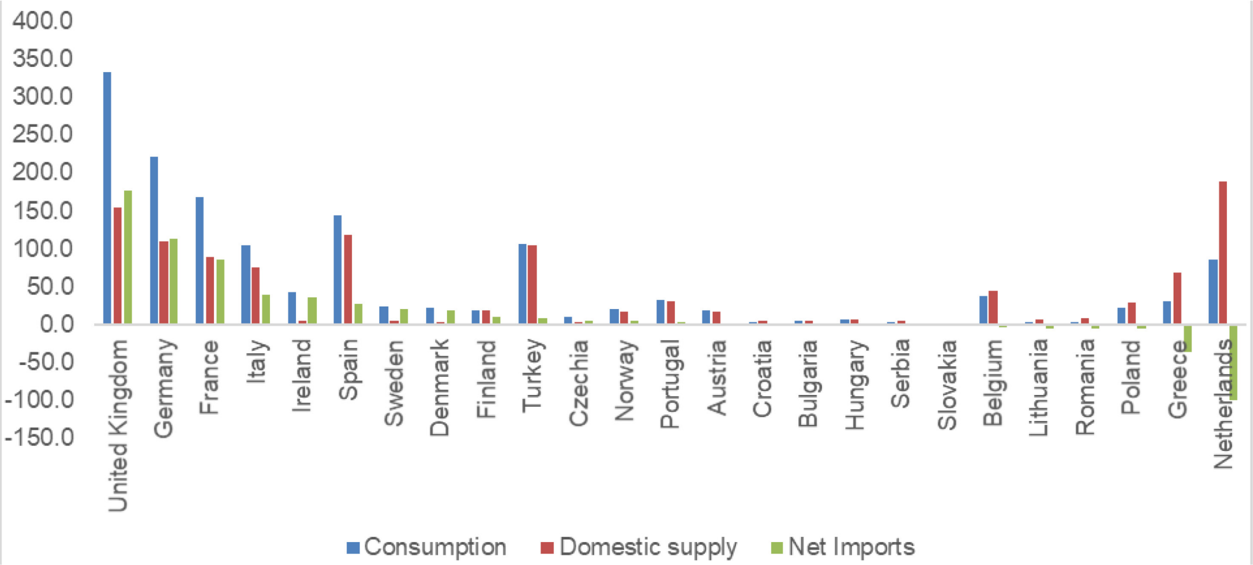


Figure D-2: Consumption, Domestic Supply, and Net Imports of Jet Fuel and Kerosene (kb/d). Source: Eurostat 2018 [37].

D.7 GERMANY AND ENERGY TRANSIT

The Central European Pipeline System (CEPS) provides refined fuel to strategic locations across much of northwestern Europe. The CEPS and its counterpart, the North European Pipeline System (NEPS), are two multinational networks that, along with eight national pipeline systems, comprise the NATO Pipeline System (NPS). This pipeline system was created during the Cold War to supply NATO forces, and specifically their airbases in Central Europe, with refined jet fuel and lubricants. The CEPS is the largest oil product pipeline system in Europe, carrying and storing jet aviation fuel across Belgium, France, Germany, Luxembourg, and the Netherlands. The current total pipeline has a length of 5,314 km [38] with 82 cm to 122 cm diameter pipes and an overall storage capacity of greater than 1 million cubic meters [38]. Management of the CEPS is controlled by the five host nations and the United States, as a user nation.

Refined fuel is injected into the CEPS by tankers at various ports, including Le Havre, Dunkirk, and Marseille (France), Ghent and Antwerp (Belgium), and Amsterdam (the Netherlands). The fuel flows from the entry points and connects directly to 20 military airbases, six civilian airports in Central Europe, and storage tanks. Fuel can also be injected from refineries connected to the CEPS network. The refineries in Germany connected to the CEPS are listed in Table D-1. Three of the refineries – the aforementioned Bayernoil refineries at Vohburg and Neustadt an der Donau, as well as a refinery in Karlsruhe – are partially owned by Rosneft, a Russian state-owned company.

Table D-1: German Refineries Connected to CEPS and their Ownership. Source: Global Energy Monitory Wiki (https://www.gem.wiki/Main_Page) and other sources.

