LUISS

Department of Political Science

Master's Degree in International Relations

Chair of Security Policies

Cybersecurity Risks and Challenges of the Energy Transition: Securing Critical Energy Infrastructure

Gen. S.A Carlo Magrassi

Supervisor

Prof. Marco Simoni

Co-Supervisor

Matr.653342 Yasmina Dionisi

Candidate

ACADEMIC YEAR 2023/2024

A Paolo, Tala e Yara

Un ringraziamento sincero ai Professori Magrassi e Pasquazzi, che mi hanno incoraggiata costantemente e guidata nell'opera bibliografica e nell'organizzazione logica del mio lavoro.

Grazie a Flavia, Anna, Marella,
Irene, Alice, Bianca e Camilla.

L'ingegno è vedere possibilità dove altri non ne vedono.
ENRICO MATTEI

ABSTRACT

This dissertation analyses the cybersecurity challenges facing critical energy infrastructure, notably in the context of the global energy transition to renewable sources. With the increasing digitalization of energy systems, these infrastructures are more susceptible to cyber-attacks, posing significant risks to national security, economic stability, and public safety. This study examines the typologies of cyberattacks, with particular attention to actors, methods, motivations, and targets. The effectiveness of existing cybersecurity policies is assessed, ranging from national security strategies, regulatory frameworks, cyber diplomacy, technology and innovation research & development and investments, and public-private partnerships. The need for a holistic approach that integrates these different key players is emphasized. The thesis also acknowledges the continued vulnerability of these infrastructures to physical attacks. The goal is to provide findings to enhance the resilience of critical energy infrastructure of the energy transition, for the public and private sector alike, underscoring the necessity for adaptive and robust security measures in safeguarding the future of energy systems.

Summary

List of figures

List of abbreviations

ACER	European Union Agency for the Cooperation of Energy Regulators
CEER	Council of European Energy Regulators
CESER	U.S. Office of Cybersecurity, Energy Security and Emergency Response
CSIS	Center for Strategic and International Studies
DDErS	Distributed Energy Resources
ESCAP	United Nations Office Economic and Social Commission for Asia and the Pacific
IEA	International Energy Agency
ILO	International Labor Organization
IRENA	International Renewable Energy Agency
IoTs	Internet-of-Things
OSCE	Organization for Security and Co-operation in Europe
UNOCT	United Nations Office of Counterterrorism
UNODC	United Nations Office on Drugs and Crime

Introduction

Energy is crucial to ensure critical societal needs. In addition to being an issue of utmost importance to policymakers, businesses, and societies whose quality of life depends on its uninterrupted supply, energy is a precondition to economic growth, political stability, and prosperity. In this context, the energy transition from fossil fuels to renewable sources is crucial for combating climate change and ensuring a sustainable future. Modern energy consumption, particularly the use of fossil fuels like oil, coal, and natural gas, has significantly contributed to climate change by increasing CO_2 levels, which are major drivers of global warming.

Combating climate is not the only reason driving this transition, as energy security - of polysemous and multidimension nature - is deeply linked to geopolitical influence and control.
More than half of the energy consumed in Europe is imported. Energy-rich countries with significant reserves of fossil fuels use their energy resources as a leverage in international relations.

The shock of the Russia-Ukraine served as a jolting revelation for Europe as European countries realized the stable flow of affordable energy was no longer a given. Renewable energy systems emerge as a paradigm that can approve the security of energy supply for electricity, cooling, heating, and transport fuels: diversifying the energy mix reduces risks associated with over-reliance on any single energy resource, if faced with supply disruptions due to geopolitical issues, among other things.

The energy transition can add additionally entail economic growth and innovation, as emerging industries are being forged as well as markets focused on renewable energy and policies promoting sustainable energy directly contribute to broader sustainable development goals, from poverty reduction, environmental conservation.

As such: how is this green transition taking place? A study of the changing landscape of critical energy infrastructure entails an exploration of two of the most important foundational pillars of the energy transition, that is, digitalization and decentralization.

Digitalization in the energy sector is bringing forward the integration of digital technologies, from advanced analytics, Internet of Things (IoT) devices, artificial intelligence, and notably, smart grid technologies. This transformative process is not only transforming how energy is generated, distributed, and consumed, it is equally facilitating the seamless integration of renewable energy sources.

Decentralized energy systems refer to the shifting from centralized energy generation, and distribution systems, towards more distributed and localized sources of energy production. It is characterized by positioning energy production facilities closer to the site of energy consumption, allowing for more optimal use of renewable energy.

In digitalization, smart grids, Internet of Things applications and artificial intelligence are key assets. With decentralization, the reorganization of a single, concentrated, energy-generation facility into smaller more autonomous energy generation units, distributed generation - through rooftop solar panels, electric vehicles and battery storage are examples of the shift to small-scale energy generation. Electricity production is no longer limited to large and centralized generators and retailers but rather, sees consumers grasp the opportunity to be more proactive, producing their electricity for their own production, or to be sold on the market.

Insights reveal that the current pace of renewable deployment showcases significant opportunities for growth. These transformations are supported by policy initiatives, crucial for fostering the needed transformation, starting from digitalization. Examples include the main EU policy framework for achieving the renewable revolution known as the “European climate law”, the Fit for 55 Package, which makes reaching the EU’s climate goal of reducing its emissions by at least 55% by 2030 a legal obligation. Moreover, industries and the private sector are manifesting themselves in the digitalization of energy systems in keyways, including technology research and innovation, investment and funding, partnerships, and collaboration.

The critical infrastructure of the energy transition is therefore undergoing a profound transformation, driven by the rapid advancements in digitalization and technology, in an evolution that brings numerous benefits including enhanced efficiency, better resource management and a significant boost in our ability to integrate renewable energy sources seamlessly.

However, some key challenges still need to be addressed. Two main challenges that exist posing barriers and threats to progress one concerns the economic and management costs associated with the adoption of technologies, the other, concerning the security of the infrastructures involved.

This dissertation focuses on the latter. Incorporating digital technologies will be a key factor in shaping the industry's future, but it paves the way for emerging, sophisticated, and particularly dangerous cyberthreats.

In fact, the cyberspace has acquired a pivotal role in most present economic, commercial, cultural, social and government activities and interactions between countries. The modern world is highly dependent on electronic technology and most importantly, on the Internet.

Within this vast global network which the Internet has created, vital and sensitive infrastructures and systems are an integral part.

Cyber-threats are particularly unique threats that must be distinguished from traditional national security threats. The Russia-Ukraine war has in fact significantly contributed to increasing the frequency, spread, and intensify of cyber-attacks against the energy sector but these have roots that precede the beginning of the military confrontation between Moscow and Kiev.

As critical energy infrastructure is deemed, by virtually every jurisdiction, as an object of national security, with risks heightened due to critical infrastructure cross-sectoral and cross- brooder interdependencies a study of the main threats, actors, and motivation is essential for developing adequate and efficient cyber strategies and policies.

Case studies of known cyberattacks against critical energy infrastructures will be discussed. In particular, the Stuxnet attack on Iran's nuclear Programme in 2010, the Shamoon attack to Saudi Aramco in 2012, the Black Energy and Industroyer attacks on the Ukraine Power Grid in 2015 and 2016 respectively. These case-studies reveal a taxonomy of cyber-attacks for the contemporary and evolving energy infrastructure.

Types of attacks include malware, the most widely used cyber security threat, constantly tailored and aimed at industrial control systems, social engineering, defined as malicious activities accomplished through human interactions precisely, psychological manipulation aimed at tricking users into making security mistakes, or giving away sensitive information, blockchain-related cyber risks - which combine novel cryptographic methods and blockchains, decentralized digital records that allow both data integrity and transparency, manipulation of artificial intelligence and machine learning to make them malfunction, and finally, man-in-the middle and denial of service attacks, attacks that target communication infrastructure. However, real threats ultimately stem from how these attacks methods will affect cyberwarfare, hybrid conflict, and cyber-physical attacks, which wield impacts across human security from both a national and global perspective.

Moving on to attributing attacks, the issue is challenging in cyberspace, both due to technical factors and a lack of agreement on basic definitions, namely on what constitutes an attack or what counts as a critical infrastructure. For instance, holding a government responsible even for attacks originating within its borders, proves a difficult attack - but the recent involvement of state actors as major players in cyber activities has shifted the paradigm from individualism underfunded hackers exploiting systems out of opportunity, to a more strategic approach driven by state interests, as highlighted by the contemporary volatile geopolitical scene. Other attackers include terrorists, cybercriminals, hacktivists, and individuals, but a mention is done to insider threats, which occur when authorized users such as employees, contractors or business partners intentionally or accidentally misuse their legitimate access or have their own accounts hijacked by attackers.

Different attackers have diverse motivations, as different methods of attack have different targets. The next dimension explored is in fact that of the "new" critical infrastructure targets. Smart Grids,

and Distributed Energy Resources such as hydropower, wind farms, and solar farms can be jeopardized by cyberattacks, notably through exploitation of their industrial control systems and operational technology vulnerabilities. Potential attack vectors for these DERs include their own or collector substation physical access to notably cyber access via remote connections. These attacks have a range of impacts on the assets and the systems to which they are connected, notably the smart grid. In addition, a mention is done to critical minerals and the mining sector, which AR although subject of a debate, are part of the energy transition: because of its criticality and strategic position in the global supply chain, the mining industry is particularly under threat from cyberattacks.

Moving on, the analytical framework of cyberattacks goes on to explore the type of security impacts. These range from societal security, economic security, political security, and reputational security.

The final part of the dissertation is dedicated to policies for cybersecurity of critical and digitalized energy infrastructure. Security policies worldwide are transforming in an era where information is as valuable as physical assets. The primary purpose of a security policy is to establish a set of guidelines and procedures that help protect an organization, state, information systems and assets from threats, whether they originate from internal or external sources.

The policies required for cybersecurity of Renewable critical energy infrastructure encompass various essential elements that the dissertation delves to, from regulatory and legal frameworks that have so far underpinned cybersecurity efforts, focusing on national strategies and the challenges faced by international and regional organizations in crafting effective cybersecurity.

Regulatory and legal frameworks, notably though National Cybersecurity Strategies, international decision-making processes, and international intelligence and knowledge sharing are crucial elements of a global cybersecurity strategy in the energy sector, as effects of cyberattacks are cascading and in most cases have cross-border and cross-sectoral impacts.

These go hand in hand with cybersecurity imperatives and investments on key areas of cybersecurity, which this dissertation seeks to identify and prioritize, notably, risk assessments, incident response management, network security through information and operation technology (IT and OT).

Notable other efforts that are explored are policies tackling cybercrime, cyberterrorism, and peacebuilding and cyberdiplomacy to mitigate and prevent cyberwarfare.

Finally, an attention is given to public-private partnerships, which are jointly and mutually actively supported strategies reflecting a convergence of interests. On the one hand, public policy success is assumed to depend on private actor participation, on the other hand, private actors consider their contribution to reaching policy goals to be beneficial in achieving their own goals.

This dissertation ends with an analytical assessment of these policies, as well as an overview of future trends, which are expected to concern emerging AI threats, the further deployment of critical minerals into the smart grids entailing geopolitical incentives for attacks, and the advancement of energy, cyber, and infrastructure diplomacies.

Chapter I: The Critical Infrastructure of the Energy Transition

Access to energy is crucial to ensure critical societal needs. In addition to being an issue of utmost importance to policymakers, businesses, and the substantial community whose quality of life depends on its uninterrupted supply, energy is a precondition to economic growth, political stability, and prosperity[1]. Energy security emerges as a critical challenge and one of the main targets of any energy policy [2].

All societies rely on energy services to meet fundamental human needs. Access to energy is crucial to ensure critical societal needs, from food, lighting, mobility, and communication. Energy is essential for powering modern society's homes, businesses, hospitals, schools, and other essential infrastructure[3].

Energy is equally indispensable for industries like healthcare, manufacturing, and transportation; it fuels industrial processes by powering factories, transportation networks, cars, trains, and airplanes, and agricultural machinery, essential for food production. It supports the operation of communication networks from data centers to information technology infrastructure, supplying servers, internet connectivity, telecommunication systems, and digital devices used in daily life. Further analysis could delve into the ways that energy is energizing society[4].

It is crucial to recognize that the energy sector is experiencing a profound shift, driven by the imperative of climate, referred to as the energy transition. Historically, energy transitions, such as the transition from wood to coal beginning with the Industrial Revolution in the late 18th century,

---

[1] Organization for Security and Co-Operation in Europe (OSCE), *Energy Security* (2017) https://www.osce.org/resources/factsheets/energy-security

[2] Aleh Cherp and Jessica Jewell, "The concept of energy security: Beyond the four As", *Energy Policy* 75 (December 2017): 416, https://doi.org/10.1016/j.enpol.2014.09.005

[3] International Energy Agency (IEA), OECD, *World Energy Outlook* (2023), https://www.oecd-ilibrary.org/energy/world-energy-outlook-2023_827374a6-en

[4] William Moomaw and Mihaela Papa, "Creating a mutual gains climate regime through universal clean energy services", *Climate Policy* 12, no. 4 (January 2012), https://doi.org/10.1080/14693062.2011.644072

and later from coal to natural gas, beginning in the mid 20th century, have responded to need of improving efficiency. Today's "green" transition, however, is primarily focused on the decarbonization of our energy systems[5].

Decarbonization refers to the process of reducing and, ultimately, eliminating carbon dioxide emissions from the energy sector; a goal that can be achieved by transitioning from fossil fuels through electrification, alternative energy sources and renewable energy[6].

On top of that, the current transition underway is uniquely linked to digitalization. Digital technologies are transforming modern energy systems bringing numerous benefits such as enhanced connectivity, real-time access to services, and new opportunities. They have proved to be crucial in tackling climate change and meeting current demand[7].
Furthermore, digitalization fosters innovation and creates new job opportunities, contributing to sustainability and efficiency; in a dual approach that not only addresses environmental concerns but also drives economic growth and technological advancements[8].

When examining the digital transformation of the energy sector, a priority focus should be placed on how digital technologies are transforming critical energy infrastructures. Critical energy infrastructure refers to the systems, facilities, and networks essential for the production, storage, transmission, and distribution of energy; crucial for ensuring the reliable supply of energy necessary for various societal functions and economic activities. Critical energy infrastructure typically includes power plants, transmission and distribution networks, and storage facilities[9].

---

[5] Ibid.

[6] International Labour Organization (ILO), Green jobs, green economy, just transition and related concepts: A review of definitions developed through intergovernmental processes and international organizations (June 2023), https://www.ilo.org/publications/green-jobs-green-economy-just-transition-and-related-concepts-review

[7] International Energy Agency (IEA), OECD, *World Energy Outlook* (2023), https://www.oecd-ilibrary.org/energy/world-energy-outlook-2023_827374a6-en

[8] Ibid.

[9] Nexus Integra, *Digital transformation in 4 large industrial sectors: water, ceramics, oil and energy* (2024), https://nexusintegra.io/ebook-digital-transformation-4-large-industrial-sectors/

In this chapter, we delve into the multifaceted aspects of the energy transition to focus on its profound implications for critical energy infrastructure.

As such, our discussion will encompass not only climate mitigation efforts but also the imperative of energy security, economic opportunities, and the broader projections for sustainable development. The focus will then move to examine how the energy transition is reshaping essential critical energy infrastructure and what constitutes "green energy infrastructure". In particular, the latter is adopting advanced and broad digital technologies to improve efficiency, monitoring, and response capabilities. There is also a trend towards decentralized energy production and incorporating distributed energy resources like solar panels, and wind turbines, into the so-called smart grid. We will also nod to the evolution of smart cities, where critical infrastructure integrates seamlessly with advanced technologies to enhance urban energy efficiency, sustainability, and resilience.

Finally, the current state of the art through real-world applications will be examined.

The ultimate objective of this first chapter is to pave the way for the subsequent discussion and review of cyber-attacks on contemporary critical energy infrastructures. To understand why the green transition has reignited the debate on the security of our energy systems, it is crucial to understand the significant impact of the introduction of digital technologies and the digital revolution within the energy transition.

1.1. Introduction to the Energy Transition

1.1.1. Climate change mitigation and adaptation

Modern energy consumption has been an undeniable cause behind climate change. In particular, the use of fossil fuels is a major contributor to the dramatic increase of Co2 levels: global greenhouse emissions account for over 75% of the latter, and carbon dioxide emissions are nearly 90% attributed to fossil fuels[10].

[10] Mohammad Fazle Rabbi, József Popp, Domician Máté, and Sándor Kovács, "Energy Security and Energy Transition to Achieve Carbon Neutrality", *Energies* 15, no. 21 (October 2022), https://doi.org/10.3390/en15218126

Fossil fuels - namely oil, coal, and natural gas, are non-renewable resources that in the long term will be exhausted. They have been used, in the present Anthropocene epoch, as the primary energy source[11]. Their use by mankind became common practice by 1860, and could continue, because there were no global shortages of cheap fossil fuels in their various forms[12]. In fact, fuel reserves were more than adequate to meet projected energy demand growth, though their exploration required large investments in production and in transportation infrastructure[13].

It was only in the mid 1980s that it was acknowledged that the enormous amounts of Co2 released into the atmosphere were causing global warming[14] . Ever since, climate policies have gained impetus worldwide, through several States and international legislation, as well as international conferences aiming to address climate change[15]. To name a few, the 2015 Paris Agreement, the international treaty aimed at limiting global warming to below 2 degrees Celsius, the 1997 Kyoto Protocol, that commits state parties to reduce greenhouse gas emissions, the 1992 United Nations Framework Convention on Climate Change, and the 2019 European Green Deal, promoted by the Von Der Leyen Commission, which envisions an energy system serving climate neutrality[16].

Mitigating climate change is a security priority, as climate security has been recognized as one of the contemporary world's *complex crises,* both social and environmental[17], and an issue our

---

[11] Vincenzo Balzani, "Saving the planet and the human society: renewable energy, circular economy, sobriety", *Substantia: An International Journal of the History of Chemistry* 3, no. 2 (2019), https://doi.org/10.13128/Substantia-696

[12] Ralph E.H. Sims, "Can Energy Technologies Provide Energy Security and Climate Change Mitigation?", *Energy and Environmental Challenges to Security* (2009), https://doi.org/10.1007/978-1-4020-9453-8_19

[13] IEA, *Energy and Climate Change. World Energy Outlook Special Report* (2015), https://www.iea.org/reports/energy-and-climate-change

[14] Vincenzo Balzani, "Saving the planet and the human society: renewable energy, circular economy, sobriety".

[15] Ibid.

[16] Marco Giuli, "Bringing Paris into the EU'S Energy Infrastructure Policy: What Future for Gas?", *IAI Commentaries* (2020), https://www.iai.it/it/pubblicazioni/bringing-paris-eus-energy-infrastructure-policy-what-future-gas

[17] Vincenzo Balzani, "Saving the planet and the human society: renewable energy, circular economy, sobriety".

society, industries and states must address. As reiterated by UN initiatives, climate change is imitated to have global security impacts from livelihoods and health to extreme weather conditions, such as drought, waves, floods, and landslides, and heavy rains, which are already becoming prevalent worldwide[18] Other significantly drastic outcomes include biodiversity losses, rising levels and ocean acidification.

Most importantly, as global energy consumption is estimated to increase by about 80% by 2030[19], several countries are seeking new alternatives for new energy sources, to reduce emissions and pursue the goal of carbon neutrality.

The increasing frequency of extreme weather, changes in average temperature, and shifts in the seasons require immediate adaptation efforts. According to the United Nations Framework Convention on Climate Change (1992), the longer these latter are put off and the more expensive and difficult responding to climate change will become[20].

Adaptation pertains to adjustments in ecological, social, or economic systems in response to actual or expected climatic stimuli: this entails changes in processes, practices, and structures to moderate potential damages and even benefit from opportunities associated with climate change. Responding to future climate change impacts therefore pushes countries and communities to develop precise adaptation solutions and implement specific action[21].

In such a two-pronged approach, responding to climate change involves mitigation - concretely the reduction of emissions, and adaptation[22]. There exist various adaptation strategies or options

---

[18] Mohammad Fazle Rabbi, József Popp, Dominicián Máté Sándor Kovács, "Energy Security and Energy Transition to Achieve Carbon Neutrality", *Energies* 15, no. 2 (2022), https://doi.org/10.3390/en15218126

[19] Ibid.