Location	Lat	long	Refining Capacity (kbd)	Main Owner	Ownership
Bayernoil	48.78676	11.753143	220	Vitol	51.43% Vitol through Varo Energy, 28.57% Rosneft, 20% ENI
Inglostadt	48.79193	11.48214	110	Gunvor	Gunvor
Karlsruhe	49.04701	8.328769	287	Shell	32.25% Shell, 25% ExxonMobil, 24% Rosneft, 18.75% ConocoPhillips
Lingen	52.55868	7.310258	95	BP	BP
Rheinland	50.81415	7.00547	325	Shell	Shell

The CEPS network (Figure D-3) reached its peak coverage in terms of pipeline length and number of outlet locations in the 1980s. With the end of the Cold War and a decline in military demand for refined petroleum products, NATO started progressively deactivating pipeline sections, decommissioning injection and offloading points, and/or leasing pipeline connection points to commercial companies [38]. As a result, between 1993 and 2016, the German part of the network was reduced from 3,026 kilometers to 1,750 kilometers, while the number of high-pressure pumps was reduced from 50 to 22, tanker-truck filling stations from 31 to 11, and railway tank filling stations from 3 to 2 [39]. Although commercial contracts include provisions permitting granting Western militaries priority access during a crisis, the contraction of the CEPS has meant a decline in the redundancy of outlet terminals and an overall weakening of system-wide resilience.

Moreover, because the CEPS was built to support a Cold War force posture, it terminates near the border between the former East Germany and the former West Germany, creating a lack of a product pipeline between Western and Central-Eastern Europe. The lack of a dedicated pipeline distribution network for military-grade products challenges the ability to support land and air forces operating east of the previous intra-German border.

D.8 GERMANY AND ENERGY STORAGE

According to EU regulations, EU countries are required to maintain emergency stocks of crude oil and/or oil products equal to at least “90 days of average daily net imports or 61 days of average daily inland consumption, whichever of the two quantities is greater” [40]. The EU directive aligns with Germany’s Petroleum Stockholding Act which led to the creation in 1978 of the Erdölbevorratungsverband (EBV). EBV is a public corporation, responsible for holding Germany’s emergency oil stocks [41].

Germany has a total storage capacity of 62 million cubic meters (mcm), of which 40 percent is composed of caverns [34], p. 189. As of 2019, Germany consistently maintained at least 91 days of its average daily demand in storage [34]. According to EBV’s website, average demand is based on the average of crude oil and petroleum products imported into the Federal Republic of Germany over 90 days. EBV is currently holding approximately 24 mcm of product or approximately 39 percent of the available storage capacity. Furthermore, “reserves can be held as crude oil or as products, namely gasoline, diesel, heating oil, and aviation fuel. At least one-third of the stockholding must be in products” [41]. Storage locations are distributed throughout Germany in stock areas such that the minimum stock in any area is equivalent to 15 days of supply [41].