[20] United Nations, United Nations Framework Convention on Climate Change. Concluded at New York on 9 May 1992, https://treaties.un.org/doc/source/RecentTexts/unfccc_eng.pdf

[21] Ibid.

[22] NASA Science, "Responding to Climate Change". Accessed on August 17th, 2024, https://science.nasa.gov/climate-change/adaptation-mitigation/

that can concretely help manage impacts and risks to people and nature and are essential of four types: infrastructural, institutional, behavioral, and nature-based[23] .

The EU strategy on adaptation to climate for instance, was adopted by the European Commission on 24 February 2021, setting out how the European Union can adapt to the unavoidable impacts of climate change, and become climate resilient by 2050. Four principal objectives appear in the strategy - to make adaptation smarter more systemic, and to step up international action on adaptation to climate change[24].

In this context, the energy transition, defined, in its most simplistic form, as the shift from fossil fuels to renewable energy sources, emerges as a necessary pathway to effectively combat climate change and achieve carbon neutrality, whilst ensuring a sustainable future for the next generation with enough energy to meet its needs[25].

1.1.2. Energy Security

Combating climate change is not the sole reason driving this transition, and the benefit it brings. In fact, as mentioned previously, due to energy's paramount importance for economic stability, national security, and societal well-being, energy security is a critical challenge[26].

The nature of energy security is polysemous and multi-dimensional[27], as a consensus on a widely accepted definition still needs to be developed; the scope of energy security has expanded, and as

---

[23] Udayan Singh and Samarth Singh, "Future research directions to facilitate climate action and energy transitions", *Energy and Climate Change* 4 (December 2023), https://doi.org/10.1016/j.egycc.2022.100092

[24] European Commission, "EU Adaptation Strategy". Accessed on August 17th, 2024, https://climate.ec.europa.eu/eu-action/adaptation-climate-change/eu-adaptation-strategy_en#:~:text=The%20European%20Commission%20adopted%20its,become%20climate%20resilient%20by%202050.

[25] Mohammad Fazle Rabbi, József Popp, Dominician Máté Sándor Kovács, "Energy Security and Energy Transition to Achieve Carbon Neutrality".

[26] Aleh Cherp and Jessica Jewell, "The concept of energy security: Beyond the four As", *Energy Policy* 75 (December 2014), https://doi.org/10.1016/j.enpol.2014.09.005

[27] B.W. Ang and T.S. Ng, "Energy security: Definitions, dimensions and indexes", *Renewable and Sustainable Energy Reviews* 42, (February 2015), https://doi.org/10.1016/j.rser.2014.10.064

a result, from their classical beginnings following the 1980 oil crisis, energy security studies now include different energy sectors, and diverse issues. Based on the traditional approach of energy security intended as the "four As" (availability, affordability, and acceptability), energy security is defined as the interrupted availability of energy sources at an affordable price. The current energy systems largely relying on fossil fuels have inherent vulnerabilities and limitations which can be addressed through the energy transition. Fossil fuels reserves are geographically concentrated, leading to geopolitical tensions, and market volatility, as shown by the 190s oil crisis but equally, by the Russia-Ukraine war which has exacerbated the European Union's dependency on natural gas[28].

Energy security is deeply linked to geopolitical influence and control; currently, more than half of the energy consumed in Europe is imported, which can be seen, above all, in fossil fuels. In 2019, 90% of all the oil and 69% of all the natural gas consumed was imported[29]. The EU had expressed some concern in this regard due to the possibility of disruptions in the supply of these products, due to both infrastructure failure, political or trade disputes.

Energy-rich countries, particularly, those with significant reserves of fossil fuels exert political influence as they use their energy resources as leverage in international relations, conflict negotiations and diplomacy, affecting global stability and regional dynamics. The geopolitics of oil and gas are alive and well[30].

The shock of the Russia-Ukraine war was a jolting revelation for Europe as European countries realized the stable flow of affordable energy was no longer a given, sparking what has been defined as an *energy panic,* as securing affordable heating for homes rapidly became the number one

---

[28] Ibid.

[29] Jason Bordoff and Meghan L. O' Sullivan, "Green Upheaval", *Foreign Affairs* 101, no. 1 (November 2021), https://www.foreignaffairs.com/articles/world/2021-11-30/geopolitics-energy-green-upheaval

[30] Ibid.

political priority[31]. If successful, green energy technologies may leave Europe significantly less reliant on energy imports than it has been since 1945. That said, such success depends upon the political choices that will be pursued in the coming years, on policy efforts to attract investment and to promote sustainable green energy industries on the continent[32].

Renewable energy sources are vastly "indigenous" and can be found across the planet. Countries with abundant renewable resources can generate a significant portion of their electricity domestically, reducing exploration to trade disputes and geopolitical tensions related to imports. Investing in renewable energy reduces reliance on imported fuels by enabling countries to strengthen their energy security and achieve greater energy independence[33].

Appropriate deployment of renewable energy systems can thus help improve the security of energy supply for electricity, cooling and heating and transport fuels; diversifying the energy mix reduces risks associated with over-reliance on any single energy resource if faced with supply disruptions due to geopolitical issues, natural disasters, or other factors. Diversification through other sources, renewables in particular, help meet demand and stabilize energy availability[34].

1.1.3. Economic growth and innovation

There are multiple avenues through which the shift towards sustainable practices is entailing economic growth and innovation. Emerging industries are being forged as well as markets focused on renewable energy, energy efficiency, sustainable agriculture, waste management and clean transportation; overall, these sectors foster opportunities for investment catalyzing economic growth[35] .

---

[31] Thijs Van de Graaf and Hans Kribbe, *Energy diplomacy: Europe's new strategic mission*, Brussels Institute for Geopolitics (March 2024), https://big-europe.eu/publications/big003-energy-diplomacy

[32] Ibid.

[33] International Renewable Energy Agency (IRENA), *A New World: The Geopolitics of the Energy Transition* (2019), https://www.irena.org/publications/2019/Jan/A-New-World-The-Geopolitics-of-the-Energy-Transformation

[34] Ibid.

[35] ILO, Green jobs, green economy, just transition and related concept: A review of definitions developed through intergovernmental processes and international organizations.

Bloomberg New Energy Finance (NEF) reported that global clean energy investments jumped 17%, hitting 1.8$ trillion in 2023. The increase in clean energy investments highlights strong investor enthusiasm and financial commitment to renewable energy and other clean technologies[36].

The International Labor Organization (ILO) has additionally re-iterated how investment in renewable energy generates jobs, each distinct renewable energy source creates distinct economic opportunities. For the solar energy industry, for instance, jobs in the installation and maintenance of photo-voltaic panels on residential, commercial, and industrial buildings are required; large-scale solar farms provide opportunities for construction and maintenance jobs, and developing Concentrated Solar Power for large-scale electricity generation involves engineering, construction, and ongoing operational roles. In the hydropower sector, plant construction involves civil engineering, construction, and project management roles, the same goes for the other renewable sectors as geothermal, wind, and bioenergy[37]. Occupations in selected renewable energy sub.-sectors vary by value chain, which has four major elements (equipment manufacture and distribution, project development, construction and installation, and operations and maintenance).

The Green Jobs Report[38] (2008) provides a forecast for employment in renewable energy sectors by 2030, assuming strong policy support. The biofuels have an employment potential of up to 12 million people, up to 2.1 million people could work in wind energy, and up to 6.3 million people could be employed in solar PV.

Data published by the International Renewable Energy Agency additionally highlights the increasing importance of renewable energy in the global job market: in 2022, the global renewable energy sector employed 13.7 million people, up from 12.7 million in 2021. Asia is the leading region, with nearly two-thirds of all renewable energy jobs, and China alone accounting for 41% of the global total. Solar photovoltaic (PV) is the fastest-growing sector, providing 4.9 million jobs, with women holding 40% of these positions. Hydropower employs 2.5 million people, with

[36] Ibid.

[37] Ibid.

[38] Ibid.

the majority working in operation and maintenance. Biofuels also account for 2.5 million jobs, primarily in agriculture. Wind power employs 1.4 million people, with China and Europe leading the way. This growth highlights the increasing importance of renewable energy in the global job market[39].

1.1.4. The Green Transition as a Prerequisite for Sustainable Development

It has been generally recognized that policies promoting sustainable energy directly contribute to broader sustainable development goals, from poverty reduction, environmental conservation, and social equity. The energy transition embodies a significant opportunity to improve public services, production, and transport systems[40].

Benefits have also been observed from renewable projects that aim to empower local populations, notably community renewable energy (CRE), ranging from an increase in social cohesion, jobs, services, knowledge, and skills.

As reiterated by the International Energy Agency, the green transition is an opportunity to address existing socio-economic inequalities. Following the IEA, several international instances are focusing to place people and inclusivity at the center of all clean energy transitions, recognizing the former as crucial for effective energy and climate policies. The approach that is being advocated is one that includes the voices of economic vulnerable groups in the design of clean energy policies to ensure access to clean energy is equitable, just, and addressing the needs and concerns of society[41].

A 2021 United Nations report restated the interlinkages that exist between energy and other sustainable development goals, from poverty, zero hunger, education, infrastructure innovation

---

[39] IRENA, *Renewable energy, and jobs: Annual review 2023* (September 2023), https://www.irena.org/Publications/2023/Sep/Renewable-energy-and-jobs-Annual-review-2023

[40] Ibid.

[41] International Energy Agency (IEA), OECD, *World Energy Outlook* (2023), https://www.oecd-ilibrary.org/energy/world-energy-outlook-2023_827374a6-en

and gender equality: energy is essential to all SDGs[42]. To name few examples, investments in technologies and processes improving energy efficiency are expected to substantially reduce energy-related water use. Renewable energy and sustainable bioenergy have the potential to become a key component of the whole production chain of food, from harvesting, processing, expanding food life as well as transportation[43].

However, ensuring sustainability results entails a consideration of the existing and possibly existing asymmetries of some countries' commitment to the energy transition, as well as the risks posed by such asymmetries.

A starting point is for instance geopolitical risks that are carried by delivering sustainable change at this scale and within this required time frames. These could affect governments and businesses which strategic planning and decision making are not routinely accounted for. Geopolitical risks include a rebalancing of power among oil-producing states, favoring those who can produce cheaper lower-carbon oil, an increase in leverage for states in the Global South that have large deposits of critical minerals, and growing cracks between the haves and haves not over financing a clean energy transition[44].

Taking the example of China's energy and environmental policies, the country's general direction has been confusing. The commitment to peak carbon emissions before 2030 has been contrasted by China's increasing coal production. China's position at COP28 was also circumspect[45].
Oil and gas production are becoming more concentrated in a smaller number of states because of the decline for fossil fuels; in this case the most dominant suppliers concentrated in a smaller

---

[42] United Nations, Division for Sustainable Development Goals Department of Economic and Social Affairs, *Leveraging Energy Action for Advancing the Sustainable Development* (2021), https://sdgs.un.org/sites/default/files/2021-06/2021-POLICY%20BRIEFS_3.pdf

[43] Ibid.

[44] Matt Ince and Erin Sikorsky, "The Uncomfortable Geopolitics of the Clean Energy Transition", Lawfare, December 13th, 2023, https://www.lawfaremedia.org/article/the-uncomfortable-geopolitics-of-the-clean-energy-transition

[45] Anders Hove, Michal Meidan, and Philip Andrews-Speed, "Software versus hardware: How China's institutional setting helps and hinders the clean energy transition", *OIES Paper: CE No. 2,* The Oxford Institute for Energy Studies, Oxford (2021), https://www.econstor.eu/handle/10419/253276

number of states are seeing their market shares increase. Such a situation will see states such as Such araba provide an even greater share of the oil consumed globally in the medium term. Riyadh currently accounts for 13 percent of global oil production. The consequences would entail the country gaining increased influence[46].

Fossil-fuel producing States in Sub-Saharan Africa including Angola, Chad, Gabon, Nigeria, and Sudan are expected to experience annual average revenue shortfalls over the next two decades in a low-carbon scenario, ranging from 69 percent in Nigeria for instance to 87 percent in Sudan, compared to the five-year period from 2015 to 2019[47].

From a security point of view this has created predictions for increased volatility for the coup-prone region, where more than a dozen conflicts are ongoing[48].

Moreover, with the shift in global energy supply and demand dynamics progressing, appetite for critical minerals is also expected to arise at the top of the long list of minerals mostly considered essential for the energy transitions are cobalt, graphite, lithium, nickel, and rare earth elements - each a vital enable for most renewable energy technologies[49]

A further risk concerns that of "unwanted dependencies": China currently dominates the downstream refining process for cobalt, lithium, graphite, and rare earths. Reports indicate that China is already using its dominance within various critical mineral supply chains, to exert economic pressure on other countries. Scholars have suggested the likelihood of Beijing to make such moves with other minerals as a wider competition strategy with the U.S. identifies[50]. In October 2023, China's commerce ministry announced plans to introduce new export controls on

---

[46] Matt Ince and Erin Sikorsky, "The Uncomfortable Geopolitics of the Clean Energy Transition", Lawfare, December 13th, 2023, https://www.lawfaremedia.org/article/the-uncomfortable-geopolitics-of-the-clean-energy-transition

[47] Ibid.

[48] Ibid.

[49] Ibid.

[50] Ibid.

graphite on national security grounds. In July, it had already decided on impositions of similar export controls; on important semiconductor materials such as gallium, and germanium-risks. This move undermined the ability of non-Chinese manufacturers to meet growing demand for electric vehicles[51].

Thus, a multifaceted array of reasons and factors extending well beyond mere decarbonization are driving the energy transition today, driver that underscore the importance of a sustainable energy system that aligns with the broader goals of security and sustainable development.

However, the path to a sustainable energy future is fraught with challenges, including geopolitical risks. The transition can shift the balance of power among oil-producing states, increase the leverage of states with large deposits of critical minerals, and exacerbate financial divides between nations capable of funding the clean energy transition and those that cannot.

1.2. Digitalization & Decentralization

A study of the changing landscape of critical energy infrastructure entails an exploration of two of the most important foundational pillars of the energy transition, that is, digitalization and decentralization.

Digitalization in the energy sector entails the integration of digital technologies, from advanced analytics, Internet of Things (IoT) devices, artificial intelligence, and smart grid technologies. This transformative process is not only transforming how energy is generated, distributed, and consumed, optimizing operational efficiencies, it is equally facilitating the seamless integration of renewable energy sources[52].

---

[51] Anders Hove, *Clean energy innovation in China: fact and fiction, and implications for the future,* The Oxford Institute for Energy Studies (July 2024), https://www.oxfordenergy.org/wpcms/wp-content/uploads/2024/07/CE14-Clean-energy-innovation-in-China-Final.pdf

[52] Sanghita Baidya, Vidyasagar Potdar, Partha Pratim Ray, Champa Nandi, "Reviewing the opportunities, challenges and future directions for the digitalization of energy", *Energy Research & Social Science* 81 (2021), https://doi.org/10.1016/j.erss.2021.102243

Decentralized energy systems refer to the shifting from centralized energy generation, and distribution systems, towards more distributed and localized sources of energy production; as such, it is characterized by positioning energy production facilities closer to the site of energy consumption, allowing for more optimal use of renewable energy. A decentralized energy system allows for more optimal use of renewable energy as well as combined heat and power, reduces fossil fuel use and increases eco-efficiency[53]. Decentralized energy systems are controlled by multiple independent entities, as homes, organizations, and communities, rather than being controlled by a single authority such as a grid control center [54].

Both decentralized systems and digitalization are significant forces driving the transformation of critical energy infrastructure.

1.2.1. Digitalization

i. Smart Grids

Smart grids are no novelty, rather, they came about as an answer to a need to modernize the electricity grid and improve the delivery of power[55].

As the global electricity sector is currently facing its transition towards utilizing renewable energy sources to meet electricity demands, it must overcome challenges. Smart grids enable better integration of various sources of electricity generation, including renewable energy sources, such as wind, solar, hydro, and geothermal[56].

---

[53] ESCAP, "Smart Cities in Southeast Asia: A Landscape Review" (2022), https://www.zotero.org/yasminadionisi/search/escap/titleCreatorYear/items/E8WZ6ZVR/item-details

[54] Zoya Pourmirza, *Cybersecurity in Centralised vs Decentralised Energy Systems,* Supergen Energy Networks (2023), https://www.ncl.ac.uk/media/wwwnclacuk/supergenenergynetwork/files/Cyber%20Security%20in%20Centralised%20vs%20Decentralised%20Energy%20Systems%20(2).pdf

[55] Maria Lorena Tuballa and Michael Lochinvar Abundo, "A review of the development of Smart grid technologies", *Renewable and Sustainable Energy Reviews* 59 (2016), https://doi.org/10.1016/j.rser.2016.01.011

[56] Mohammed Khalid, "Smart grid and renewable energy systems: Perspectives and grid integration challenges", *Enrgy Strategy Reviews* 51 (2024), https://doi.org/10.1016/j.esr.2024.101299

The Smart Grid does not have one definition that is universally accepted. According to the Strategic Deployment Document for Europe's Electricity Networks of the Future, a Smart Grid is an electricity network that can intelligently integrate the actions of all users connected to it - generators and consumers alike. The Korean Smart Grid Roadmap 2030 defines the Smart Grid as a next-generation network that integrates information technology into the existing power grid to optimize energy efficiency, through a two-way exchange of electricity information, between suppliers and consumers in real time. Yet another definition is provided by the National Institute of Standards and Technology (NIST), according to which the Smart Grid is a grid system, integrating many varieties of digital computing and communication technologies and services, into the power system infrastructure[57].

A Smart Grid functions through the integration of advanced digital communications, control, and automation technologies throughout the electricity generation, transmission, distribution, and consumption processes[58]. Concretely speaking, Smart Grids puts information and communication technology (ICT) at the center of modernizing energy systems.

The following grid representation illustrates the integration of energy generation assets (notably those of renewable generation sources; wind, solar and hydro power plants; nuclear power plants and traditional power plants producing electricity), energy transmission assets, such as the high-voltage power lines, and electricity consumers, such as factories and industrial facilities, cities and buildings., and electric vehicles, which fall under the category of emerging load or flexible demand resources[59].

---

[57] Maria Lorena Tuballa and Michael Lochinvar Abundo, "A review of the development of Smart grid technologies", *Renewable and Sustainable Energy Reviews* 59 (2016), https://doi.org/10.1016/j.rser.2016.01.011

[58] Mohammed Khalid, "Smart grid and renewable energy systems: Perspectives and grid integration challenges", *Enrgy Strategy Reviews* 51 (2024), https://doi.org/10.1016/j.esr.2024.101299

[59] Iberdrola, "Smart grids, intelligent electricity networks". Accessed August 21st, 2024, https://www.iberdrola.com/about-us/what-we-do/smart-grids#:~:text=The%20traditional%20electricity%20grid%20is,increasing%20efficiency%20and%20energy%20savings.

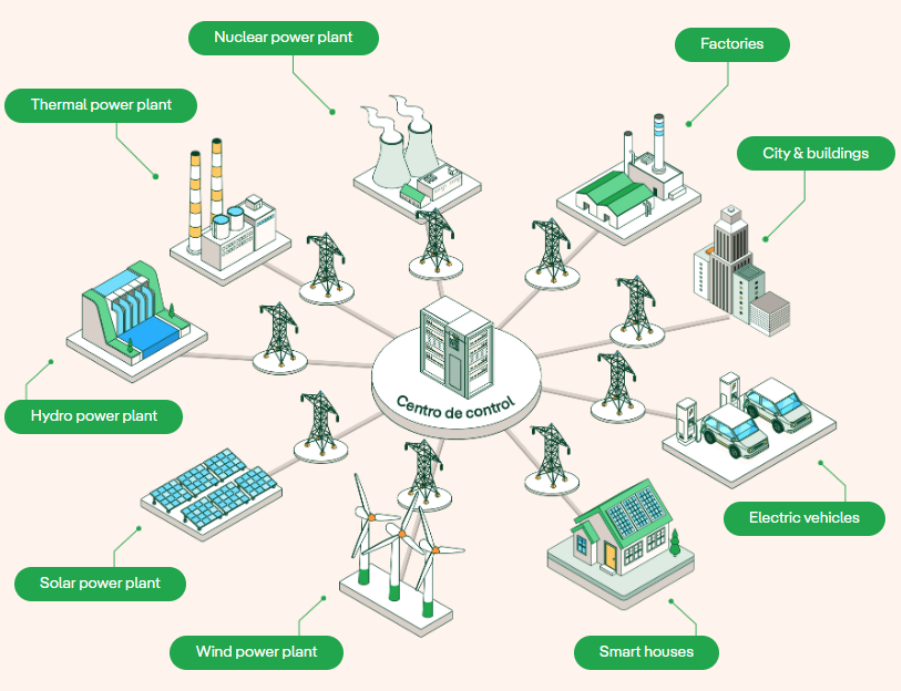


Figure 1: What differentiates smart grids from electricity grids. Source: Iberdrola, 2024.

What characterizes the architecture of a smart grid is its interconnectedness, through key assets, starting from advanced technologies. Cloud computing - the technology that allows users to access and store data, utilize computing power, and run applications over the internet - rather than relying on local servers - has become an essential component for Internet services. Cloud infrastructures are widely distributed and spread cross wide areas, interconnected through different networks, and powered by diverse energy source and providers[60] .

A conceptualization of an "ecosystem" based on these elements, would entail a hybrid Smart Grid Cloud that would be used primarily for energy data management, reporting, and analytics, in which services are provided to stakeholders, such as State Governments, Local Governments and Utilities, through a web-based environment[61].

[60] Laurent Lefèvre and Anne-Cécile Orgerie, "Designing and evaluating an energy efficient Cloud", *The Journal of Supercomputing* 51 (2010), https://doi.org/10.1007/s11227-010-0414-2

[61] Branko Primetica and Joe Helfrich, "Enabling the SmartGrid through Cloud Computing", EGlobal Tech (2012), https://www.energy.gov/sites/prod/files/Friday_Trinity_Ballroom_3_0855_Primetica_final.pdf

Thus, the Smart Grid is an electricity network that intelligently integrates the actions of all users connected to, from generators and consumers, to efficiently deliver sustainable, economic, and secure energy supplies[62]

ii. The Internet of Things (IoT)'s Applications in the Energy Sector

The concept of the Internet of Things (IoT) first emerged in 1999, however, the exact definition is still in its forming process[63]. Generally defined as an inter-connected, worldwide network, based on sensory, communication, networking, and information processing technologies. Intelligent sensing and wireless communication techniques have become part of the IoT[64].

As an emerging technology using the Internet, the IoT's aim is to provide connectivity between physical devices, or "things"[65]. As such, examples of physical devices encompass smart home devices, wearable technologies, personal medical devices, autonomous vehicles.

In the energy and power sector, automating industrial processes and supervisory control, as well as data acquisition systems, became popular in the power sector in the 1990s[66]. Today, IoT offers a wide number of applications in supply, transmission, distribution, and demand.

One of the major applications concerns smart meters. As advanced devices that measure and record electricity consumption in real-time, smart meters represent a key element in the infrastructure of

---

[62] Maria Lorena Tuballa and Michael Lochinvar Abundo, "A review of the development of Smart grid technologies", *Renewable and Sustainable Energy Reviews* 59 (2016), https://doi.org/10.1016/j.rser.2016.01.011

[63] Shancang Li and Li Da Xu, "The internet of things: a survey", *Information Systems Frontiers* 17, no. 2 (2015), https://doi.org/10.1007/s10796-014-9492-7

[64] Ibid.

[65] Naser Hossein Motlagh, Mahsa Mohammadrezaei, Julian Hunt, and Benham Zaker, "Internet of Things (IoT) and the Energy Sector", *Energies* 13, no. 2 (2020), https://doi.org/10.3390/en13020494

[66] Ibid.

the energy transition. Smart meters are integrated into the smart grid - in which they are the most important device - to optimize generation, and its eventual distribution and consumption[67].

Traditional power grids function by transmitting electrical power from a few central generation stations to numerous load centers, where electricity is consumed. The smart grid allows unconventional power flow and two-way information flow to create an advanced automatic and distributed energy delivery network. Within this network, smart meters collect information from the end users' load devices and measure the consumption of the consumers. They then provided added information to the utility company or system operator for better monitoring[68] .

Smart meters measure electrical data such as voltage and frequently and record real-time energy consumption information, thus supporting bidirectional communications between the meter and the central system. Data information is transmitted through the Local Area Network (LAN), to the data collector; a transmission process which can be executed every fifteen minutes, or as infrequently as once a day, based on the requirement of the data demand. When the data is retrieved by the collector, it is transmitted to the utility collection points which process it by using the Wide Area Network (WAN). Thus, the communications path is two-way with signals and comments being directly sent through the meters[69].

Another use of the Internet of things concerns the vehicle to grid (V2G) technology, for instance, which transfers the electric powers efficiently, encouraging two-way communication of electrical energy between electric vehicles and electrical power networks[70].

---

[67] Repsol, "What are smart or digital meters?", 11 September 2023, https://www.repsol.com/en/energy-and-the-future/technology-and-innovation/smart-meters/index.cshtml

[68] Jixuan Zheng and Lin Li, "Smart Meters in Smart Grid: An Overview", *IEEE Green Technologies Conference* (2013), https://ieeexplore.ieee.org/document/6520030

[69] Ibid.

[70] Michelle Hampson, "Yes, Your Electric Vehicle Could Be Hacked", IEEE Spectrum, August 24th. 2023, https://spectrum.ieee.org/ev-hacks

iii. Artificial Intelligence in Energy Management

The concept of artificial intelligence (AI) and machine learning (ML) emerged in the twentieth century with the aim to enable computers to simulate humans' learning and decision-making capabilities. Computer scientist John McCarthy was the first to use "Artificial Intelligence" defining it as computers' ability to mimic the cognitive functions of humans.[71]

Being an area of vast and expanding nature, AI is penetrating all scientific fields, currently being employed in banking, agriculture, healthcare, marketing, security, manufacturing. Applications of AI in energy systems have gained more focus in recent years[72].

AI is being instrumental in infrastructure operational awareness, helping system operators to identify key information in real time, in the face of the flood of data by modern energy infrastructure. Operators are given the awareness and context they need to respond[73].

A groundbreaking transformation is also given by the promise of AI's ability to control system operations at machine speed; by directly controlling infrastructure operations (AI-directed), or directly providing decision support to human operators (AI-assisted, with human-in-the-loop), with various levels of human involvement[74].

Machine learning, a specific branch of artificial intelligence, has been widely used in the modeling, design, and prediction of energy systems[75]Machine learning control techniques are being

---

[71] Ashkan Entezari, Alireza Aslani, Rahim Zahedi, Younes Noorollahi, "Artificial intelligence and maching learning in energy sysems: A bibliographic perspective", *Energy Strategy Reviews* 45 (2023), https://doi.org/10.1016/j.esr.2022.101017

[72] Ibid.

[73] US Department of Energy – Office of Cybersecurity, Energy Security, and Emergency Response (CESER), *Potential Benefits and Risks of Artificial Intelligence for Critical Energy Infrastructure* (April 2024), https://www.energy.gov/sites/default/files/2024-04/DOE%20CESER_EO14110-AI%20Report%20Summary_4-26-24.pdf

[74] Ibid.

[75] Amir Mosavi et. al, "State of the Art of Machine Learning Models in Energy Systems, a Systematic Review", *Energies 12,* no. 7 (2019), https://doi.org/10.3390/en12071301

employed on smart grids that combine photovoltaic-based power systems and other renewable energies.

As an illustrated, in a solar farm with 500 PV experiencing periodic efficiency drops, and unexpected failures, an ML-based predictive maintenance and fault detection system would collect and process data - of over several years, including maintenance records and weather conditions, sending alerts to the maintenance team, specifying the type of fault and recommended actions Hence, not only are the reliability and efficiency of PV installations improved, but the operational costs are also reduced, and the overall return on investment[76].

1.2.2. Decentralization

Based on the definitions surveyed in their paper[77], define distributed generation as a small source of electric power generation or storage (typically ranging from less than a kW to tens of MW) that is not a part of a large central power system and is located close to the load. These authors also include storage facilities in the definition of distributed generation, which is not conventional. Furthermore, their definition emphasizes the relatively small scale of the generation units as opposed to CIRED and CIGRE.

Decentralized energy is a concept that is changing the approaches to energy production. Concretely speaking, decentralization refers to the reorganization of a single, concentrated, energy-generation facility, into smaller, more autonomous energy generation units. The latter are largely separated, yet highly interconnected[78].

Yet another term lacking a universal and commonly accepted definition, with definitions shifting in relation to the context, decentralization is commonly presented as a counterpoint to

---

[76] Jorge Felipe Gaviria, Gabriel Narváez, Camillo Guillen, Luis Felipe Giraldo, Michael Bressan, "Machine learning in photovoltaic systems: A review", *Renewable Energy* 196, https://doi.org/10.1016/j.renene.2022.06.105

[77] E. Judson et. al, "The centre cannot (always) hold: Examining pathways towards energy system de-centralisation", *Renewable and Sustainable Energy Reviews* 118 (2020), https://doi.org/10.1016/j.rser.2019.109499

[78] Ibid.

centralization energy as the differentiation is represented by the fact decentralized energy production occurs closer to points of consumption[79].

The terms 'decentralized' and 'distributed' are interchangeably used in the relevant literature, both grey and academic[80].An example of distributed generation concerns many small sources of electric power generation or storage facilities[81], where electricity travels a much shorter distance from point of production to point of consumption, specifically sites of electricity use[82]. Rooftop solar panels, electric vehicles and battery storage are examples of the small-scale energy[83]

The International Energy Agency has additionally confirmed that their rapid expansion is transforming not only the way electricity is generated, but also how it is traded, delivered, and consumed[84] .

As such, electricity production is no longer limited to large and centralized generators and retailers, but rather, consumers are given the opportunity to be more proactive. New players, such as aggregators, who pool together small-scale resources, and act on their owners' behalf, are entering power markets[85]. Electricity can be produced by consumers, for their own consumption, or to be sold on the market.

---

[79] Ibid.

[80] Junjan Qi and Adam Hahn, and Cheng-Chiang Liu," Cybersecurity for distributed energy resources and smart inverters", *IET Cyber-Physical Systems: Theory & Applications* 1, no. 1 (2016), https://doi.org/10.1049/iet-cps.2016.0018

[81] Ibid.

[82] E. Judson et. al, "The centre cannot (always) hold: Examining pathways towards energy system de-centralisation", *Renewable and Sustainable Energy Reviews* 118 (2020), https://doi.org/10.1016/j.rser.2019.109499

[83] International Energy Agency, *Unlocking the Potential of Distributed Energy Resources – Analysis* (2022), https://www.iea.org/reports/unlocking-the-potential-of-distributed-energy-resources

[84] Ibid.

[85] Ibid.

Ultimately, what is created are bidirectional electricity flows in which consumers are increasingly able to take control of their own energy demand, through a complex web of interactive smart devices, promoting energy efficiency and sustainability[86].

Another transformation in critical energy infrastructure is unfolding with Energy Communities, intended as citizen-driven energy actions which through collective actions are advancing energy efficiency within their local communities[87].
Energy communities are supported by actors, which may be a natural person or household, an institution as a school or university, a non-governmental organization, a business - whose primary area of economic activity is not energy-related, a local authority, etc.[88].

1.3 The Critical Infrastructure of the Energy Transition: A State of the Art

Insights reveal that the current pace of renewable deployment showcases significant opportunities for growth. Yet, while growing rapidly, renewables still account for a small sliver of the overall global energy mix, with significant disparities across regions and markets.

1.3.1. The Geography of Green Critical Infrastructure

Despite its strong momentum, near-term exigencies recently challenged the energy transition, starting from the COVID-19 pandemic which entailed affordability challenges, shortages, and blackouts in different parts of the world, along which supply chain constraints[89].

---

[86] Ibid.

[87] European Commission, "Energy communities". Accessed August 21st, 2024, https://energy.ec.europa.eu/topics/markets-and-consumers/energy-consumers-and-prosumers/energy-communities_en#:~:text=Energy%20communities%20allow%20local%20communities,field%20with%20other%20market%20actors.

[88] Vladimir Z. Gjorgievski et. al, "Energy sharing in European renewable energy communities: Impact of regulated charges", *Energy* 281 (2023), https://doi.org/10.1016/j.energy.2023.128333

[89] Muqsit Ashraf and Roberto Bocca, "Fostering Effective Energy Transition: 2023 Edition", World Economic Forum (June 2023), https://www3.weforum.org/docs/WEF_Fostering_Effective_Energy_Transition_2023.pdf

Nevertheless, several countries are also leading the way in the energy transition with significant investments and innovative strategies in their green infrastructure, and some efforts and projects are worth a mention.

The country that is leading the way in the energy transition is China, whose solar and wind power generation are outpacing that of any other country[90]. As suppliers of equipment for more than half of all newly installed wind power capacity globally in 2022 and representing more than 80% of the world's solar panel manufacturing capacity, Chinese firms have been dominating the international market for renewable infrastructure. Moreover, the country has become a leading producer and exporter of electric vehicles and electric battery manufacturing, with firms such as BYD, recently overtaking Tesla to become the world's biggest-selling EV makers. Its electric vehicles shipment was up by over 300% to the European Union, from 2021.

China additionally hosts the world's largest hydro-solar power station in Tibet, the Kela solar power plant, planned, by the Chinese government, to generate energy for 100 million households, operating since 2023[91].

Concerning the green transition in Europe, several institutions have elaborated benchmarks assessing states on their energy system performance and measuring their transition readiness.

Among these, the World Economic Forum annual Energy Transition Index (ETI). The global ETI improved by 10%, supported by an increase of 19% in transition readiness scores, and a 6% increase in system performance scores. The countries scoring highly on both system performance and transition readiness were the Nordic countries as Sweden, Denmark, Norway, and Finland[92]

---

[90] Lombard Odier, "The countries leading the energy transition". Accessed July 12, 2024, https://www.lombardodier.com/contents/corporate-news/responsible-capital/2024/april/picking-the-winners-in-the-energ.html

[91] International Hydropower Association, "World's largest hydro-PV station now operating in China World's largest hydro-PV station now operating in China", July 28, 2023, https://www.hydropower.org/news/worlds-largest-hydro-pv-station-now-operating-in-china

[92] Muqsit Ashraf and Roberto Bocca, "Fostering Effective Energy Transition: 2023 Edition", World Economic Forum (June 2023), https://www3.weforum.org/docs/WEF_Fostering_Effective_Energy_Transition_2023.pdf

Worldwide efforts are being driven by countries notably in the digitalization of energy. In addition to China and the Scandinavian countries, other States as Germany, the UK, the United States, the Netherlands, Australia, and Japan, among others, are integrating advanced technologies digital technologies in their energy optimization facilities.

For instance, the German Federal Ministry of Economics and Technology, in an inter-ministerial partnership with the Federal Ministry for the Environment, Nature Conservation and Nuclear Safety, funds E-Energy, defined as the "ICT-based Energy System of the Future". E-Energy stands for Smart Grids made in Germany (German Federal Ministry of Economics and Technology, 2008). Furthermore, along with Netherlands, the country developed the Tennet project to incorporate blockchain for managing the electricity grid and pave the way for decentralized flexible energy sources[93]. France also began its nationwide smart meter rollout (Linky), which oversaw the deployment of 28 million smart meters by 2021[94].

A comprehensive overview of the state of smart grids in Europe is provided, every year, by the European Commission's Joint Research Center in the annual report "Clean Energy Technology Observatory: Smart Grids in the European Union - Status Report on Technology Development Trends, Value Chains and Markets". The 2023 report provided relevant data on smart meters, showcasing the various wide scale smart meter installations, in both Europe and the world. The following figure is illustrative of the smart meter worldwide situation:

[93] Tennet, "TenneT unlocks distributed flexibility via blockchain", May 2, 2017, https://netztransparenz.tennet.eu/tinyurl-storage/detail/tennet-unlocks-distributed-flexibility-via-blockchain/

[94] Smart Energy International, "A guide to France's Linky smart meter", December 27, 2018, https://www.smart-energy.com/features-analysis/smart-meters-101-frances-linky-electricity-meters/

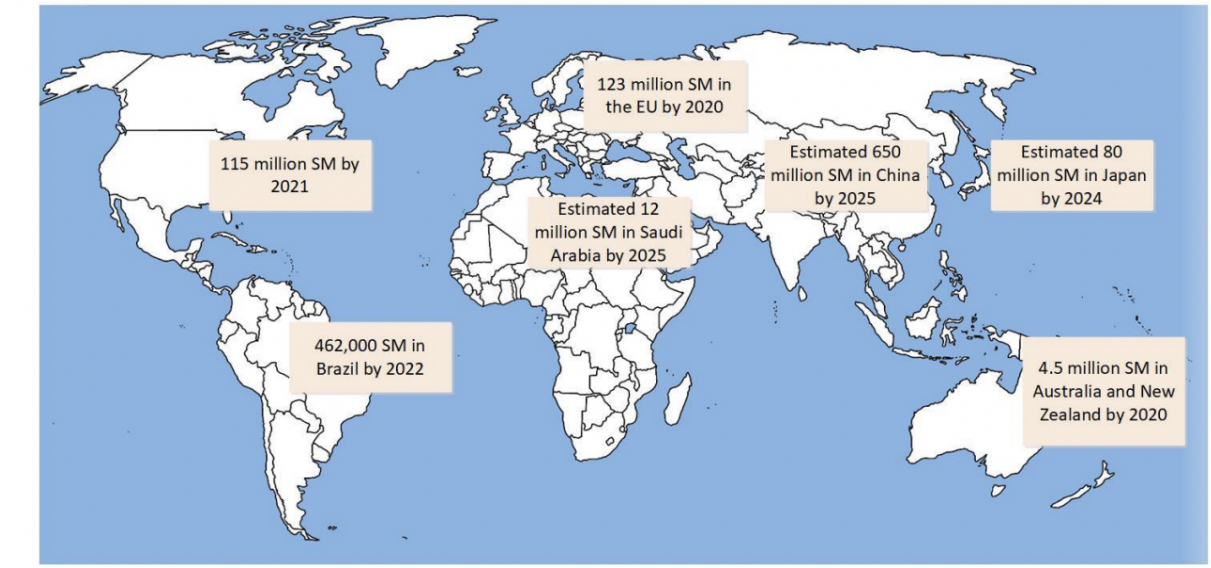


Figure 2: Smart meters installations and their estimations. Source: Joint Research Center - European Commission, 2023.

In other continents, relevant examples of energy transition transformations include Asia and Southeast Asia, major cities are paving the way to become "smarter" and are now pioneers at making better use of technology to improve energy efficiency in urban environments[95]Notable case studies feature Singapore, Chiang Mai in Thailand, Surabaya in Indonesia, and Sihanoukville in Cambodia[96]

1.3.2. Policy Support

It is safe to say these transformations would not be possible without policy support, crucial for fostering the needed transformations, starting from digitalization.

[95] Lola Woetzel et. al, "Smart cities: Digital solutions for a more livable future", McKinsey Global Institute, June 5th, 2018, https://www.mckinsey.com/capabilities/operations/our-insights/smart-cities-digital-solutions-for-a-more-livable-future

[96] ESCAP, "Smart Cities in Southeast Asia: A Landscape Review" (2022), https://www.zotero.org/yasminadionisi/search/escap/titleCreatorYear/items/E8WZ6ZVR/item-details

The main EU policy framework for achieving the renewable revolution is supported by the main initiative, the Fit for 55 Package, "the European climate law" which makes reaching the EU'S climate goal of reducing its emissions by at least 55% by 2030 a legal obligation. The package is a set of proposals to revise and update current EU legislation, and to put in place new initiatives which would ensure EU policies are into line with the climate goals agreed by the Council and the European Parliament.

The Fit for 55 Package includes the following strategies: shifting from fossil gas to renewable and low-carbon gases, reforming the EU emissions trading system, reducing emissions from key sectors (agriculture, transport, buildings, and waste), reaching climate goals in land and forestry sectors, sustainable transport, revising energy taxation, among others[97].