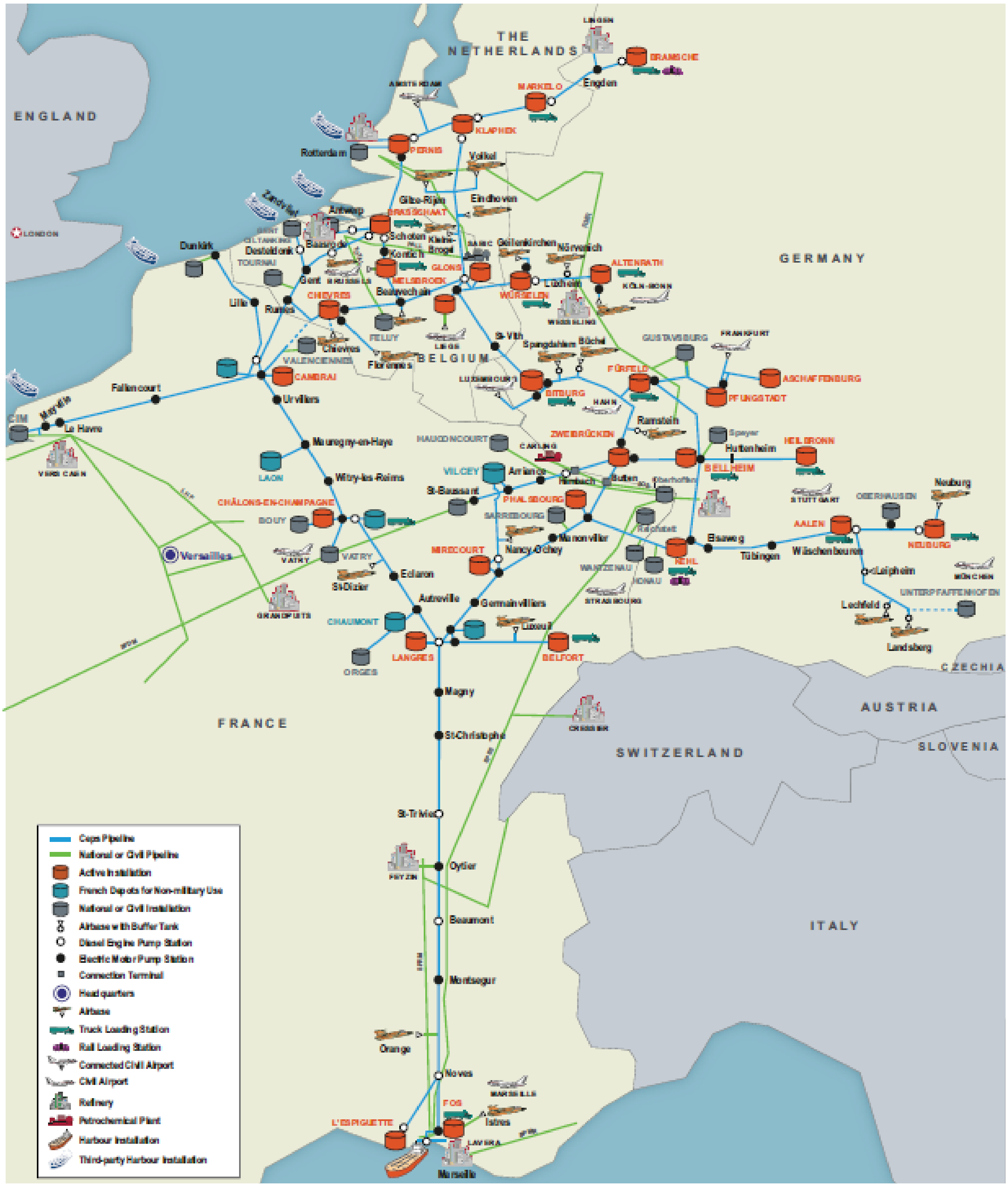


Figure D-3: CEPS Consolidated Pipeline Map (Source: NATO NSPA) [42].

Commercially owned and operated fuel depots represent another source of energy storage in Germany. Currently, fuel depots in Germany are almost exclusively used for gasoline and diesel fuel. Most of the tanks dedicated to jet fuel are located at major airports, but even these have a limited capacity. However, converting existing diesel or gasoline tanks into jet fuel storage (pumping and cleaning) can be accomplished in a matter of hours or days. Therefore, potentially every tank farm can be considered a storage location for military-grade jet fuel. The abundance and diversity of these tank farms offer a large amount of flexibility and redundancy in fuel storage options throughout Germany, and it could significantly increase fuel supply and resolve challenges with the distribution of fuel.

D.9 CONCLUSION

Germany's geographic location, its complex history with Russia, and its leadership role in the European Union as well as NATO make it a lynchpin in energy security on the continent. The Russian war in Ukraine has both complicated Germany's role and thrown its entire energy security strategy into question. Previously, Berlin's choices regarding domestic production of energy, the completion of the Nord Stream 2 pipeline, and the designation of natural gas as a sustainable energy source looked likely to strengthen the mutual interests of Germany and Russia. However, with the Scholz government's decision to indefinitely freeze certification of Nord Stream 2, to invest in new liquified natural gas terminals, and to reexamine the closure of Germany's remaining nuclear power plants, it seems clear that serious change is afoot.

Assuming the *Energiewende* objectives are further pursued – and leaving aside questions of whether they will be fully achieved – Scholz's government faces certain unavoidable considerations. For example, sorting out the competing imperatives on energy security, foreign policy, economics, and defence among the three governing parties will not be an easy task in the years ahead. Although the parties have a mutually accepted coalition agreement that prescribes the coalition's stance in each of these areas, the new security situation across the continent as a result of the war in Ukraine will demand creative political skills and compromise [43]. Ultimately, this sorting out may prove to be the most difficult task of all for the three-party government in Berlin.

Beyond domestic political party concerns, Berlin must consider what constitutes energy security and civil preparedness for Germany in the context of the NATO Treaty's Article 5, which commits the allies to mutual defence, and Article 3, which requires allies to build and maintain their individual capacity to resist attack. Germany's announcement of a EUR100 billion defence investment fund will significantly strengthen the country's conventional defence capacity and capabilities. This should enable Germany to play a stronger role in defence matters especially in Eastern Europe, where Berlin's cozy energy relationship with Russia has caused most concern. Meanwhile, non-traditional defence investment – including in societal resilience – has become especially salient in recent years given Russia's willingness to use energy as a political weapon in strategic competition below the threshold of armed conflict, China's efforts to acquire control over utilities and other militarily relevant infrastructure across Europe, and the ability of non-state actors to attack energy infrastructure through the internet [44], [45], [46]. Related to this are questions regarding the cost effectiveness of wind, solar, and hydro power, as well as the economics, logistics, and timeline for an eventual conversion of domestic pipeline infrastructure and powerplants from natural gas to hydrogen [47], [48]. As Germany's energy transition unfolds, its ability to navigate the various international, national, regional, public, and private interests at the intersection of energy security and hybrid conflict will continue to challenge policy-makers in Berlin.

D.10 REFERENCES

[1] Statistisches Bundesamt, data for 2021. https://www.destatis.de/DE/Themen/GesellschaftUmwelt/Bevoelkerung/Bevoelkerungsstand/_inhalt.html;jsessionid=43E63F3F0494244127F701ED8F5156BF.live732

[2] Statista. “Gross domestic product at current market prices of selected European countries.” Data for 2020. https://www.statista.com/statistics/685925/gdp-of-european-countries/

[3] Calimanu, S. “The Top 20 largest economies in the world by GDP.” February 8th, 2021. https://researchfdi.com/world-gdp-largest-economy/

[4] Romanova, T. “Is Russian energy policy towards the EU only about geopolitics? The case of the Third Liberalisation Package,” Geopolitics, 21(4), 2016, 857-879. DOI: 10.1080/14650045.2016.1155049.

[5] Statistisches Bundesamt, “Gross electricity production in Germany,” January 11, 2022. https://www.destatis.de/EN/Themes/Economic-Sectors-Enterprises/Energy/Production/Tables/gross-electricity-production.html

[6] Hockenos, P. “The history of the Energiewende,” Clean Energy Wire, June 22, 2015, https://www.cleanenergywire.org/dossiers/history-energiewende

[7] Bordoff, . and O’Sullivan, M. “Green upheaval: The new geopolitics of energy,” Foreign Affairs, 101(1), January/February 2022, 68-84.

[8] “Germany closes half its remaining nuclear power plants.” https://www.dw.com/en/germany-closes-half-its-remaining-nuclear-power-plants/a-60302362 Accessed 31 December 2021.

[9] Appunn, K. “Coal in Germany,” Clean Energy Wire, February 7, 2019, https://www.cleanenergywire.org/factsheets/coal-germany Accessed 5 January 2022.

[10] Platts Analytics Consulting for the European Commission, “Study on Member States Notifications on Investment Projects in Energy Infrastructure, according to Regulation” EU 256/2014, 2014

[11] Umweltbundesamt, “Primärenergiegewinnung und -importe”. (May 10, 2021). https://www.umweltbundesamt.de/daten/energie/primaerenergiegewinnung-importe

[12] World Energy Council Weltenergierat Deutschland, Energie für Deutschland: Fakten, Perspektiven und Positionen im globalen Kontext 2020. (Berlin 2020). 134ff. https://www.weltenergierat.de/wp-content/uploads/2020/06/Energie-f%C3%BCr-Deutschland-2020_small.pdf

[13] International Energy Association (IEA), “World energy outlook,” 2020.

[14] Kirsten Westphal, “German-Russian gas relations in face of the energy transition,” Russian Journal of Economics 6(4), 2020, pp. 406-423, DOI: 10.32609/j.ruje.6.55478.

[15] Meister, S. “From ostpolitik to EU-Russia interdependence: Germany’s perspective,” in Kristi Raik and András Rácz, eds., Post-Crimea Shift in EU-Russia Relations: From Fostering Interdependence to Managing Vulnerabilities, Tallinn, Estonia: International Centre for Defence and Security, 2019, pp. 25-44.

[16] Treverton, G.F. America, Germany, and the Future of Europe, Princeton University Press, 1992.

[17] Karnitschnig, M., von der Burchard, H., Eder, F., and Desiderio, A. “Inside Olaf Scholz’s historic shift on defense, Ukraine and Russia,” Politico, March 5, 2022, https://www.politico.eu/article/olaf-scholz-historic-shift-defense-ukraine-russia-war

[18] Federal Ministry of Defence, "White Paper 2006 on German Security Policy and the future of the Bundeswehr," 2006, p. 47.

[19] Steitz, C., Alkousaa, R. and Sheahan, M. "Nuclear, coal, LNG: 'no taboos' in Germany's energy about-face," Reuters, February 27, 2022, https://www.reuters.com/business/energy/germany-step-up-plans-cut-dependence-russia-gas-2022-02-27/

[20] Besch, S. and Brockmeier, S. "Waking a sleeping giant: What's next for German security policy?" War on the Rocks, March 9, 2022, https://warontherocks.com/2022/03/waking-a-sleeping-giant-whats-next-for-german-security-policy/

[21] Knight, B. "Germany's Russia policy in tatters after Russian invasion of Ukraine," Deutsche Welle, February 24, 2022, https://p.dw.com/p/47QHx

[22] Rácz, A. "Germany's shifting policy towards russia: The sudden end of ostpolitik," Finnish Institute of International Affairs Briefing Paper 335, March 2022, https://www.fiia.fi/wp-content/uploads/2022/03/bp335_germanys-shifting-policy-towards-russia_the-sudden-end-of-ostpolitik_andras-racz.pdf