How is digitalization boosted in the EU's energy strategy? In October 2022, the European Commission adopted the "Digitalizing the energy system - EU action plan" (COM/2022/552). Both the European Green Deal and REPowerEU had reiterated the need for a deep digital and sustainable transformation of our energy systems[98].

Electrification sits at the core of the European Commission's energy goals, notably through the Energy System Integration strategy[99] as it stresses the importance that the increasing projected electricity (from 23% today to around 50% by 2050), shall be entirely supplied by renewable sources, and deeply based on an adequate deployment of smart grid of smart grid solutions. A report published in 2022 goes even further by stating how failure to accomplish such task would nullify any achievement, for instance made on clean energy production.

---

[97] European Council and Council of the European Union, "Fit for 55". Accessed August, 22, 2024, https://www.consilium.europa.eu/en/policies/green-deal/fit-for-55/#:~:text=for%2055%20package%3F-,What%20is%20the%20Fit%20for%2055%20package%3F,Council%20and%20the%20European%20Parliament.

[98] European Commission, "Questions and Answers: EU action plan on digitalizing the energy system", October 18, 2022, https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_6229

[99] European Commission and Joint Research Centre, "Clean Energy Technology Observatory, smart grids in the European Union: status report on technology development, trends, value chains and markets" (2022), https://data.europa.eu/doi/10.2760/276606

Following a directive issued by Brussels in 2006, European Union member states were legally obliged to turn 80% of their legacy meter stock to smart meters, by 2020. In 2010, some forms of smart meters market perception could be observed in Europe at the country-level. Italy could be defined as in-early adopter, notably through the "Progetto Telegestore", an initiative beginning in 2002 resulting in the installation of over 30 million smart meters points, covering close to 100 percent of Italian households. Sweden, Norway, Finland, and Denmark were also listed among the in-early adopters category, as penetration rates were already at above 50% [100].

The following chart, produced by Giglioli, Panzacchi and Senni as part of a McKinsey analysis, illustrated the progress of smart meter deployment by EU members stats.

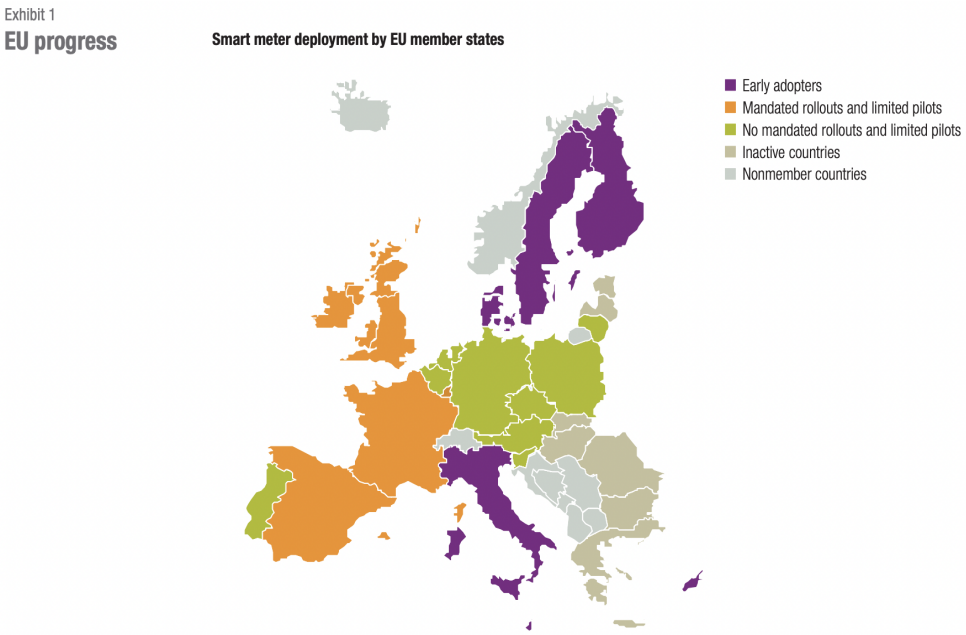


Figure 3: Smart meter deployment by EU Member States in 2010. Giglioli, Panzacchi, and Senni - McKinsey.

[100] Enrico Giglioli, Cosma Panzacchi, and Leonardo Senni, "How Europe is approaching the smart grid", McKinsey on Smart Grid (2010), https://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/EPNG/PDFs/McK%20on%20smart%20grids/MoSG_Europe_VF.ashx

In 2021, as stated in the annual Market Monitoring Report produced by the EU Agency for the Cooperation of Energy Regulators ("Energy Retail and Consumer Protection Volume", the penetration rate was over 80% at the end of 2022 in 13 EU countries, and 54% of European households had an electricity smart meter at the end of 2021[101].

On an international level, several bodies, such as international organizations are actively involved in promoting and supporting digitalization in the energy sector and are recognized for their crucial roles in developing standards, fostering collaboration, and providing guidance and funding for digital energy initiatives. Among these, the International Energy Agency, the International Renewable Energy Agency, and the World Economic Forum.

1.3.3. Industry support

Just as policy support, industries and the private sector are equally crucial: industry support is manifesting in the digitalization of energy systems in key ways, including technology research and innovation, investment and funding, partnerships and collaboration, and deployment.
Studies examining the contributions of industries, including technology providers, energy companies and investors are highlighting their role in support the transition to green critical infrastructure.

Various companies in the energy sector have recognized the potential of digital technologies and feel an urgent to "turn digital"[102]. Digitalization also serves as opportunity to gain direct economic benefits and revenue growth through the development of new products, services, and access to new customers.

---

[101] ACER and CEER, "Energy Retail and Consumer Protection. 2023 Market Monitoring Report" (September 2023), https://www.acer.europa.eu/sites/default/files/documents/Publications/2023_MMR_Energy_Retail_Consumer_Protection.pdf

[102] Justyna Światowiec-Szczepańska and Stepién Beata, "Drivers of Digitalization in the Energy Sector – The Managerial Perspective from the Catching Up Economy", *Energies* 15, no. 4 (2022), https://www.mdpi.com/1996-1073/15/4/1437

From cloud computing service providers (Amazon Web Services, Microsoft Azure), offering platforms for energy companies to store, process, and analyze data in a scalable and cost-effective manner, leading companies as Tesla and Vestas, developing technologies to integrate energy sources into the grid, or Siemens or Schneider Electric, developing IoT devices and smart sensors.

Researchers have demonstrated that public-private partnerships represent an important policy tool promoting sustainable economic development. They have played a role in improving the trend regarding economic sustainability of investment in infrastructure, though it can be argued that most public-private partnerships in the sector have shown a greater degree of participation of private investors, the latter assuming more responsibility and representing the main source of income[103]

1.3.4. Inequalities and Challenges in Smart Energy Transitions

If the transition of the European energy sector is effectively taking place, with a common, unified, regional energy policy, divergences in its implementation still exists, as the latter is still decentralized, politized, and dependent on the individual policies of Member States[104].

Contributions in literature suggest that the techno-centrism driving the smart energy transitions risk undermining the people, suggesting a need for energy sector digitalization to become people-centric and inclusive. Studies have found that planning and implementing sustainability transitions can exacerbate existing inequalities but equally offer opportunities to enable inclusive smart energy transitions[105].

---

[103] Olena Dyagileva et. al, "The use of the mechanism of public-private partnership in the investment processes management in the context of digitalization", *Cuestiones Politicas* 40, no. 72 (2022), https://produccioncientificaluz.org/index.php/cuestiones/article/view/37767

[104] (Justyna Światowiec-Szczepańska and Stepién Beata, "Drivers of Digitalization in the Energy Sector – The Managerial Perspective from the Catching Up Economy", *Energies* 15, no. 4 (2022), https://www.mdpi.com/1996-1073/15/4/1437

[105] Sareen Siddarth, "Digitalisation and social inclusion in multi-scalar smart energy transitions", *Energy Research & Social Science* 81 (2021), https://www.sciencedirect.com/science/article/pii/S2214629621003443

In fact, the digital divide is a contemporary issue worldwide, especially pronounced in rural and undeveloped regions. In 2021, according to the International Telecommunication Union (ITU), around 37% of the world's population remained unconnected to the internet[106].

Previous research has suggested that digitalization as a means of addressing energy poverty can involve an over reliance on technological solutions, distracting from the types of collaboration between multiple social actors and services, as well as systemic change required[107] . Digitalization may create the need for new and more complex socio-technical arrangements in the energy system, which may generate newer forms of inequality and exclusion[108], especially when the digital transformation entails challenges that require countries and the private sector to keep pace with technological change and user adoption rates, which is not always the case. For example, technologies such as cloud computing were once considered emerging, but are now seen as mainstream. Newer technologies such as blockchain, augmented reality and virtual reality, may not have a current significant impact within the organizations of our respondents, but are expected to have a heavy potential in the energy industry when it comes to managing large volumes of data and offering transparency, allowing multiple people to access the same data[109].

Concluding remarks

As the critical infrastructure of the energy transition undergoes a profound transformation, driven by the rapid advancements in digitalization and technology, this evolution brings numerous benefits including enhanced efficiency, better resource management and a significant boost in our ability to integrate renewable energy sources seamlessly, though continuous efforts are needed to refine and expand these digital solutions.

---

[106] International Telecommunications Union, "Digital inclusion of all". Accessed August 22, 2024, https://www.itu.int/en/mediacentre/backgrounders/Pages/digital-inclusion-of-all.aspx

[107] Joseph Cambers, Caitlin Robinson, and Matthew Scott, "Digitalisation without detriment: A research agenda for digital inclusion in the future energy system", *People, Place and Policy Online* 16, no. 2 (2023),

[108] Ibid.

[109] Joseph Cambers, Caitlin Robinson, and Matthew Scott, "Digitalisation without detriment: A research agenda for digital inclusion in the future energy system", *People, Place and Policy Online* 16, no. 2 (2023),

Digitalized energy systems represent a transformative shift towards more resilient and sustainable energy infrastructures by integrating digital technologies such as smart grids, the Internet of

Things, artificial intelligence and blockchain. Energy systems are becoming increasingly capable of real-time monitoring, predictive maintenance and automated management, qualities that not only facilitate the integration of distributed renewable energy sources, enhance grid stability, and enable more effective demand response strategies.

As it empowered consumers with detailed insights into their energy consumption, allowing for more informed decisions and greater energy savings, digitalization supports the development of new business models fostering a more decentralized and democratized energy market, from peer-to-peer energy trading to virtual power plants.

Countries and regions are continuing to invest in and adopt these digital solutions, therefore, increasing the potential for significant reductions in carbon emissions, and improvements in energy efficiency.

The global transition towards a greener and more sustainable future is therefore made increasingly attainable.

Some key challenges still need to be addressed. There are two main challenges that exist posing barriers and threats to progress one concerns the economic and management costs associated with the adoption of technologies, the other concerning the security of the infrastructures involved.
As a matter of fact, the vulnerability of critical energy infrastructure continues to be an issue of concern, as due to the lucrative nature of cybercrime, criminals are constantly seeking new means of attack[110].

[110] Musadag El Zein and Girma Gebrensenbet, "Digitalization in the Renewable Energy Sector", *Energies* 17, no. 9 (2024), https://doi.org/10.3390/en17091985

Considering their significance on a global level, incorporating digital technologies will be a key factor in shaping the industry's future, and adoption, while also reducing costs, yet it is crucial to identify the challenges the energy transition faces today.

Chapter II: Cyberattacks to Critical Energy Infrastructure

The cyberspace has acquired a pivotal role in most present economic, commercial, cultural, social and government activities and interactions of countries. This goes at all levels, from government and governmental institutions, non-governmental organizations, businesses, and individuals. As a matter of fact, the modern world is highly dependent on electronic technology, and most importantly, on the Internet[111].

Within the vast global network which the Internet has created, vital and sensitive infrastructures and systems are an integral part, as they either are part of the cyberspace themselves, or are exploited, controlled, and managed through this space, where their vital and most sensitive information is continuously transferred to[112].

Cyber-threats are particularly unique threats that must be distinguished by traditional national security threats. The latter are largely transparent in nature, with actors that are governments and nations or likewise, groups or individuals, that can be identified in a specific geographical area[113]. The new emerging cyber-threats have been challenging national security in its traditional sense.

The Russia-Ukraine war has significantly contributed to increasing the frequency, spread, and intensity of cyber-attacks against the energy sector. Yet, it is important to note that these have roots that precede the beginning of the military confrontation between Moscow and Kiev[114].

A growing trend of these actions against the energy sector had been previously favored by the Covid-19 pandemic, during which the increase in remote activities structurally amplified the

---

[111] Yuchong Li and Qinghui Liu, "A comprehensive review of cyber-attacks and cyber security; Emerging trends and recent developments", *Energy Reports* 7, no. 8 (2021), 10.1016/j.egyr.2021.08.126

[112] Ibid

[113] Ibid.

[114] Simone Pasquazzi e Adriano Savarino Morelli, "*Cyber-attacks,* geopolitica e settore energetico" in *Europea* 1 (June 2023), DOI: 10.53136/97912218086436

exposure to cyber-attacks for many targets, as the increase in remote activities effectively incentivized cybercrime in general[115].

Most importantly, as it has been analyzed, the current energy infrastructure is ever-so integrated within cyberspace. Cyber infrastructure can provide a backbone for economic stability, growth, agility, and new business opportunities[116]. However, a decisive question must now be addressed, and it is that of the cyber-vulnerabilities that arise from the many weaknesses in infrastructure design and operations[117].

Cyber vulnerability includes the many security weaknesses that can lead to cyber-attacks. The latter use tools consisting of Internet-based data communications and its associated infrastructure that national critical infrastructures rely on.

2.1. Energy Infrastructures as Targets

2.1.1. Critical Energy Infrastructures as an Object of National Security

The multitudinous and increasingly complex nature of security threats has been recognized, by States, international organizations, as well as private and public stakeholders as a primordial challenge.

i. In the United States

Attacks on energy infrastructure fall into attacks on a broader category of attacks against critical infrastructures and critical information infrastructures, which have become more frequent, complex, and targeted to the recent, contemporary energy systems. To comprehend why this issue is pertinent to security policies, it is crucial to understand the integral role that critical infrastructure plays in the broader context of security and defense strategies.

---

[115] Simone Pasquazzi e Adriano Savarino Morelli, "*Cyber-attacks,* geopolitica e settore energetico" in *Europea* 1 (June 2023), DOI: 10.53136/97912218086436

[116] Frederic Lemieux, *Current and Emerging Trends in Cyber Operations* (London: Palgrave Macmillan UK, 2015).

[117] Ibid.

The concept of "critical infrastructure" has been a subject of political debate. Broadly speaking, critical infrastructure can be defined as those physical and virtual systems underlying modern societies and considered as vital for their survival[118]. In fact, modern societies rely on a complex tapestry of infrastructures encompassing virtually every essential sector. From energy, communications, health, transportation, food, and agriculture[119]. Most States have a detailed definition regarding their critical infrastructure, including, its importance to society, its various parts, and sectors, oftentimes, the continent by which it is safeguarded and finally, their associated threats. National definitions may differ slightly in the criteria used to define the criticality of infrastructure, though most countries use cross-cutting criteria which covers infrastructure of all sectors[120]. Notwithstanding, today critical infrastructure systems are recognized as the literal foundations of any state. They provide essential-to-life public (and private) services upon which people are dependent on[121]. The safe and effective management of critical infrastructure constitutes an indicator of a state's social welfare and economic development[122]. As such, critical infrastructure protection emerges as a primary concern for national security, as can be demonstrated by the examination of historical events, government policies, and strategic documents.

Starting from the United States, the definition of critical infrastructures as well as its list of examples has broadened over time, and scholars and practitioners have argued that this has exerted an effect on the development and implementation of critical infrastructure protection policy Before

[118] A. Burak Daricili and Soner Çelik, "National Security 2.0: The Cyber Security of Critical Infrastructure", *Perceptions* 26, no. 2 (2021), https://dergipark.org.tr/en/download/article-file/2181981

[119] Lior Tabanski, "Critical Infrastructure Protection against Cyber Threats", *Military and Strategic Affairs* 3, no. 2 (2011), https://www.inss.org.il/wp-content/uploads/2017/02/FILE1326273687-1.pdf

[120] A. Burak Daricili and Soner Çelik, "National Security 2.0: The Cyber Security of Critical Infrastructure".

[121] Cybersecurity & Infrastructure Security Agency, "Critical Infrastructure Sectors". Accessed August 20th, 2024, https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

[122] A. Burak Daricili and Soner Çelik, "National Security 2.0: The Cyber Security of Critical Infrastructure".

the addition of "critical", the seemingly labeled term "infrastructure" has been a subject debated by public policy makers[123].

In the United States, even before the events of 9/11, despite a lively debate on infrastructure security in the 1980s, a common understanding or generally accepted definition of the term was absent[124]. A non-agreed definition or standard renders the concept of infrastructure fluid in policy terms[125].

Notwithstanding, a starting point for key legislation is identified in July 1996, when President Clinton signed the Executive Order 13010, which established the President's Commission on Critical Infrastructure Protection. The PCCIP was created partly in response into the bombing of the Murrah Federal Building, in Oklahoma City in 1995. President Bill Clinton gave it the mandate of studying the complexities of the nation's critical infrastructure and issue recommendations for improving their security. Defined as the "worst act of homegrown terrorism in the nation's history", the bombing, supposedly on little-known federal building, located well outside of the "nervous system" of Washington, D.C., entailed a devastating human toll with 1968 deaths, including 19 children, several hundred more injured, and more than 300 nearby buildings damaged or destroyed[126] off a chain of reactions and events as government officials recognized the crippling effects that rose from the disruption[127]

---

[123] National Research Council, *Terrorism, and the Electric Power Delivery System* (Washington D.C.: National Academies Press, 2012.

[124] Jan Metzger, "The concept of critical infrastructure protection" in *Business and Security. Public-Private Sector relationships in a New Security Environment* (Stockholm: Sipri, 2004), https://doi.org/10.1093/oso/9780199274505.003.0018

[125] John Moteff, Claudia Copeland, John Fischer, "Critical Infrastructures: What Makes an Infrastructure Critical?", *Defense Technical Information Center* (2015), http://www.fas.org/sgp/crs/homesec/RL30153.pdf

[126] Kathi Ann Brown, *Critical Path. A Brief Critical Infrastructure Protection in the United States* (Spectrum Publishing Group Inc: Fairfax, Virginia, 2006), https://cip.gmu.edu/wp-content/uploads/2016/06/CIPHS_CriticalPath.pdf

[127] Ibid.

The Order pointed at what rendered an infrastructure critical as such[128]:

"Certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States".[129]

The following clarifying definitions were provided. Critical infrastructure encompasses "the framework of interdependent networks and systems compromising identifiable industries, institution, including people and procedures, and distribution capabilities that provide:

1. A reliable flow of products and services essential to the defense and economic security of the United States.
2. A smooth functioning of government at all levels, and society.
3. Defense security, intended as "the confidence that Americans' lives and personal safety, both at home and abroad, are protected, and the United States' sovereignty, political freedom, and independence, with its values, institutions, and territory intact are maintained.
4. Economic security, intended as the confidence that the nations' goods and services can successfully compete in global markets while maintaining or boosting real incomes of citizens."

1. Infrastructures as the framework of interdependent networks and systems compromising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide are eligible flow of products and services essential to the defense and economic security of the United States".[130]

In addition, safeguarding critical infrastructure would involve addressing the condition of being debilitated, which refers to a state of defense or economic security marked by ineffectiveness[131].

---

[128] John Moteff, Claudia Copeland, John Fischer, "Critical Infrastructures: What Makes an Infrastructure Critical?", *Defense Technical Information Center* (2015), http://www.fas.org/sgp/crs/homesec/RL30153.pdf

[129] Executive Order 13010 – Critical Infrastructure Protection, https://www.presidency.ucsb.edu/documents/executive-order-13010-critical-infrastructure-protection

[130] John Moteff, Claudia Copeland, John Fischer, "Critical Infrastructures: What Makes an Infrastructure Critical?", *Defense Technical Information Center* (2015), http://www.fas.org/sgp/crs/homesec/RL30153.pdf

[131] Ibid.