[23] Wehrmann, B. "Russia's invasion of Ukraine forces Germany to come clean on energy transition strategy," Clean Energy Wire, February 28, 2022, https://www.cleanenergywire.org/news/russias-invasion-ukraine-forces-germany-come-clean-energy-transition-strategy

[24] Brew, G. "From pledges to action? Europe's move away from Russian fossil fuels," War on the Rocks, March 4, 2022, https://warontherocks.com/2022/03/from-pledges-to-action-europes-move-away-from-russian-fossil-fuels/

[25] Pronczuk, M. "E.U. sees adequate winter energy, but seeks longer-term independence," New York Times, February 28, 2022, https://www.nytimes.com/2022/02/28/business/energy-environment/russia-eu-energy.html

[26] Kurmayer, N.J. "Germany takes firm pro-gas stance in green taxonomy feedback to EU," EURACTIV.com, January 24, 2022, https://www.euractiv.com/section/energy-environment/news/germany-takes-firm-pro-gas-stance-in-green-taxonomy-feedback-to-eu/

[27] Geropoulos, K. "EU wants gas, nuclear energy classified green, sustainable," New Europe, January 6, 2022. https://www.neweurope.eu/article/eu-wants-gas-nuclear-energy-classified-green-sustainable/

[28] Heddenhausen, M. "Privatisations in Europe's liberalised electricity markets – the cases of the United Kingdom, Sweden, Germany and France". Stiftung Wissenschaft und Politik, December 2007, pp. 4-16. https://www.swp-berlin.org/publications/products/projekt_papiere/Electricity_paper_KS_IIformatiert.pdf

[29] Monstadt, J. and Neumann, M. Netzgebundene infrastrukturen unter Veränderungsdruck – Sektoranalyse Stromversorgung. Berlin: Leibniz-Institut für Regionalentwicklung und Strukturplanung, 2003, 17. https://www.irbnet.de/daten/rswb/04039004571.pdf

[30] Bundesamt für Sicherheit in der Informationstechnik (BSI), Die Lage der IT-Sicherheit in Deutschland 2018. Bonn, September 2018. 11. https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/bsi-lagebericht-2018.pdf?__blob=publicationFile&v=3

[31] Bundesamt für Sicherheit in der Informationstechnik (BSI), Die Lage der IT-Sicherheit in Deutschland 2019. Bonn Oktober 2019. 47. https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/bsi-lagebericht-2019.pdf?__blob=publicationFile&v=4

[32] Conventional Energy Sources, Federal Ministry of Economic Affairs and Climate Action https://www.bmwi.de/Redaktion/EN/Textsammlungen/Energy/gas.html?cms_artId=253734

[33] Monforti, F. and Szikszai, A. “A Monte Carlo approach for assessing the adequacy of the European gas transmission system under supply crisis conditions,” Energy Policy 38 (2010), pp. 2486-2498.

[34] International Energy Agency (IEA). Germany Energy Policy Review, 2020. https://www.iea.org/reports/germany-2020

[35] BP Statistical Review of World Energy 2021.

[36] Perkins, R. “Rosneft to become Germany’s number two refiner after move on Shell stake,” SP Global, November 2021 https://www.spglobal.com/platts/en/market-insights/latest-news/oil/111721-rosneft-expands-german-refining-footprint-with-move-to-buy-shells-schwedt-stake

[37] Eurostat 2018. https://ec.europa.eu/eurostat/data/database

[38] NATO Support and Procurement Agency (NSPA),” website, NATO Support and Procurement Agency, January 23, 2018. As of March 2, 2021: http://www.nspa.nato.int/en/organization/CEPS/network.htm

[39] http://www.fbg.de/broschuere/fbg_broschuere.pdf p. 3.

[40] Council Directive 2009/119/EC of 14 September 2009 imposing an obligation on the Member States to maintain minimum stocks of crude oil and/or petroleum products, as of August 21, 2020: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0119&from=EN

[41] EBV corporate website About Us https://www.ebv-oil.org/cmse/cms2.asp?sid=57&nid=&cof=57, December 2021.

[42] NATO NSPA. N.d. CEPS Network. As of 23 January 2018: http://www.nspa.nato.int/en/organization/CEPS/network.htm

[43] Besch, S., Odendahl, C., Gordon, N. Six Questions On Germany’s New Coalition Agreement Insight 26 November 2021. [PDF of Agreement embedded here] https://www.cer.eu/insights/six-questions-germanys-new-coalition-agreement Accessed 4 January 2022.