The Commission deliberated for fifteen months and in October 1997, published its final report, Critical Foundations: Protecting America's Infrastructure. The report created a new understanding of the nation's strengths and weaknesses and outlined principles that became entering arguments in the debate over the post 9/11[132]. The then PCCIP (chaired by General Robert T. Marsh), included several senior-level government officials, private industry executives, and leaders from the academic community.

The definition "critical infrastructures as assets whose prolonged disruption could cause significant military and economic dislocation"[133].

However, as homeland security has been assigned the highest national priority, the term "critical infrastructure" has developed into a major policy concern. Documents dealing with critical infrastructure protection have provided broad definitions of what makes an infrastructure critical. In fact, the events of 9/11 profoundly reshaped the concept and approach to critical infrastructure protection. As the terrorist attacks demonstrated national level physical vulnerability to the threat posed by mass destruction terrorism, the development of national plans for physical protection became even more of an imperative[134]

In June 2002, President Bush issued a proposal for establishing a Department of Homeland Security, prescribing the responsibilities of the Department's for Information Analysis and Infrastructure Protection. These included:

1. A comprehensive assessment of the vulnerabilities of the key resources and critical infrastructures in the United States.
2. An identification of the protective priorities and supporting protective measures

---

[132]

[133] Jan Metzger, "The concept of critical infrastructure protection" in *Business and Security. Public-Private Sector relationships in a New Security Environment* (Stockholm: Sipri, 2004), https://doi.org/10.1093/oso/9780199274505.003.0018

[134] White House Administrative Office, "The national strategy for the physical protection of critical infrastructures and key assets", February 1st, 2003, https://rosap.ntl.bts.gov/view/dot/33977

3. A development of a comprehensive national plan for security the key resources and critical infrastructures in the country
4. A commitment to take or seek to effect necessary measures to protect the key resources and critical infrastructures in the United States[135].

Today, various lists and frameworks categorize and define critical infrastructure to help in their protection and management. Some key frameworks for infrastructure protection include the US' Department of Homeland Security's identification of 16 critical infrastructure sectors, namely,

1. Chemical,
2. Commercial facilities,
3. Communications,
4. Critical manufacturing,
5. Dams,
6. Defense industrial base,
7. Emergency Services
8. Energy,
9. Financial services,
10. Food and agriculture,
11. Healthcare and public health,
12. Information technology,
13. Nuclear reactors,
14. Materials and waste,
15. Postal and shipping
16. Water and wastewater systems.

A comprehensive framework for managing risk to critical infrastructure is provided in the National Infrastructure Protection PLAN (NIPP), ultimate in 2013, which incorporates these 16 DHS sectors into its approach. On April 30th, 2024, the White House released the National Security Memorandum-22 (NSM) on Critical Infrastructure Security and Resilience which updates national

[135] National Research Council, *Terrorism, and the Electric Power Delivery System* (Washington D.C.: National Academies Press, 2012.

policy on how the governments should protect and secure critical infrastructure from "cyber and all-hazard threats. As stated, the document recognizes the changed risk landscape over the past decade, leveraging the enhanced authorities of agencies and federal departments to implement a new risk management cycle which priorities collaborating with partners to identify and mitigate sector, cross-sector, and nationally significant risks. The NSM-22 was released to guide the creation of the 2025 National Infrastructure Risk Management Plan (National Plan), that would update and replace the 2013 National Infrastructure Protection Plan[136] .

ii. In the European Union

The European Critical infrastructures include power grids, the transport network and information and communication systems. Protection of these infrastructures is vital for the security of the EU and the well-being of its citizens.

The European Union defines critical infrastructure through its European Program for Critical Infrastructure (EPCIP), which specifically focuses on energy, transport, information technology, financial services, and health[137]. In fact, "critical infrastructures include power grids, the transport network, and information and communication systems" [138]. The EPCIP is a framework under which a package of different measures together aims to improve the protection of critical infrastructure, with a package of measures aimed at improving the protection of critical infrastructure across all EU States and in all relevant sectors of economic activity [139].

The EPCIP was endorsed by intention of the Commission to propose a European program for this purpose, as it came after the Communication on Critical Infrastructure Protection in the Fight against Terrorism, which was adopted by the Commission on 20 October 2004. The

[136] Ibid.

[137] Madeleine Lindsörm and Stefan Olsson, "The European Programme for Critical Infrastructure Protection" in *Crisis Management in the European Union. Cooperation in the Face of Emergencies* (Springer, 2009).

[138] EU. Science Hub, "Critical infrastructure protection". Accessed August 28th, 2024, https://joint-research-centre.ec.europa.eu/scientific-activities-z/critical-infrastructure-protection_en

[139] Ibid.

Communication had already put forward suggestions on what would enhance European prevention, preparedness, and response to terrorist attacks involving Critical Infrastructures (CI).

While recognizing the threat from terrorism as a priority, it affirmed the protection of critical infrastructure to be based on an all-hazards approach.

Moreover, it laid a procedure for the identification and designation of European Critical Infrastructure (ECI), to be implemented by the way of a Directive. The responsibility for protecting National Critical Infrastructure falls on the NCI owners and operators and on the Member States; with the Commission supporting the Member State in doing so.

The criteria for identification and designation of National Critical Infrastructures would be predefined and developed by each Member State, considering, as minimum, the following quantitative effects of the disruption or destruction of a particular infrastructure:

1. Scope
2. Severity, assessed based on
    a. Economic effect
    b. Environmental effect
    c. Political effect
    d. Psychological effects
    e. Public health consequences

The rating of the scope of the disruption and destruction of a particular critical infrastructure would be rated by the extent of the geographic area and could be affected by its loss or uncivility.
With due regard to existing Community competences, the responsibility for protecting National Critical Infrastructures falls on the NCI owners/operators and on the Member States. The Commission will support the Member States in these efforts where requested to do so.
An additional key document is the EU initiative on Critical Infrastructure (CIIP), which aims to strengthen the security and resilience of vital information and Communication Technology (ICT)

infrastructures[140]. Technical support is provided by bodies like the European Reference Network for Critical Infrastructure Protection (ERNCIP) which supports the review of the Directive on European Critical Infrastructures and carries out different research activities, notably the development of methods and tools for international cyber security exercises, the assessment of the vulnerability of networked infrastructure in case of extreme weather events, and the evaluation of the resistance of buildings and transport systems against explosions[141].

Infrastructures listed by the EU also include global navigation systems, such as the Global Positioning System (GPS) and Galileo, primary sources of precise position and timing information and deemed critical to safe operation of several critical infrastructures, including the power grid[142] Since the first Union list of common projects of interest, published in 2013, cross-border energy infrastructure projects have been primordial as these contribute to provide affordable, secure, and sustainable energy to EU citizens and businesses. Projects of common interest (PCIs) are key-cross border infrastructure projects that link the energy systems of EU Countries, helping the EU achieve its energy policy and climate objectives, and the long-term decarburization of the economy in accordance with the Paris agreement[143]

iii. International and global definitions

Within this framework, on 11 January 2023, the President of the European Commission Ursula von Der Leyden, and the Secretary General of NATO, General Jens Stoltenberg, announced the institution of a dedicated NATO-EU Task Force on the resilience of critical infrastructure[144]- (as ensuring the resilience of infrastructure is critical to EU Member States and NATO Allies.

---

[140] EU. Science Hub, "Critical infrastructure protection". Accessed August 28th, 2024, https://joint-research-centre.ec.europa.eu/scientific-activities-z/critical-infrastructure-protection_en

[141] Ibid.

[142] Ibid.

[143] European Commission, EU-NATO Task Force: Final assessment report on strengthening our resilience and protection of critical infrastructure", June 29th, 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3564

[144] Ibid.

Moreover, the United Nations Security Council unanimously adopted Resolution 2341 on Protection of Critical capacities, to Prevent Attacks against Critical Infrastructure, as "the first ever global instrument entirely devoted to the protection of CIs against terrorist attacks". It called upon Member States to address the danger of terrorist attacks against critical infrastructure, and inviting Member States to consider possible preventive measures in developing national strategies and policies In its *Compendium of Good Practices ("The protection of critical infrastructure against terrorist attacks)* published by the United Nations Office of Counter-Terrorism (UNOCT), with the Counter-Terrorism Committee Executive Directorate (CTED), and INTERPOL, it defined critical infrastructures as the assets and processes from which our societies depend on for its survival[145].

The importance of the concept in contemporary security thought is observed by just the fact that national plans for the protection of critical infrastructure thrive everywhere. Australia, Canada, Japan, Germany, and some African nation-states such as Kenya also have plans including a definition of critical infrastructure[146]

Defining the term is the first logical step before implementing programs or plans defending it, but most definitions of critical infrastructure are always followed by a list of critical sectors. Identifying these facilitates identification, prioritization, assessment, and protection of critical infrastructure.

Based on a study by Gallais and Filiol on a comparison of the definitions of 'critical infrastructure', lists of critical sectors greatly vary but most of the nation-states and organizations seem to agree on the importance of specific critical sectors, namely, energy, communication technology, finance, transport, and water.

---

[145] United Nations Office of Counter-Terrorism, "Opening remarks by Vladimir Voronkov », High-level hybrid event to launch the updated United Nations Compendium of Good Practicces on the Protection of Critical Infrastructure against Terrorist Attacks", June 5th, 2023, https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/230605_usg_opening_remarks_cip_launch_madrid_as_delivered.pdf

[146] C. Gallais and E. Filiol, "Critical Infrastructure. Where do We Stand Today?", *Journal of Information Warfare* 16, no. 1 (Winter 2017), https://www.jstor.org/stable/26502877

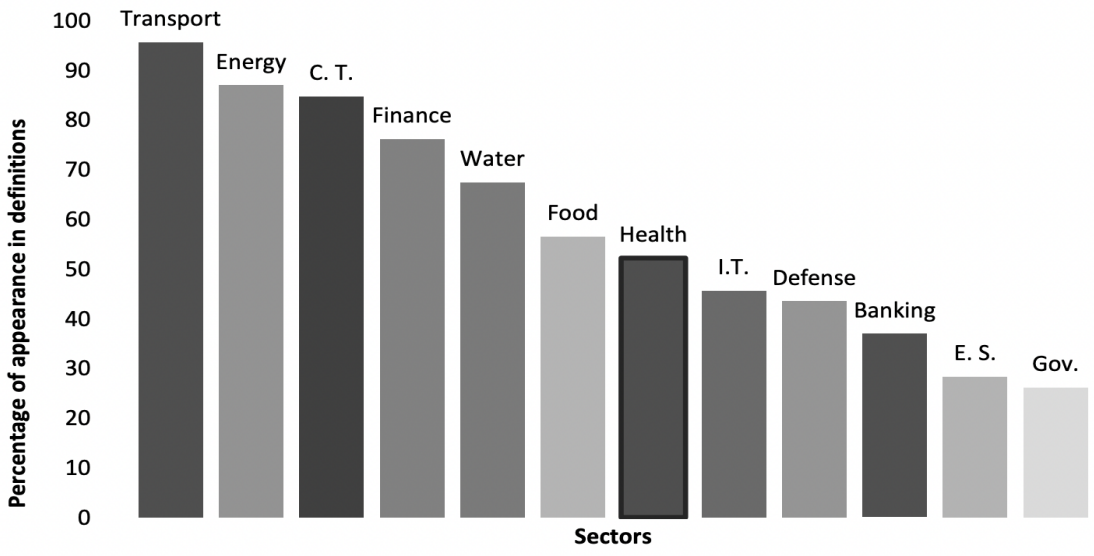


Figure 4: Histogram of the most cited sectors in lists of critical sectors. Source: Gallais and Filiol, 2017.

2.1.1. CI Interdependencies and the Energy Sector

Sector-specific entities have their own infrastructure networks, designed and evolving within their sector. However, these networks have inevitable interdependencies between each other. According to the UK Infrastructure Transitions Research Consortium (ITRC), the concept of interdependence has not attracted a significant deal of attention yet [147].

Yet the concept is more that abstract and theoretical, as can be shown by early examples of failure and other recent infrastructure disruptions. In 1998, the Galaxy 4 telecommunications satellite lost contact with Earth and the lives of people all over North America were disrupted and resulted in

[147] R. Pant, S. Thacker, J.W. Hall, S. Barr and D. Alderson, "Building an integrated assessment methodology for critical infrastructuer risk assessment", *Society for Risk Analysis Annual Meeting,* Maryland, US, 8-11 December 2013, https://www.itrc.org.uk/itrcpublications/building-an-integrated-assessment-methodology-for-critical-infrastructure-risk-assessment/

an outage of nearly 90% of all pagers nationwide[148].What's more was that a variety of banking and financial services, such as credit card purchases and automated teller machine transactions were disrupted, threatening key segments of the vital human services network by disrupting communications with doctors and emergency workers. From and interdependency perspective, the assumption that networks in what sector - as, for example, transport for the delivery of chemicals - will continue to function come-what-may was shattered; and it continues to be as such because of a series of disruptive and damaging, and ever so frequent incidents. The UK flooding of an electricity substation in Lancaster in December 2015 caused days without electric power for information and communications technologies, revealing how rapidly, *all* societal functions can cease without electricity[149].

Digital connectivity and electricity, as the dominant energy vector, emerge as essential for all infrastructure networks to function. These interdependencies are being reinforced by the dominant direction of technological change towards electrification and digitalization[150].
The property that all the critical infrastructures have in common is that they all represent complex collections of interacting components, that is, they are complex adaptive systems (CASs). Each component of an infrastructure constitutes a small part of the intricate web that forms the overall infrastructure. Infrastructures are therefore more than just an aggregation of their components.

The identification, understanding and analysis of such interdependencies are significant challenges greatly magnified by the complexity and the breadth of our critical infrastructures. A broad range of interrelated systems conditions and factors, that Rinaldi et. as defined in terms of six "dimensions" further complicate this challenge. The degree to which the infrastructures are linked strongly influences their operational characteristics. If some linkages are relatively flexible, thus,

---

[148] Gianmario Rinaldi, Michele Cucuzella, Prathyush P. Menon, Antonella Ferrara, Christopher Edwards "Load Altering Attacks Detection, Reconstruction and Mitigation for Cyber-Security in Smart Grids with Battery Energy Storage Systems", European Control Conference (ECC), IEEE (2023), https://ieeexplore.ieee.org/abstract/document/9838515/authors#authors

[149] R. Pant, S. Thacker, J.W. Hall, S. Barr and D. Alderson, "Building an integrated assessment methodology for critical infrastructuer risk assessment", *Society for Risk Analysis Annual Meeting,* Maryland, US, 8-11 December 2013, https://www.itrc.org.uk/itrcpublications/building-an-integrated-assessment-methodology-for-critical-infrastructure-risk-assessment/

[150] Ibid.

"loose", other are tight, the system is left with little or no flexibility to respond to changing conditions or failures, exacerbating problems or cascading from one infrastructure to another[151]. The linkages can be physical, cyber, related to geographic location, or logical in nature. As depicted in the figure, the dimensions include the technical, economic, business, social/political, legal/regulatory, public policy, health and safety, and security concerns affecting infrastructure operations [152].

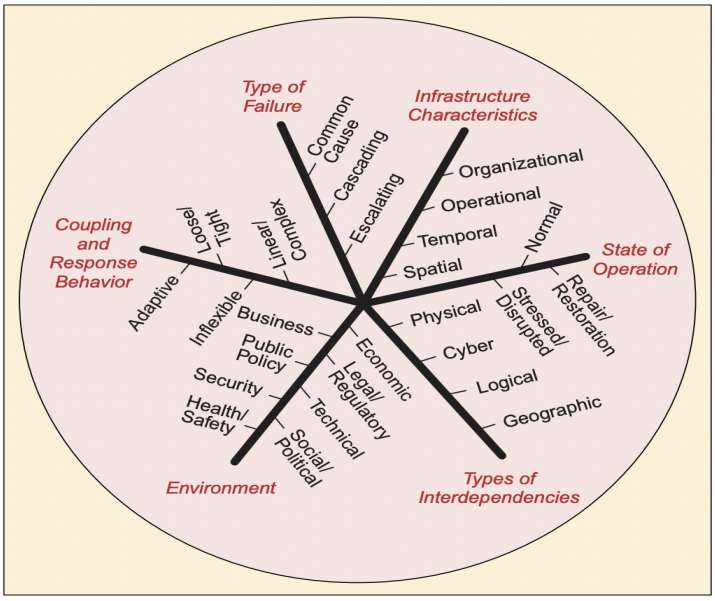


Figure 5: Dimensions for describing infrastructure interdependencies. Source: Rinaldi, Perenboom and Kelly, 2001.

The dimensions of interdependencies involve different relation. As stated, these can be:

1. Physical
2. Cyber
3. Geographic
4. Logical

[151] Gianmario Rinaldi, Michele Cucuzella, Prathyush P. Menon, Antonella Ferrara, Christopher Edwards "Load Altering Attacks Detection, Reconstruction and Mitigation for Cyber-Security in Smart Grids with Battery Energy Storage Systems".

[152] Ibid.

Two infrastructures are physically interdependent when the state of each is dependent on the material output of others. When one infrastructure requires another infrastructure for it to operate, it becomes a commodity produced or modified by one infrastructure. A rail network and a coal-fired electrical generation plant are physically interdependent, given that each supplies commodities requires others to function properly, and a change in the state in the railroad - for instance, a halt in the delivery of coal, can drive a corresponding connection state change in the electrical grid - such as a switch to alternative fuels or additional generation from non-coal-fired plants[153]

Cyber interdependencies usually concern information transmitted to the information infrastructure. An infrastructure whose states depends on information transmitted through the information infrastructure is largely cyber interdependent. As mentioned, they are the result of the persuasive computerization and automation of infrastructures over the last several decades. The concept of cyber-interdependency is more in-depth developed in the following paragraph[154] (see 2.1.2.)

Moving on, when a local environment event can generate state changes in all infrastructure, then these are geographically interdependent. An explosion of a fire could create correlated disruptions or change in these geographically interdependent. Such interdependencies are to be distinguished by cyber and physical interdependencies as they are considered as such when infrastructures are closely located.

Finally, logical interdependencies concern infrastructures which are logically interdependent on another when the state of each depends on the state on another because of a connection that is, however, not physical, cyber, or geographic. These connections often might include variables like the financial state and the bond ratings of infrastructures, and human decisions. For instance, the

[153] Gianmario Rinaldi, Michele Cucuzella, Prathyush P. Menon, Antonella Ferrara, Christopher Edwards "Load Altering Attacks Detection, Reconstruction and Mitigation for Cyber-Security in Smart Grids with Battery Energy Storage Systems".

[154] Ibid.

logical interdependency between the petroleum and transportation infrastructures is due to human actions and decisions and is not the result of physical processes.
It is important to understand that interdependencies are the result of infrastructure topologies - which enable interactions and feedback mechanisms, the same which often lead to unintended behaviors and consequences during disruptions [155].

The concept of interdependence is not to be confused with the one dependency, which usually concerns two infrastructures. Individual connections between two infrastructures are in most cases unidirectional: if an infrastructure *x* depends on an infrastructure *y* to their link, *y* does not usually depend on the same link. For instance, electricity is used to power a telecommunications switch and not vice versa.

In the general case, when examining the framework of multiple infrastructures connected as a "system of systems"; infrastructures are frequently connected through multiple points through a wide variety of mechanisms, in a bidirectional relationship existing between the states of any given pair of infrastructures.

The following figure is illustrative of the concept.

[155] Gianmario Rinaldi, Michele Cucuzella, Prathyush P. Menon, Antonella Ferrara, Christopher Edwards "Load Altering Attacks Detection, Reconstruction and Mitigation for Cyber-Security in Smart Grids with Battery Energy Storage Systems".