[44] Sestanovich, S. “Is Russia using energy as a weapon again?” Council on Foreign Relations, October 28, 2021, https://www.cfr.org/in-brief/russia-using-energy-weapon-again

[45] Deni. J.R. et al., China, Europe, and the Pandemic Recession: Beijing’s Investments and Transatlantic Security, Carlisle, PA: U.S. Army War College Press, 2022.

[46] Plumer, B. “Pipeline Hack Points to Growing Cybersecurity Risk for Energy System,” New York Times, May 13, 2021, https://www.nytimes.com/2021/05/13/climate/pipeline-ransomware-hack-energy-grid.html

[47] “NATO’s role in energy security.” https://www.nato.int/cps/en/natohq/topics_49208.htm Accessed 4 January 2022

[48] “Resilience and Article 3.” https://www.nato.int/cps/en/natohq/topics_132722.htm Accessed 1 January 2022.

REPORT DOCUMENTATION PAGE

1. Recipient's Reference	2. Originator's References	3. Further Reference	4. Security Classification of Document
	STO-TR-SAS-163 AC/323(SAS-163)TP/1164	ISBN 978-92-837-2476-6	PUBLIC RELEASE

5. Originator

Science and Technology Organization
North Atlantic Treaty Organization
BP 25, F-92201 Neuilly-sur-Seine Cedex, France

6. Title

Energy Security in the Era of Hybrid Warfare

7. Presented at/Sponsored by

Final technical report.

8. Author(s)/Editor(s)	9. Date
Multiple	May 2024

10. Author's/Editor's Address	11. Pages
Multiple	174

12. Distribution Statement

There are no restrictions on the distribution of this document. Information about the availability of this and other STO unclassified publications is given on the back cover.

13. Keywords/Descriptors

Cyber; Energy; Hybrid warfare; Operational energy; Readiness; Risk; Supply chain; Warfare

14. Abstract

NATO's military logistics and supply chain systems are now challenged by the tyranny of distance, near peer adversaries, and tight energy in a manner unseen since World War II. Moreover, the ability to leverage technology for geo-political gain against an adversary's vulnerabilities, broadly referred to as hybrid warfare, has become increasingly prevalent in the 21st Century. The project's focus on energy security is rooted in the pretext that it is fundamentally the most vulnerable sector and possesses the largest potential to destabilize a society. This includes mitigating the impact on civilian and military infrastructure and interests and develop countermeasures.

Additionally, the two main components of the hybrid warfare and energy security dynamic are cyber defence and malign influence. There is a need to raise awareness of the energy-hybrid warfare nexus, identify its broader impact in the civilian and military realms within NATO, and define courses of action. The key findings from the study can be categorized as the near-term energy insecurity among the NATO Member States, persistent cyber threats to the energy sector, energy sector supply chain vulnerabilities, the impact on NATO's operational energy and military capabilities, and malign influence in the energy sector can have significant consequences into the future.

NORTH ATLANTIC TREATY ORGANIZATION

NATO
OTAN

BP 25
F-92201 NEUILLY-SUR-SEINE CEDEX • FRANCE
Télécopie 0(1)55.61.22.99 • E-mail mailbox@cso.nato.int

SCIENCE AND TECHNOLOGY ORGANIZATION

DIFFUSION DES PUBLICATIONS
STO NON CLASSIFIEES

Les publications de l'AGARD, de la RTO et de la STO peuvent parfois être obtenues auprès des centres nationaux de distribution indiqués ci-dessous. Si vous souhaitez recevoir toutes les publications de la STO, ou simplement celles qui concernent certains Panels, vous pouvez demander d'être inclus soit à titre personnel, soit au nom de votre organisation, sur la liste d'envoi.

Les publications de la STO, de la RTO et de l'AGARD sont également en vente auprès des agences de vente indiquées ci-dessous.

Les demandes de documents STO, RTO ou AGARD doivent comporter la dénomination « STO », « RTO » ou « AGARD » selon le cas, suivi du numéro de série. Des informations analogues, telles que le titre est la date de publication sont souhaitables.

Si vous souhaitez recevoir une notification électronique de la disponibilité des rapports de la STO au fur et à mesure de leur publication, vous pouvez consulter notre site Web (http://www.sto.nato.int/) et vous abonner à ce service.