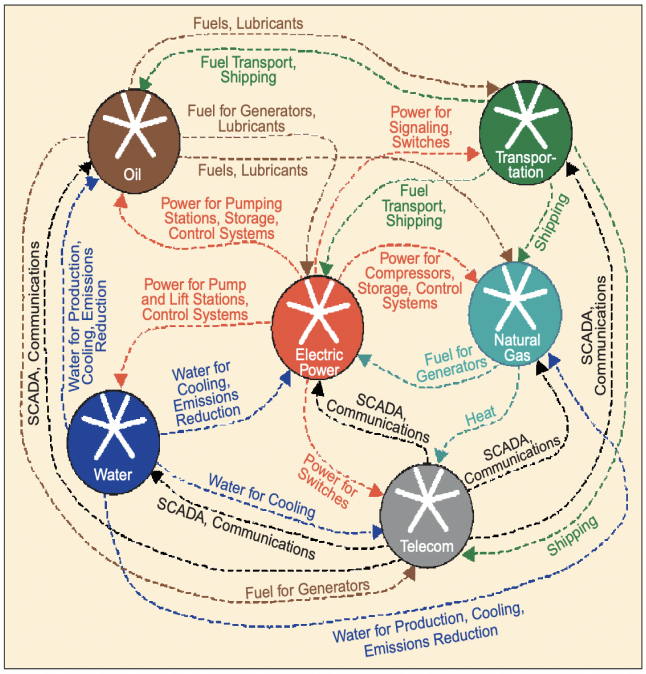


Figure 6: Examples of Infrastructures Interdependencies within the Oil, Electric Power, Transportation, Natural Gas, Telecom and Water sectors. Source: Rinaldi, Perenboom and Kelly, 2001.

Cross-sector settings signified by diverse interest, distributed decision-making authorities, and fragmented ownership and knowledge exacerbate interdependence-related risks[156]

For this reason, the prioritization on sectors is since many other societal functions are strongly dependent on these. The energy sector is highly recognized fundamental to operation and efficiency of various other sectors. In the power sector, one attack can bring down an entire power network and have severe cross-sector implications[157].

The following diagrams, published by the U.S. department of Energy, illustrate the direct connections between the energy sectors, its infrastructures, and various other sectors.

---

[156] Tove Rydén Sonesson, "Governance and interdependencies of critical infrastructures: Exploring mechanisms for cross-sector resilience", *Safety Science* 142 (October 2021), https://www.sciencedirect.com/science/article/pii/S0925753521002277

[157] Bridget R. Kane et. al, "Threats to Critical Infrastructure. A Survey", RAND, June 11th, 2024, https://www.rand.org/pubs/research_reports/RRA2397-2.html

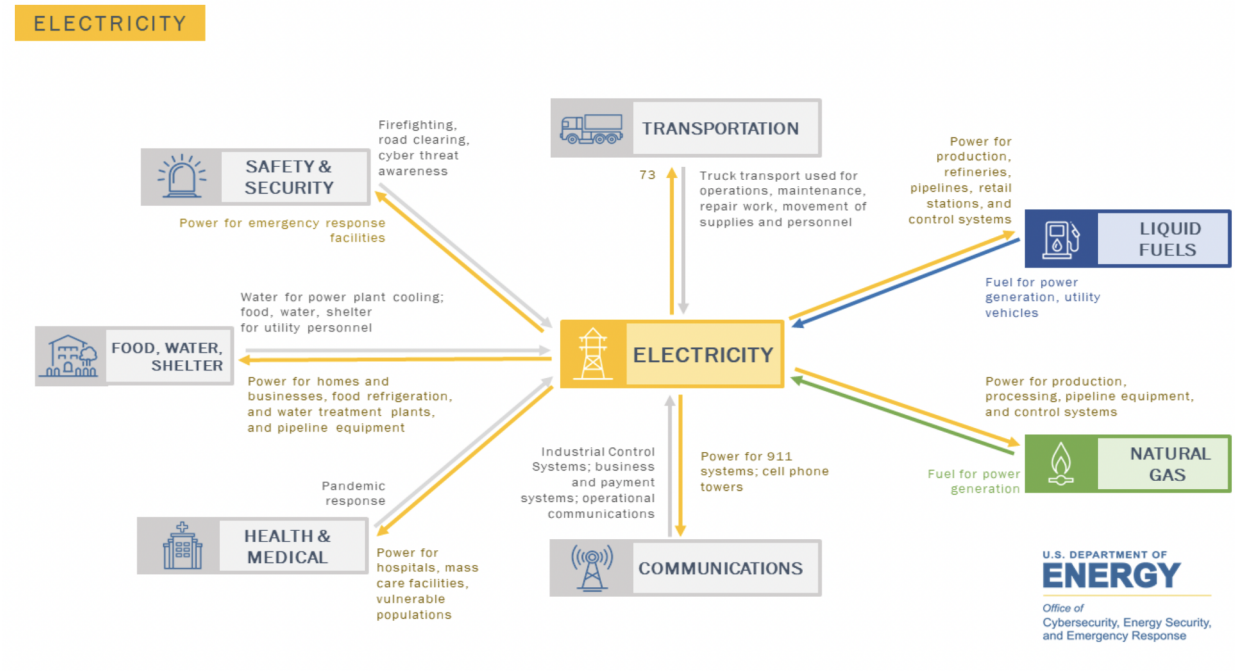


Figure 7: State Energy Security Plan Optional Drop-In: Cross Sector Interdependency Diagrams - Electricity. Source: U.S. Department of Energy, 2022.

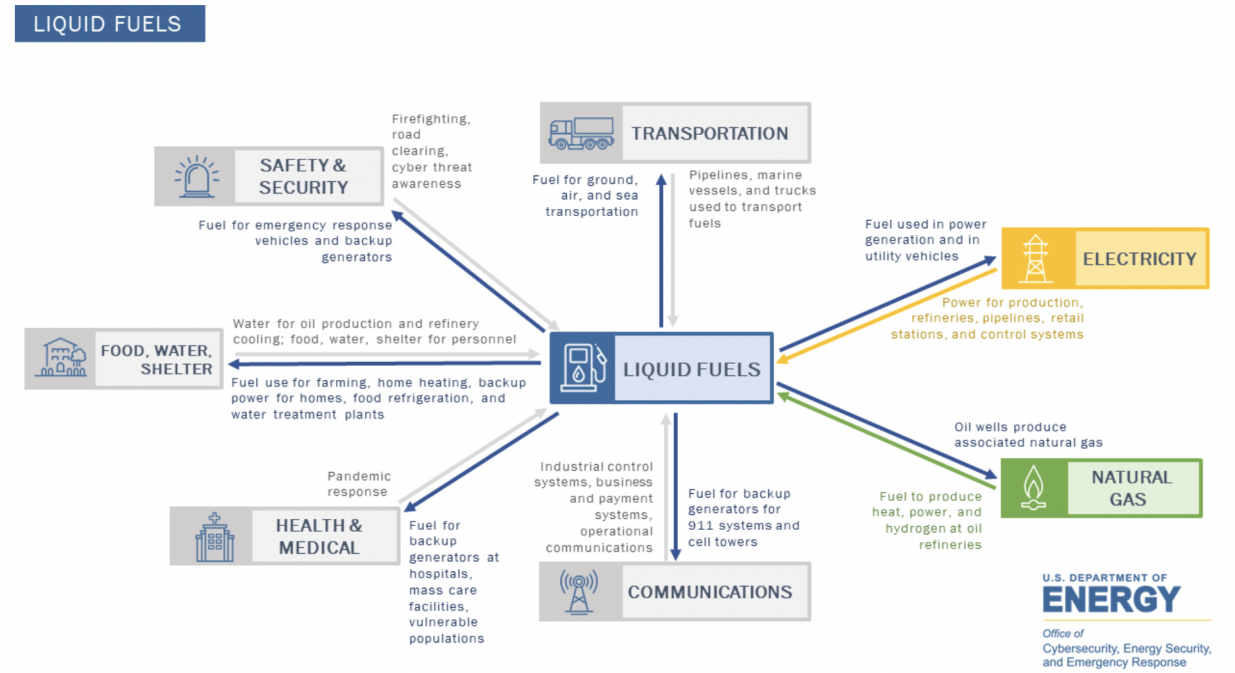


Figure 8: State Energy Security Plan Optional Drop-In: Cross Sector Interdependency Diagrams - Liquid Fuels. Source: U.S. Department of Energy, 2022.

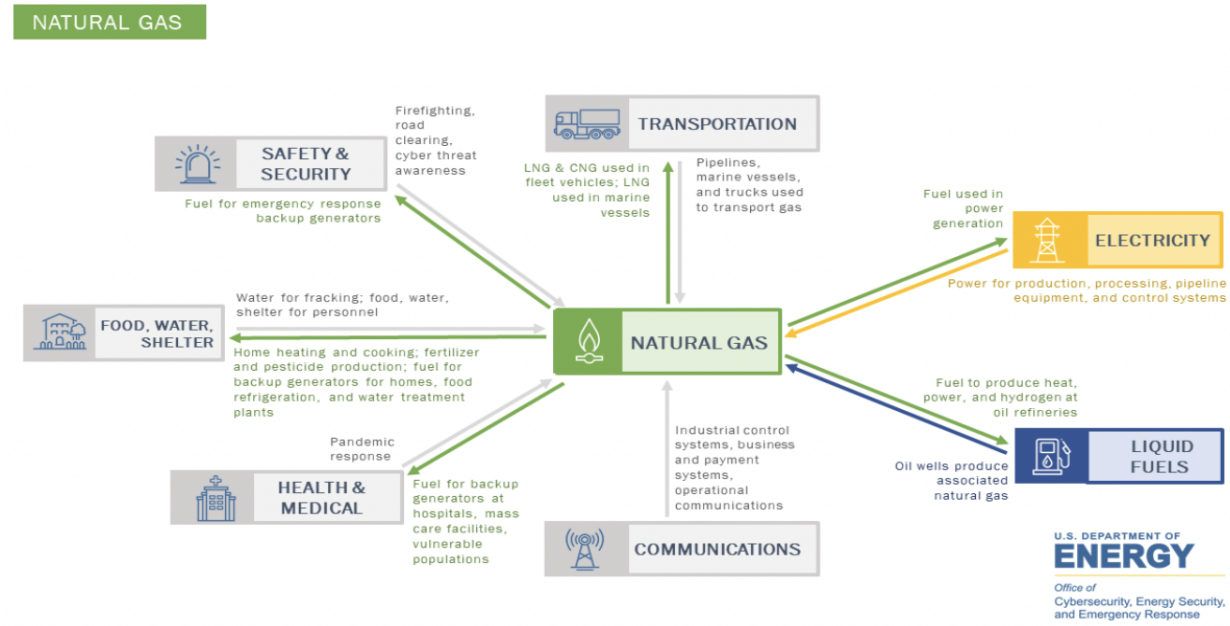


Figure 9: State Energy Security Plan Optional Drop-In: Cross Sector Interdependency Diagrams - Natural Gas. Source: U.S. Department of Energy, 2022.

In sum, it is imperative to comprehend that perturbations in one infrastructure can ripple over to other infrastructures; as the risks of failure or deviation from normal operating conditions in one infrastructure can be a function of risks in a second, or more, infrastructures, when these are interdependent[158].

[158] Gianmario Rinaldi, Michele Cucuzella, Prathyush P. Menon, Antonella Ferrara, Christopher Edwards "Load Altering Attacks Detection, Reconstruction and Mitigation for Cyber-Security in Smart Grids with Battery Energy Storage Systems".

Failure to properly manages risks and accidental events like cyberattacks could cause incidents of various magnitude, which could lead, in a worst-case scenario, to serious consequences, including loss of life, damage to properties, environmental pollution, among others[159] .
In this manner, perturbations in one infrastructure can ripple over to other infrastructures.

Consequently, the risk of failure or deviation from normal operating conditions in one infrastructure can be a function of risk in a second infrastructure if the two are interdependent.

2.1.2. Vulnerabilities of Contemporary Critical Energy Infrastructure (CEI)

Contemporary critical energy infrastructure is particularly vulnerable to cyber interdependencies, which are relatively new threats, driven by the persuasive computerization and automation of infrastructures, over the last several decades[160].

It has been acknowledged that the technologies and algorithms that drive the digital transformation and not neutral, in the sense that they do not provide guarantees that the positive effects promised by digitalization will result[161]. Unintended side effects may occur ì, and these can be often hardly calculable and difficult to control.

What components of the digitalization and decentralized energy infrastructure rendering it most vulnerable to cyber-attacks?

---

[159] Eni, *A Just Transition* (Report) (2023), https://www.eni.com/content/dam/enicom/documents/eng/sustainability/2023/eni-for-2023-just-transition-eng.pdf

[160] Gianmario Rinaldi, Michele Cucuzella, Prathyush P. Menon, Antonella Ferrara, Christopher Edwards "Load Altering Attacks Detection, Reconstruction and Mitigation for Cyber-Security in Smart Grids with Battery Energy Storage Systems".

[161] Emily. M Wells, Mariel Boden, Ilana Tseytlin, Igor Linkov, "Modeling critical infrastructure resilience under compounding threats: A systematic literature review", *Progress in Disaster Science* 15 (October 2022), https://doi.org/10.1016/j.pdisas.2022.100244

i. SCADA systems

A concern that applies to the energy sector but not only is the risk related to the misuse of data and the rise of data asymmetries. Energy providers, distributors and users disclose personal energy-management data which is stored, used, and controlled in complex technical systems, which increases vulnerability to internal system failure and potentially attracts malicious actors aiming to compromise this cybersecurity[162]

In fact, information infrastructure is particularly critical when analyzing the vulnerabilities of infrastructure in the cyberspace. For instance, automation of energy systems, which is enabled by SCADA systems that control electric power grids to computerized systems. These infrastructures require information transmitted and delivered by the information infrastructures; therefore, their state will depend on outputs of the information infrastructure[163] .

As Cyber-Physical Systems (CPS) and namely the Internet of Things (IoT) are supplementing traditional CI with data-rich operations, Supervisory Control and Data Systems (SCADA) and Industrial Control Systems (ICS) play a pivotal role in controlling and managing the CI [164].

The power, gas and water sectors have historically been using SCADA systems, which serve to monitor and control geographically distributed assets. But with advancements in technology, these systems have adopted not only CPS / IoT, but also big data analytics, artificial intelligence and machine learning and cloud technology [165].

---

[162] Ibid.

[163] G. Yadav and Kolin Paul, "Architecture and security of SCADA systems: A review", *International Journal of Critical Infrastructure Protection* 34 (September 2021), https://doi.org/10.1016/j.ijcip.2021.100433

[164] Ibid.

[165] Ibid.

Some of the frameworks associated with SCADA including giving aid identification and quick alerts, warnings to the observing stations using an attested monitoring stage, advanced communications, and state-of-the-art sensors [166].
However, the initial designs of SCADA never incorporated security features because these systems were designed to work in a standalone way, relying on air-gapped networks and proprietary protocols for securing itself[167] .

Today, SCADA systems have evolved into sophisticated complex open systems connected to the Internet using advanced technology. With their association to the web, many SCADA systems work from topographically inaccessible areas, possibly leading the system to be more susceptible for attackers to target from anywhere in the world[168].

Moreover, with decentralization, the composite operational environment of energy infrastructure is now made up of complex ownership and regulatory structures and different levels of human involvement. The main levels constitute of Operation & Maintenance (O&M), monitoring and control. One of the main vulnerabilities is the increasing of entry points for potential cyber-attacks, incentivized by the increased connectivity of the grid. All the devices of a smart grid contribute to the growing attack surface, as all of them may be differently vulnerable to attacks - from advanced meters, Internet of Things (IoT), and smart grids. Examples of these entry points include the introduction of digital systems, telecommunication equipment, and sensors across the grid.

The expanded attack surface is exacerbated by decentralized energy sources, such as solar PV units, which require a greater need for automation for their management and operation. The consequence is that more the exchange of information between the DER and an energy company's distribution control system is incremented. Internet of Things (IoT) technologies often enable this communication.

---

[166] Ibid.

[167] Ibid.

[168] Ibid.

The risks of digitalization and decentralization are intertwined: the increasingly disparately located generation, transmission and distribution infrastructure creates increased assets, thus rendering digitalization a precious resource for their management, which, in turn, causes a rise of the power's sector attack surface. Here, key vulnerabilities include network and endpoint security.
Concerning the context of vulnerabilities, has become vital to address critical infrastructure protection not only in a conflict zone, but also in the context of protection and response to the so called "gray zone threats", that is, hybrid or sub-military threats that do not meet the threshold of an announced war. These can be unattributed or unannounced sabotage or acts[169] .

ii. Vulnerabilities in grid-connected renewable power systems and DERs

Renewable power systems, such as wind farm and solar farm deployments, are set to become increasingly attractive targets for malicious entities as modern society becomes more reliant on renewable energy sources[170].

Wind farms, for instance, because of the geographic scale, remoteness of assets, flat logical control networks, and insecure control protocols, expose them to myriad threats. Wind farm infrastructure comprises of wind turbines that generate electricity, each of these is connected to a step-up transformer whose power output is sent to a substation. Electricity generated by multiple turbines is collected by the substation, which steps-up the power, before injecting it into the grid[171]
Attack vectors can be leveraged to target not only its information technology, but additionally, their industrial control and physical assets[172]. Insecure SCADA protocols, for instance, expose wind farm assets to threats which can be realized by attackers to disrupt operations or damage turbines and substations, leading to significant financial losses regarding business operations - on

---

[169] N. M. Schmitt, "Peacetime Cyber Responses and Wartime Cyber Operations under International Law. An Analytical Vade Mecum", *Harvard National Security Journal* 8 (2017), https://www.scirp.org/reference/referencespapers?referenceid=2476198

[170] Jason Staggs, David Ferlemann and Sujeet Shenoi, "Wind farm security: attack surface, targets, scenarios and mitigation", *Information Journal of Critical Infrastructure Protection"* 17 (June 2017), https://doi.org/10.1016/j.ijcip.2017.03.001

[171] Ibid.

[172] Ibid.

the part of wind farm owners and operators, but mainly, the potential to disrupt the transmission of electricity, and, on a greater scale, inject disturbances into the bulk power grid[173]

Smart cities, which emerge from innovations in information technology, also pose challenges to our security, notably privacy related. With the interconnection of smart energy meters, security devices, and smart appliances, many social systems are more and more fully connected to the Internet of Things. Integrated systems are expected to aid emergency responders, in disaster recovery, and public safety. Interconnected data from GPS location to weather and traffic updates is already improving intelligent transportation. While these standards promise unprecedented improvements in the quality of life, the challenges of security and privacy are still important to address. Illegal access to information can once more cause attacks and physical disruptions in service availability[174].

Ultimately, the challenges posed by energy critical infrastructure are treated by the existing national and international legal frameworks in a fragmented manner. This leaves CI, including energy CI, vulnerable to threats, in particular the cyber kind. Approaches to govern cyber-threats to infrastructure must be included in digitalization promises: the latter is on the one hand a means to achieve economic and social development, as well as increasing environmental protection and climate change mitigation, but it is necessary for it to ensure protection against cyber-threats for future generations to meet their own needs[175].

Drawing from these vulnerabilities, cybersecurity must emerge as a player in advancing sustainable digitalization. If digitalization is considered as a growing trend in which digital technology is used to promote environmental, social, and economic sustainability, cyber threats undermine these sustainability efforts resulting in economic and social disruptions.

---

[173] Ibid.

[174] Sandra Cassotta and Roman Sidortsov, "Sustainable cybersecurity? Rethinking approaches to protecting energy infrastructure in the European High North", Energy Research & Social Sciences 51 (May 2019), https://vbn.aau.dk/en/publications/sustainable-cybersecurity-rethinking-approaches-to-protecting-ene-2

[175] Ibid.

It is pivotal to consider cyber security as an integral component of sustainable digitalization; in a multi-stakeholder approach that considers the interests of all parties involved, including governments, businesses, and individuals, and to navigate the complex challenges of integrating the cyber-dimension.

At this point fully grasp the implications of these vulnerabilities, it is crucial to examine recent cyber-attacks that have exploited similar weaknesses. By analyzing these incidents, the aim is valuable insights into the evolving threat landscape and better understand how such vulnerabilities are being targeted to our evolving critical energy infrastructures, in practice.

2.2. Case studies of Cyberattacks against Critical Energy Infrastructure

The energy sector has historically been susceptible to attacks. According to Benjamin Schmitt, Senior Fellow at the Kleinman Center for Energy Policy at the University of Pennsylvania, physical energy, and communications infrastructures threats can be traced back to the 1800s.

Notably, physical attacks had already been threatening energy security, and the pace of the low-carbon transition. In the last two years, critical European energy infrastructure was particularly hit by a growing number of physical attacks since the outbreak of the war in Ukraine. In fact, Europe has notably experienced episodes of sabotage of critical energy infrastructure, to a large extent, attacks targeting subsea electric transmission cables and natural gas pipelines, including the attack on the Nord Stream gas pipeline on September 26, 2022, the highest profile of these attacks.

As these disruptions come at a time of upheaval in the energy system, as states are pushing forward with the construction of expansive carbon-free energy infrastructure, the vulnerability of energy infrastructure concretely comes to the fore.

2.2.1. Stuxnet (2010): Zero-day-vulnerabilities attacks targeting Industrial Control Systems

One cyber-attack marked a turning point in geopolitical conflicts.

In November 2010, Iranian President Mahmoud Ahmadinejad publicly acknowledged that a computer worm "created problems for a limited number of nuclear centrifuges'[176]. The sabotage of these centrifuges was attributed to a hijacking of industrial control systems[177] . It was reported that recognition of such threats exploded even before Ahmadinejad's declaration, in June 2010, with the discovery of at least 14 industrial sites in Iran - including the uranium-enrichment plant - were infected by a 500-kilobyte computer worm.

A computer malware relies on an unknowing victim to install it; a worm, however, spreads on it often over a computer network. The worm, an unprecedented malicious piece of code, relied on three phases of attack. Firstly, it targeted Microsoft Windows machines and networks, onto which it replicated itself. Secondly, its aim was to attack Siemens Step7, a Windows-based software used to program industrial control systems, the basis behind the operation of equipment such as centrifuges [178].

[176] Kushner David, "The real story of Stuxnet. How Kaspersky Lab tracked down the malware that stymied Iran's nuclear-fuel enrichment program", IEEE Spectrum, February 26th, 2013, updated May 21st, 2024, https://spectrum.ieee.org/the-real-story-of-stuxnet

[177] Ibid.

[178] Ibid.

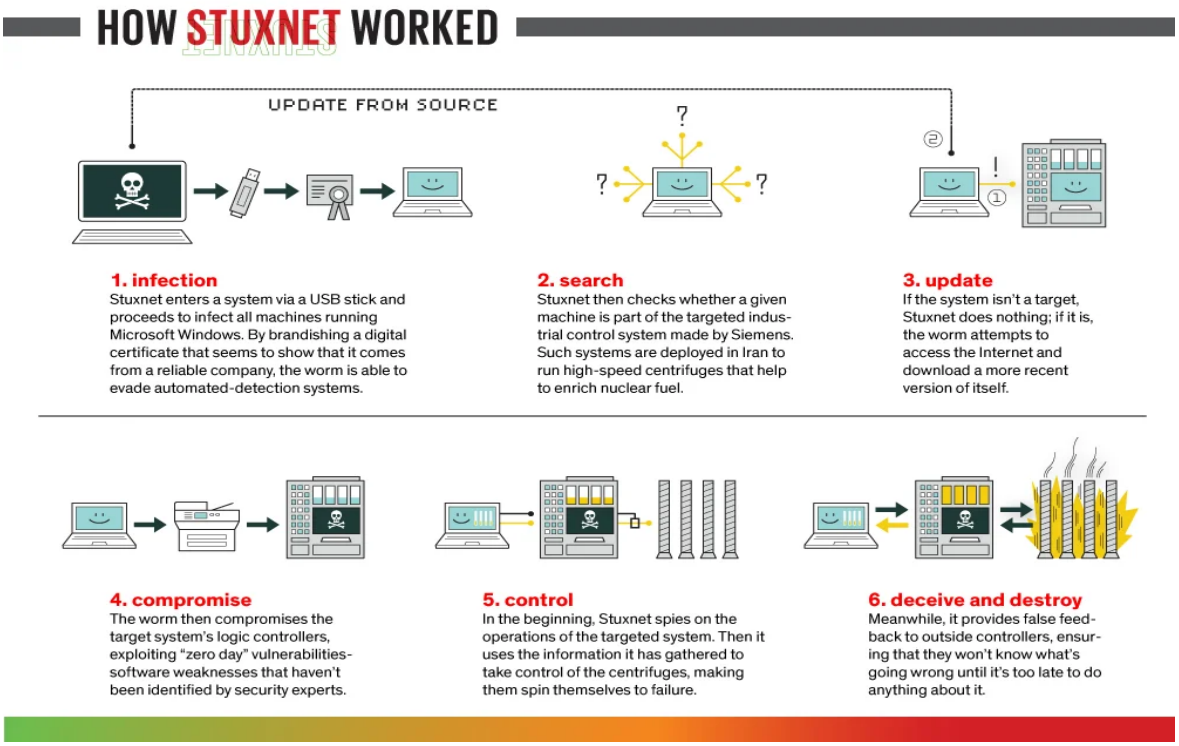


Figure 10: "How Stuxnet Worked". Source: "The Real Story of Stuxnet", IEEE Spectrum, 2024.

Computers running Windows software allowed the Stuxnet worm to spread stealthily, letting the worm proliferate over local networks[179].

Concerning the authors, these weren't officially identified. However, in its aftermath, because of its size and sophistication, the worm attack was attributed to the sponsorship of a nation-state, with experts reinforcing these affirmations. What followed particularly bolstered up these speculations: leaks to the press from officials in the United States and Israel appeared, strongly suggesting the two nations' involvement, and orchestrating of the deed[180].

[179] Kushner David, "The real story of Stuxnet. How Kaspersky Lab tracked down the malware that stymied Iran's nuclear-fuel enrichment program", IEEE Spectrum, February 26th, 2013, updated May 21st, 2024, https://spectrum.ieee.org/the-real-story-of-stuxnet

[180] Ibid.

According to Roel Schowenberg, a Senior Researcher on new technologies at the Kaspersky Lab, the Russian multinational cyber-security and anti-virus provider, the first utilizations of malware were typically the work of hackers in the 1990s[181].
Chevron, American multinational energy corporation, was the first U.S. corporation to admit that Stuxnet had spread across its machines. Declarations followed from institutional figures. U.S. Defense Secretary Leon Panetta warned about a "cyber–Pearl Harbor" that could cripple power grids, poison water supplies and derail trains, referring to the worm, in October 2012[182].Since the discovery of Stuxnet, computer-security engineers and professionals have been addressing other weaponized viruses, to name a few, Duqu, Flame and Gauss[183].

Stuxnet represents a new generation of 'fire-and-forget' malware, that is, aimed in cyberspace against selected targets. In the cases, the targets were air-gapped, in the sense that they were not connected to the public Internet. Penetrating these devices required the use of intermediary devices such as USB sticks[184].

The Stuxnet worm employed Siemens' default passwords to access Windows operating systems running the WinCC and PCS 7 programs; programmable logic controller (PLC) programs that manage industrial plants.[185]

The "geniality" of the worm is owed to the fact that it can strike and reprogram a computer target. In the case of the attack on Iranian centrifuges, Stuxnet first operated by hunting down frequency-converter drives made by Fararo Paya, Iranian manufacturing firm. Set at the very high speeds, these frequency converter drives are required by centrifuges to separate and concentrate the uranium-235 isotope for use in light-water reactors, and at higher levels of enrichment, for use as fissile material for nuclear weapons.

---

[181] Ibid.

[182] Ibid.

[183] Ibid.

[184] Ibid.

[185] Ibid.

Then, the worm alternated the frequency of the electrical current that powers the centrifuges. The centrifuges switched back and forth, between high and low speeds, at intervals for which the machines were not designed. It interfered with the speed of the motors, which sabotages the normal operation of the industrial control process, by changing the output frequencies and thus the speed of the motors, for short intervals over a period of months.

The worm in fact contains a rootkit that conceals commands downloaded from the Siemens system.

The push towards Industry 4.0, accelerating the adoption of networked technologies impacts external interfaces enabling interconnected transnational supply chain management. The utilization of USB-stick devices in manufacturing automation infrastructures is one specific use within a supply chain[186].

Was the risk related to the USB predictable and even more, fully acknowledged? Gajek et. al (2021) have argued that enterprise procedures, education of staff and rules for selecting USB-stick suppliers can only be auxiliary measures as they still rely on human behavior to identify, authenticate, and track devices in IIoT environments. A system is therefore required to execute these activities all throughout the lifecycle of the device. From an operator's viewpoint, the physical level of the hardware device must be connected to an entity in the IT level, which addresses the concept of a digital twin[187].
In this case, the risks that had to be considered were the fact that.

The USB sticks were only used within a dedicated IT infrastructure with a dedicated goal[188]. It was assured that the USB had only been used for the intended procedures on specific machines, along with the production cycle of devices Stuxnet was a zero-day-attack, meaning that it exploited

---

[186] Gajek Sebastian, Michael Lees and Christopher Jansen, "IIoT and cyber-resilience: Could blockchain have thwarted the Stuxnet attack?", AI & Society 32, no. 2 (September 2021), DOI:10.1007/s00146-020-01023-w.

[187] Ibid.

[188] Ibid.

a vulnerability that had not been disclosed. Zero-day-attacks have no defense, as, during the time that the vulnerability remains unknown, the software affected cannot be patched and anti-virus products cannot detect the attack through signature-based scanning[189].

Vulnerabilities in popular software such as Microsoft Office or Adobe Flash are a free pass for any cybercriminal, to any target they might wish to attack. In addition to Stuxnet worm, which combined zero-day-vulnerabilities to target industrial control systems, other notable attacks include the "Aurora" attack, which aimed to steal information from several companies and the 2011 attack against Saudi Arabia[190].

Moreover, it was discovered that the Stuxnet malware had impaired an air gap to compromise nearly a fifth of Iran's nuclear centrifuges. Air-gapping is a common method of bullet-proofing an Internet connected system by disconnecting it from the internet and from wireless networks[191].
How did the USB stick get infected? A question that raised infinite speculations. The virus was designed to be delivered via a removable drive like the USB stick. In response to allegations, *The Times of Israel* initially reported that an Iranian engineer recruited by the Netherlands AIVD had planted the virus in the Iranian research site himself in 2007, at the request of the CIA and the Mossad[192].

[189] Leyla Bilge, Tudor Dumitraș, "Before we knew it: an empirical study of zero-day attacks in the real world", CCS Proceedings of the 2012 ACM conference on Computer and communications security, https://doi.org/10.1145/2382196.2382284

[190] Kushner David, "The real story of Stuxnet. How Kaspersky Lab tracked down the malware that stymied Iran's nuclear-fuel enrichment program", IEEE Spectrum, February 26th, 2013, updated May 21st, 2024, https://spectrum.ieee.org/the-real-story-of-stuxnet

[191] Ibid.

[192] Ibid.

The Stuxnet malware was credited to the United States and Israel's collaborative action to cripple the Iranian nuclear program[193]. In fact, use of Stuxnet on Iranian networks was attributed to the CIA and the Mossad, who allegedly spied on a critical Iranian computer system for two years [194]. Although neither government officially acknowledged developing Stuxnet, a 2011 video, created to celebrate the Israeli of a Head of the Defenses Forces and claimed and celebrated the attack on the Iranian Nuclear Programme as on the country's best successes (Williams, 2011).

It is feared that Iran could be operating secret centrifuge facilities to produce highly enriched uranium, and Stuxnet's capabilities were to attack both known and unknown centrifuges. In fact, the more likely target is Iran's uranium-enrichment programme, and not specifically Bushehr, an unlikely target because the plutonium produced by such light-water reactors is not well suited for weapons purposes[195]. Iran confirmed that Stuxnet infected personal computers while denying that much damage was infected.

Examples of scenarios that would be caused using similar malware include the crippling of water supplies, power plants, banks - the very infrastructure that once seemed invulnerable to attack[196].

2.2.2. Shamoon and the Attack to Saudi Aramco (2012): The Wiper Virus

On 15 August 2012, Saudi's Arabia national oil and gas firm, Aramco, suffered a cyber-attack for which it took two years to recover from, according to reports[197].

Precisely, a self-replicating virus that infected as many as 30,000 of its Windows Based machines struck its computer network.

---

[193] Kushner David, "The real story of Stuxnet. How Kaspersky Lab tracked down the malware that stymied Iran's nuclear-fuel enrichment program", IEEE Spectrum, February 26th, 2013, updated May 21st, 2024, https://spectrum.ieee.org/the-real-story-of-stuxnet

[194] Ibid.

[195] Ibid.

[196] Ibid.

[197] Christopher Bronk and Eneken Tikk-Ringas, "The Cyber Attack on Saudi Aramco", *Survival. Global Politics and Strategy* 55, no. 2 (2013), https://doi.org/10.1080/00396338.2013.784468

The attack was considered as “alarming because of its scale” and for the way it was carried out against a company so critical to global energy markets and owned by the world’s largest oil producer. The disruption caused was significant[198]. It was reported that the virus was made specifically for cyber-espionage in the energy sector[199]. Many computers were shut off because the day of the attack occurred on an Islamic holiday when many employees were on vacation[200].

Shamoon also spread to the networks of other oil and gas firms, including RasGas 2 Conventional Gas Field in Qatar, operated by QatarEnergy LNG.

The main functions of Shamoon were the indiscriminate deletion of data from computer hard drives[201]. It worked by focusing on user files, configuration files, and system data[202]. Symantec stated that Shamoon consisted of the following components, three “modules”, that allowed the creators of the virus to delete files on randomly selected Aramco computers. The way it operated was through the following modules:

1. A Dropper, the source of the original infection, and the main component.
2. A Wiper, the model that destroys data on the infected computer,
3. A Reporter, which sends information back to the attacker.

The malware stole passwords, wiped data, and prevented computers from rebooting[203].
The attack was claimed by hackers who called themselves the “Cutting Sword of Justice". They claimed the attack as a retaliation against the Saudi al-Saud regime for what the group called

[198] Ibid.

[199] Alaa Alsaaed, “The Cyber Attack on Saudi Aramco in 2012”, *Asian Journal of Engineering and Technology* 10, no. 2 (2021), https://doi.org/10.51983/ajeat-2021.10.2.3057

[200] Christopher Bronk and Eneken Tikk-Ringas, “The Cyber Attack on Saudi Aramco”.

[201] Ibid.

[202] Ibid.

[203] Ibid.

widespread crimes against attack[204]. Shamoon was designed to activate at a certain time, overwriting files and displaying a partial image of the American flag[205].

The attack was also attributed to Iran by the U.S. intelligence sources, in relation to the RasGas attack that had occurred less than two weeks after Aramco, leaving the Qatari gas giant RasGas knocked offline by suspected state-sponsored attackers.

It could have signaled Iran's growing cyber-capabilities and the country's willingness to use them to promote its interests, particularly in its battle of influence in the Middle East, or as a possible response to a previous attack against the Iranian Oil Ministry and the National Iranian Oil Company that employed a malware called Wiper[206].

Shamoon was allegedly linked to Wiper, though researchers from Russia-based Kaspersky Lab assured the file and services from the original Wiper weren't present in Shamoon; as a result, the two pieces of malware were deemed likely not connected[207].

The virus was released from one of the workstations on the company's internal networks. It was released into the networks of the company. A 900KB PE malware file contained several encrypted resources, the virus rendered the infected computers unusable: Shamoon erased the data on the hard drives and overwriting, that is, replacing, them with an image of the burning American flag, and then reported the addresses of infected computers back to a computer inside the company's networks[208].

---

[204] Ibid.

[205] Ibid.

[206] Alaa Alsaaed, "The Cyber Attack on Saudi Aramco in 2012", Asian Journal of Engineering and Technology 10, no. 2 (2021), https://doi.org/10.51983/ajeat-2021.10.2.3057

[207] Ibid.

[208] Ibid.

The specific network compromise methods leading to the attacks have remained unclear in the reported case. Yet, Shamoon's attack life cycle has been researched by X-Force Incident Response and Intelligence Service, a group of experts that specialize in breach investigations across the public and private sectors[209], who have claimed that actor(s)' entry point to compromise the data was a document containing a malicious macro that, when approved to execute, enabled C2 communications to the attacker's server, built to leverage PowerShell - a scripting language and a command-line executor developed by Microsoft to manage and automate administrative tasks for administrations[210]. As such, they established their first foothold and subsequent operations[211].

1. "Attackers send a spear phishing email to employees at the target organization. The email contains a Microsoft Office document as an attachment.
2. Opening the attachment from the email invokes PowerShell and enables command line access to the compromised machine.
3. Attackers can now communicate with the compromised machine and remotely execute commands on it.
4. The attackers use their access to deploy additional tools and malware to other endpoints or escalate privileges in the network.
5. Attackers study the network by connecting to additional systems and locating critical servers.
6. The attackers deploy the Shamoon malware.
7. A coordinated Shamoon outbreak begins and computer hard drives across the organization are permanently wiped."

The deletion of data had a destructive payload on the company, leaving the affected machines inoperable and paralyzing Aramco's operations. Nearly 85% of all the IT systems were knocked out, a damage that wasn't confined to desktop computers, it encompassed critical infrastructure

---

[209] Christopher Bronk and Eneken Tikk-Ringas, "The Cyber Attack on Saudi Aramco".

[210] Ibid.

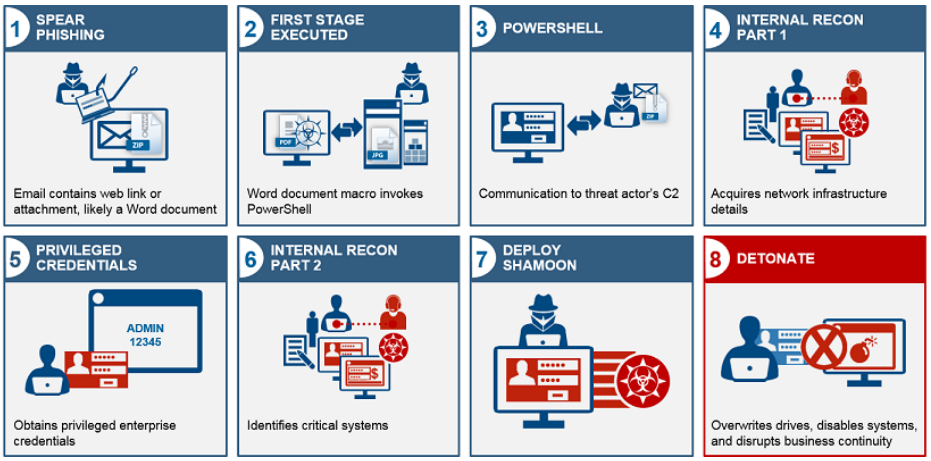
[211] Kevin Albano and Limor Kessem, "The Full Shamoon: How the Devastating Malware Was Inserted Into Networks", Security Intelligence, February 15th, 2017, https://securityintelligence.com/the-full-shamoon-how-the-devastating-malware-was-inserted-into-networks/

such as servers, payroll systems, research and development data, databases, causing disruption on all facets of their businesses[212]

It can be said that the costs were both tangible and intangible and served as a stark reminder of the potential consequences of cyber threats to critical infrastructure[213].

No official attribution has been made, yet several cybersecurity experts and government officials claimed Iran-sponsored actors had been behind the attacks, with geopolitical thought to be political in nature and possibly, as mentioned, as retaliation for previous attacks[214].

The attack did not result in an oil spill, nor an explosion or other major fault of the company's operations. However, it caused negative consequences to its business processes, and most likely, a loss of drilling and production data[215]: Shamoon ensured destroyed data could never be recovered, an unusual if not rare feature in targeted attacks[216].



[212] Ibid.

[213] Ibid.

[214] Ibid.

[215] Christopher Bronk and Eneken Tikk-Ringas, "The Cyber Attack on Saudi Aramco".

[216] Ibid.

Figure 11: "Attack chain for the Shamoon malware". Source: IBM, 2017.

2.2.3. Black Energy and Industroyer: Ukraine Power Grid Hacks (2015 and 2016).

On December 23, 2015, a third-party illegally entered the computer and SCADA systems of Kyivoblenergo, a Ukrainian regional electricity distribution company. Seven 110kV and 23 35kV substations were disconnected for three hours. Soon later, the company reported service outages to its customers. Initially, the outages were reportedly thought to affect approximately 80,000 customers, yet it was later revealed that as three different distribution energy companies (oblenergos) were attacked, several outages followed causing approximately 225,000 customers to lose power across various areas[217].