CENTRES DE DIFFUSION NATIONAUX

ALLEMAGNE
Streitkräfteamt / Abteilung III
Fachinformationszentrum der Bundeswehr (FIZBw)
Gorch-Fock-Straße 7, D-53229 Bonn

BELGIQUE
Royal High Institute for Defence – KHID/IRSD/RHID
Management of Scientific & Technological Research for Defence, National STO Coordinator
Royal Military Academy – Campus Renaissance
Renaissancelaan 30, 1000 Bruxelles

BULGARIE
Ministry of Defence
Defence Institute "Prof. Tsvetan Lazarov"
"Tsvetan Lazarov" bul no.2, 1592 Sofia

CANADA
DGSIST 2
Recherche et développement pour la défense Canada
60 Moodie Drive (7N-1-F20), Ottawa, Ontario K1A

DANEMARK
Danish Acquisition and Logistics Organization
Lautrupbjerg 1-5, 2750 Ballerup

ESPAGNE
Área de Cooperación Internacional en I+D
SDGPLATIN (DGAM), C/ Arturo Soria 289
28033 Madrid

ESTONIE
Estonian National Defence College
Centre for Applied Research
Riia str 12, Tartu 51013

ETATS-UNIS
Defense Technical Information Center
8725 John J. Kingman Road
Fort Belvoir, VA 22060-6218

FINLAND
Ministry for Foreign Affairs
Telecommunications Centre (24/7)
P.O Box 176, FI-00023 Government

FRANCE
O.N.E.R.A. (ISP)
29, Avenue de la Division Leclerc
BP 72, 92322 Châtillon Cedex
O.N.E.R.A. (ISP)

GRECE (Correspondant)
Defence Industry & Research General
Directorate, Research Directorate
Fakinos Base Camp, S.T.G. 1020
Holargos, Athens

HONGRIE
Hungarian Ministry of Defence
Development and Logistics Agency
P.O.B. 25, H-1885 Budapest

ITALIE
Ten Col Renato NARO
Capo servizio Gestione della Conoscenza
F. Baracca Military Airport "Comparto A"

LUXEMBOURG
Voir Belgique

NORVEGE
Norwegian Defence Research Establishment, Attn: Biblioteket
P.O. Box 25, NO-2007 Kjeller

PAYS-BAS
Royal Netherlands Military Academy Library
P.O. Box 90.002, 4800 PA Breda

POLOGNE
Centralna Biblioteka Wojskowa
ul. Ostrobramska 109,
04-041 Warszawa

PORTUGAL
Estado Maior da Força Aérea
SDFA – Centro de Documentação
Alfragide, P-2720 Amadora

ROUMANIE
Romanian National Distribution Centre
Armaments Department
9-11, Drumul Taberei Street
Sector 6
061353 Bucharest

ROYAUME-UNI
Dstl Records Centre
Rm G02, ISAT F, Building 5
Dstl Porton Down
Salisbury SP4 0JQ

SLOVAQUIE
Akadémia ozbrojených síl gen.
M.R. Štefánika, Distribučné a informačné stredisko STO
Demänová 393
031 01 Liptovský Mikuláš 1

SLOVENIE
Ministry of Defence
Central Registry for EU & NATO
Vojkova 55
1000 Ljubljana

SUEDE
Regeringskansliet,
Attn: Adam Hidestå
RK IF AR 5
S-103 33 Stockholm

TCHEQUIE
Vojenský technický ústav s.p.
CZ Distribution Information
Mladoboleslavská 944
PO Box 18, 197 06 Praha 9

TURQUIE
Milli Savunma Bakanlığı (MSB)
ARGE ve Teknoloji Dairesi
Başkanlığı
06650 Bakanliklar – Ankara

AGENCES DE VENTE

The British Library Document Supply Centre
Boston Spa, Wetherby
West Yorkshire LS23 7BQ
ROYAUME-UNI

Canada Institute for Scientific and Technical Information (CISTI)
National Research Council Acquisitions
Montreal Road, Building M-55
Ottawa, Ontario K1A 0S2, CANADA

Les demandes de documents STO, RTO ou AGARD doivent comporter la dénomination « STO », « RTO » ou « AGARD » selon le cas, suivie du numéro de série (par exemple AGARD-AG-315). Des informations analogues, telles que le titre et la date de publication sont souhaitables. Des références bibliographiques complètes ainsi que des résumés des publications STO, RTO et AGARD figurent dans le « NTIS Publications Database » (http://www.ntis.gov).

NORTH ATLANTIC TREATY ORGANIZATION

NATO
OTAN

BP 25
F-92201 NEUILLY-SUR-SEINE CEDEX • FRANCE
Télécopie 0(1)55.61.22.99 • E-mail mailbox@cso.nato.int

SCIENCE AND TECHNOLOGY ORGANIZATION

DISTRIBUTION OF UNCLASSIFIED STO PUBLICATIONS

AGARD, RTO & STO publications are sometimes available from the National Distribution Centres listed below. If you wish to receive all STO reports, or just those relating to one or more specific STO Panels, they may be willing to include you (or your Organisation) in their distribution.

STO, RTO and AGARD reports may also be purchased from the Sales Agencies listed below.

Requests for STO, RTO or AGARD documents should include the word 'STO', 'RTO' or 'AGARD', as appropriate, followed by the serial number. Collateral information such as title and publication date is desirable.

If you wish to receive electronic notification of STO reports as they are published, please visit our website (http://www.sto.nato.int/) from where you can register for this service.

NATIONAL DISTRIBUTION CENTRES

BELGIUM
Royal High Institute for Defence – KHID/IRSD/RHID
Management of Scientific & Technological Research for Defence, National STO Coordinator
Royal Military Academy – Campus Renaissance
Renaissancelaan 30, 1000 Brussels

BULGARIA
Ministry of Defence
Defence Institute "Prof. Tsvetan Lazarov"
"Tsvetan Lazarov" bul no.2, 1592 Sofia

CANADA
DSTKIM 2
Defence Research and Development Canada
60 Moodie Drive (7N-1-F20)
Ottawa, Ontario K1A 0K2

CZECHIA
Vojenský technický ústav s.p.
CZ Distribution Information Centre
Mladoboleslavská 944
PO Box 18, 197 06 Praha 9

DENMARK
Danish Acquisition and Logistics Organization (DALO)
Lautrupbjerg 1-5, 2750 Ballerup

ESTONIA
Estonian National Defence College
Centre for Applied Research
Riia str 12, Tartu 51013

FINLAND
Ministry for Foreign Affairs
Telecommunications Centre (24/7)
P.O Box 176, FI-00023 Government

FRANCE
O.N.E.R.A. (ISP)
29, Avenue de la Division Leclerc – BP 72
92322 Châtillon Cedex

GERMANY
Streitkräfteamt / Abteilung III
Fachinformationszentrum der Bundeswehr (FIZBw)
Gorch-Fock-Straße 7, D-53229 Bonn

GREECE (Point of Contact)
Defence Industry & Research General Directorate, Research Directorate
Fakinos Base Camp, S.T.G. 1020
Holargos, Athens

HUNGARY
Hungarian Ministry of Defence
Development and Logistics Agency
P.O.B. 25, H-1885 Budapest

ITALY
Ten Col Renato NARO
Capo servizio Gestione della Conoscenza
F. Baracca Military Airport "Comparto A"
Via di Centocelle, 301, 00175, Rome

LUXEMBOURG
See Belgium

NETHERLANDS
Royal Netherlands Military Academy Library
P.O. Box 90.002, 4800 PA Breda

NORWAY
Norwegian Defence Research Establishment, Attn: Biblioteket
P.O. Box 25, NO-2007 Kjeller

POLAND
Centralna Biblioteka Wojskowa
ul. Ostrobramska 109
04-041 Warszawa

PORTUGAL
Estado Maior da Força Aérea
SDFA – Centro de Documentação
Alfragide, P-2720 Amadora

ROMANIA
Romanian National Distribution Centre
Armaments Department
9-11, Drumul Taberei Street, Sector 6
061353 Bucharest

SLOVAKIA
Akadémia ozbrojených síl gen. M.R. Štefánika, Distribučné a informačné stredisko STO
Demänová 393
031 01 Liptovský Mikuláš 1

SLOVENIA
Ministry of Defence
Central Registry for EU & NATO
Vojkova 55, 1000 Ljubljana

SPAIN
Área de Cooperación Internacional en SDGPLATIN (DGAM)
C/ Arturo Soria 289
28033 Madrid

SWEDEN
Regeringskansliet, Attn: Adam Hideståł
RK IF AR 5
S-103 33 Stockholm

TÜRKIYE
Milli Savunma Bakanlığı (MSB)
ARGE ve Teknoloji Dairesi Başkanlığı
06650 Bakanliklar – Ankara

UNITED KINGDOM
Dstl Records Centre
Rm G02, ISAT F, Building 5
Dstl Porton Down,
Salisbury SP4 0JQ

UNITED STATES
Defense Technical Information Center
8725 John J. Kingman Road
Fort Belvoir,
VA 22060-6218

SALES AGENCIES

The British Library Document Supply Centre
Boston Spa, Wetherby
West Yorkshire LS23 7BQ
UNITED KINGDOM

Canada Institute for Scientific and Technical Information (CISTI)
National Research Council Acquisitions
Montreal Road, Building M-55
Ottawa, Ontario K1A 0S2, CANADA

Requests for STO, RTO or AGARD documents should include the word 'STO', 'RTO' or 'AGARD', as appropriate, followed by the serial number (for example, AGARD-AG-315). Collateral information such as title and publication date is desirable. Full bibliographical references and abstracts of STO, RTO and AGARD publications are given in "NTIS Publications Database" (http://www.ntis.gov).

ISBN 978-92-837-2476-6