The incident is referred to as the 2015 Ukrainian Power Grid Attack. The attack was attributed to the BlackEnergy trojan malware, which successfully sabotaged different electricity distributors.[218] A specific group of BlackEnergy attackers began implementing SCADA-related plugins for victims in industrial control systems (ICS) and energy markets worldwide. Kaspersky assured that BlackEnergy demonstrated a unique skill set, far above the average master Denial of Service. The malware evolved from a simple Trojan, aimed at executing denials of service, to an advanced persistent threat (APT)[219].

Following the attack, Ukrainian government officials denounced Russian security services for the incident claiming a state-sponsored cyber-attack caused the outages[220].

BlackEnergy is therefore a malware designed to automate criminal activities and was first acknowledged in 2007, starting as web-based Distributed Denial of Service (DDoS): sophisticated

---

[217] CESER, "CyOTE Case Study: Crashoverride/Industroyer", February 7th, 2022, https://cyote.inl.gov/cyote/wp-content/uploads/2022/11/CRASHOVERRIDE-CyOTE-Case-Study_508_FINAL.pdf

[218] Ibid.

[219] Ibid.

[220] Ibid.

malware then supported, in the following years, various plugins that undermine system resources[221].

According to a review study by, these were the steps undertaken by the attack:

1. Spear-phishing targeting campaign. This represented the initial foothold for launching the malware as it targeted the system administrators at local utility companies. Pretending to be either government or legitimate vendors, the attackers embedded the malware in emails with Microsoft Word and PowerPoint attachments,
2. Installation of a malicious program to deliver the malware in the local application data. The program replaced disable drivers with the malicious, causing a system restart,
3. Removal of the cautionary test watermark. The malware attested itself by self-signature, which means that bypassed protective authentication mechanism of User Access Control (UAC). Digital watermarking is a process of obtaining a digital watermarked file by embedding hidden information[222]. The malware used the TESTSIGNING feature by Microsoft.
4. Installation of Remote Access Tools (RATs) to create a backdoor, after gaining access to the system. The attacks communicated with the Command-and-Control Server (C&C).
5. Installation of a malware called "KillDisk" on the infected endpins. This was the malware that could overwrite most of the files and corrupt the master boot record to render the system unbootable.
6. Accessing the VPN credentials to gain access to the remote system in the operation technology (OT) environment, including workstations, servers, and HMIs.
7. Infiltration of the Operational Technology (OT) layer, allowing to carefully plan and coordinate a wide-scale attack on all the infected power stations.
8. Launching a DDoS attack on the telephone systems in the region to delay reporting.
9. Gaining remote access to the control room systems, disabling power supply, and applying a firmware update to disable communication[223].

---

[221] Gupta Krishna Kumar et. al, "The role of cyber security in advancing sustainable digitalization: Opportunities and challenges", *Journal of Decision Analytics and Intelligent Computing* 3, no. 1, DOI: 10.31181/jdaic10018122023g.
[222] Ibid.

[223] Gupta Krishna Kumar et. al, "The role of cyber security in advancing sustainable digitalization: Opportunities and challenges", *Journal of Decision Analytics and Intelligent Computing* 3, no. 1, DOI: 10.31181/jdaic10018122023g.

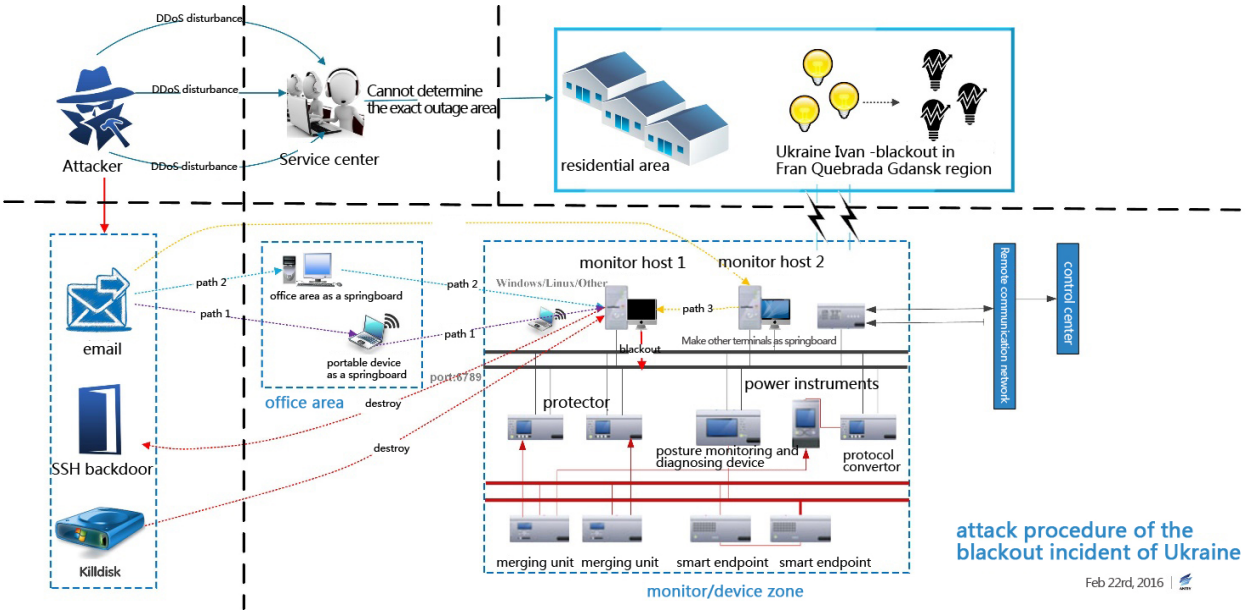


Figure 12: "Attack procedure of the blackout incident of Ukraine". Source: Antiy Labs, 2016

In December of the following year, one-fifth of Kyiv's citizens were plunged into darkness as the result of a blackout caused by malware to autonomy target the capital city's power grid[224].

The multi-component malware was known as Industroyer (also known as CrashOverride), the first malware ever seen to have been specifically designed to attack power grids. It disrupted the working processes of industrial control systems, especially those in electrical substations.[225]

Industroyer/Crash Override, like BlackEnergy, was designed to infiltrate data, that is, an objective that is not tied to cyberespionage but to cause damage. A module worked to remove data and override the Industrial Control System configurations (ICS) which rendered it unusable[226].

[224] Kaspersky, "ATT&CK for ICS: Industroyer". Accessed August 30th, 2024, https://www.kaspersky.com/enterprise-security/mitre/industroyer

[225] Kaspersky, "What's the Difference between a Virus and a Worm?". Accessed August 30th, 2024, https://www.kaspersky.com/resource-center/threats/computer-viruses-vs-worms

[226] Marie Baezner and Patrice Robin, "Stuxnet", CSS Cyber Defense Project, ETH Zurich (February 2018), https://www.researchgate.net/publication/323199431_Stuxnet

What the two attacks signified was that the alleged Russian attacker demonstrated a robust understanding of the physical industrial process.

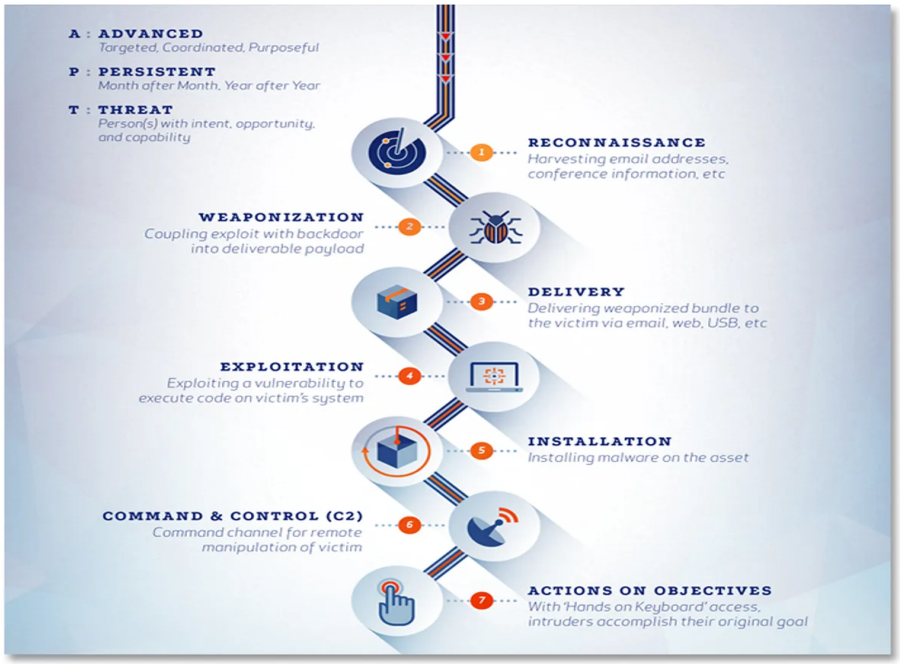


Figure 13: "The Cyber Kill Chain". Source: Zdnet, 2016.

2.3. Taxonomy of cyber-attacks for New Energy Infrastructure

The case studies reveal that creating a taxonomy of cyberattacks is possible, as it could help identify which types of new critical energy infrastructure are most vulnerable to various types of attacks.

Cyber threats can take a variety of forms. In 2022, 10.7% of observed cyber-attacks targeted the energy sector, but according to a report from cybersecurity asset intelligence firm Armis, the utilities sector saw an increase in cyberattacks of over 200% in 2023, making it the most at-risk industry, followed by manufacturing (which saw a 165% increase)[227].

[227] Cybersecurity & Infrastructure Security Agency, "Critical Infrastructure Sectors". Accessed August 20th, 2024, https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

Diverse types of cyber-attacks focus on different sections of the value chain. Cyberattacks allow unauthorized users to compromise the confidentiality, integrity, or availability of sensitive information[228]. As it has been explored, preventing these compromises is becoming increasingly information in the face of the growth in Internet use.
The skill level of attackers and the technological advances in their tools and methods of attacks is increasing[229].

2.3.1. Malware

Defined as the most widely used cyber security threats, malware is constantly tailored to industrial control systems[230].

Malware, short for malicious software, refers to any software intentionally designed to cause damage to a computer, server, client, or network. Malware can take various forms, including viruses, worms, Trojans, ransomware, spyware, and more. When malware targets critical energy infrastructure, the consequences can be severe, affecting not just digital systems but also physical operations and safety.

Virus are computer programs that spread by first infecting files or the system areas of a computer or network's router hard drive, and then make copies of themselves. When malicious, they have the potential to damage or destroy data files Viruses are primarily spread through email messages, they in fact require user action - as opening an email attachment or visiting a malicious web page - to spread[231].

According to CISCO, worms are more serious than a virus because once it infects a vulnerable machine, they can self-replicate and spread automatically across multiple devices. As mentioned,

---

[228] Cybersecurity & Infrastructure Security Agency, "Critical Infrastructure Sectors". Accessed August 20th, 2024, https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

[229] Ibid.

[230] Ibid.

[231] Ibid.

a worm is not a virus, but it can severely disrupt IT operations and cause data loss. Worms infect machines by taking advantage of software vulnerabilities. They use social engineering to get users to think the malicious files are safe to open; but as it has been demonstrated, likely by Stuxnet, removable drives like USB drives can also deliver worms [232]

The main difference lies in the fact that a virus cannot self-replicate, and it needs to be sent by a user or a software to travel between two different computers, whereas a worm can replicate and spread itself from one computer to another. A worm is a greater threat when the network consists of many computers connected to each other in a ring formation, the same could be said of a network set up in a hub formation with a server in the middle that serves all the computers in the network particularly if the server does not have adequate anti malware defenses [233]

When a virus is introduced to an unprotected network, users will still have to send the virus to each other and then open the file for each computer in the network to get infected. A worm, once introduced in the computer, can replicate itself and spread to other computers in the network.

Concerning how these two-malware spread, worms often exploit network configuration errors or security loopholes in the operating system (OS) or applications. There are multiple methods to spread across networks and these include - email attachments, external drives, downloads [234].

Ransomware is a specific type of malware which prevents use of the system or equipment it infects. Once the computer or system is infected and hijacked, the information is encrypted and the screen

---

[232] CISCO, "What Is a Worm?". Accessed August 30th, 2024, https://www.cisco.com/c/en/us/products/security/what-is-a-worm.html#:~:text=A%20worm%20is%20a%20type,files%20or%20introduce%20other%20malware

[233] Fortinet, "Malware vs Viruses vs Worms". Accessed August 30th, 2024, https://www.fortinet.com/resources/cyberglossary/malware-vs-virus-vs-worm#:~:text=What%20is%20the%20difference%20between%20a%20virus%20and%20a%20worm,a%20user%20or%20via%20software

[234] Kaspersky, "What's the Difference between a Virus and a Worm?". Accessed August 30th, 2024, https://www.kaspersky.com/resource-center/threats/computer-viruses-vs-worms

is blocked, cutting the user from their data. The latter becomes a victim of extortion, being asked for a ransom in exchange for recovering the normal functioning of the device or system[235].

Trojans are a type of malware often distinguished as legitimate software. Once more, with the employment of social engineering techniques, users are typically tricked into opening them and loading - and therefore executing - Trojans on their systems[236].

Finally, spywares are vastly defined as a malicious software designed to enter a computer device, gather data about its users and forward it to a third-party without the user's consent[237].

2.3.3. Social Engineering

Social engineering refers to malicious activities accomplished through human interactions, precisely, psychological manipulation aimed at tricking users into making security mistakes or giving away sensitive information [238]

The first step to a social engineering attack involves the investigation on behalf of the perpetrator on the intended victim to gather necessary background information which shall serve as potential points of entry and weak security protocols. The attacker then moves to gain the victim's trust, providing stimuli for subsequent actions that break security practices [239]

---

[235] Banco Santander, "Ransomware". Accessed August 30th, 2024, https://www.bancosantander.es/en/glosario/ransomware

[236] Mohammed Reza Faghani and Uyen Trang Nguyen, "A Study of Malware Propagation via Online Social Networking" in *Mining Social Networks and Security Informatics* (eds. Tansel Özyer et. al) (Springer: New York, 2013), https://link.springer.com/chapter/10.1007/978-94-007-6359-3_13

[237] Kaspersky, "What's the Difference between a Virus and a Worm?". Accessed August 30th, 2024, https://www.kaspersky.com/resource-center/threats/computer-viruses-vs-worms

[238] Imperva, "Social Engineering". Accessed August 21st, 2024, https://www.imperva.com/learn/application-security/social-engineering-attack/,

[239] Imperva, "Social Engineering". Accessed August 21st, 2024, https://www.imperva.com/learn/application-security/social-engineering-attack/

These might involve revealing sensitive information or granting access to critical resources, and data, such as program protocols. Social engineering's threat lies in its reliance on human error, exploited rather than the vulnerabilities found in software and operating systems[240].

As such, the mistakes made by legitimate users are less predictable and consequently harder to identify and thwart in a malware-based intrusion. The most common forms of social engineering attacks, which can be performed anywhere where human interaction is involved are baiting, scareware, pretexting, phishing, spear phishing[241].

Attackers who chose the baiting technique will use a false promise to pique a victim's curiosity, luring the users into a trap that may steal their personal information or inflict their systems with malware. Baiting exists both in the physical world - through the insertion of USB sticks, to be picked out by the user, and in its online forms, through enticing ads leading to malicious sites or encouraging users to download a malware-infected application[242]-
With scareware, attacks target victims with false threats and alarms, which trick them into thinking their system is infected with malware and prompts them to install software which carries the malware itself. It also goes by the name of deception software, rogue scanner software and fraudware[243].

Pretexting involves an attacker pretending to need sensitive information from a victim to perform a critical task, therefore, obtaining information through a series of cleverly crafted lies. Pretexting involves the attacker establishing some form of trust with their victim, usually done through the impersonation of co-workers, police, bank and tax officials, or other individuals with right-to-know authority[244].

---

[240] Ibid.

[241] Ibid.

[242] Ibid.

[243] Ibid.

[244] Ibid.

Finally, as one of the most popular social engineering attack types, phishing scams involve email and text message campaigns aimed at creating a sense of curiosity, fear, or urgency in victims, prodding them into revealing sensitive information, clicking on links to malicious websites, or opening attachments containing malware. Whereas spear phishing involves a more targeted version of the phishing scam whereby the attacker chooses specific individuals or enterprises, and tailor their messages based on the victim's individual characteristics to make their attack less conspicuous[245].

2.3.4. Blockchain-related cyber risks

The combination of novel cryptographic methods and blockchains are tools that can ensure that the digital revolution remains secure. Blockchains offer decentralized digital records that allow both data integrity and transparency. But these have the potential to provide an unprecedented level of privacy[246].

A blockchain is defined as a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network[247]. Virtually, anything of value can be tracked and traded on a blockchain network, reducing risk, and cutting costs for all involved.

Assets can be tangible, like a house, car cash or land, or intangible, as intellectual property, patents, copyrights, and branding.

Blockchain is believed to be a key tool to speed up the process of decarbonizing the economy as it makes transactions traceable, secure, and quick, and enhances the supply of green energy, making it more efficient, flexible, and transparent[248]. Not only is it the world's second-best

---

[245] Ibid.

[246] Andrei Manea, "Enhancing cyber security in the energy transition", DNV (February 2023), https://www.dnv.com/article/enhancing-cyber-security-in-the-energy-transition-249155/

[247] IBM, "What is blockchain?". Accessed on August 21st, 2024, https://www.ibm.com/topics/blockchain

[248] Iberdrola, "How can blockchain be used to certify the source of green energy?". Accessed August 21st, 2024, https://www.iberdrola.com/innovation/blockchain-

investment in R&D with an investment of EUR 2 billion in the last decade; but also, renewable energy companies are starting to employ the technology worldwide. For instance, blockchain is one of the pillars of the digital transformation strategy of Spanish Iberdrola[249]. In 2018, Endesa and Gas Natural Fenosa became the first companies on the Iberian Peninsula to buy and sell energy using blockchain technology[250].

According to Enel, blockchain is a "technology that could change the energy industry". Blockchain technology - through Bitcoin virtual currently enables a decentralized ledger technology. As such, transactions between two parties that normally require a third party (institutions such as banks, lawyers, and utilities) will not require the latter. In the renewable energy industry and energy transactions, it will let people trade energy amongst themselves. It is expected to create a bigger push towards more renewable energy projects as wind, solar, and hydro producers can easily connect, directly, with investors[251].

With blockchain, transactions are recorded across multiple computers. In this way, the data can only be modified once the participants in the network reach consensus. In the energy sector, this means that once the data is recorded, it remains transparent and immutable, providing stakeholders confidence in the authenticity of the data, since, with the interconnection of smart grids, an increasing amount of data is generated, ranging from consumer energy usage patterns to real-time supply metrics. Blockchain also enables a simpler trade system between users, because of more advantage costs and speed of transactions, incentivizing *prosumers* to be flexible, to use their decentralized energy resources to maintain the balance between generation and demand, to relieve congestion on the network[252].

---

energy#:~:text=We%20believe%20blockchain%20is%20a,consumption%20of%20100%20%25%20renewable%20energy

[249] Ibid.

[250] Enel, "Blockchain, a permanent revolution", February 7th, 2018, https://www.enel.com/company/stories/articles/2018/02/blockchain-energy-focus-on-santiago-chile

[251] The Renewable Energy Institute, "Blockchain for the Renewable Energy Industry". Accessed August 21st, 2024, https://www.renewableinstitute.org/blockchain-for-the-renewable-energy-industry/

[252] Andrei Manea, "Enhancing cyber security in the energy transition", DNV (February 2023), https://www.dnv.com/article/enhancing-cyber-security-in-the-energy-transition-249155/

An important challenge in this regard is data security. Prosumers' energy data becomes a crucial component of the system, as they are increasingly active in these markets. The challenge cybersecurity wise is ensuring that their data remains private, still functional within the market dynamics[253].

Hackers may threaten blockchains in four primary ways, phishing, routing, Sybil, and51% attacks.[254]

Routing happens when attackers intercept data as it's being transferred to internet service providers, since blockchains rely on real-time, large data transfers. In a Sybil attack, hackers create and use many false network identities to flood the network and crash the system. The main goal on a blockchain network is to gain disproportionate influence over decisions made in the network[255]. Finally, a 51% attack occurs when malicious cryptocurrency miners take control of tokens' blockchain[256].

Blockchain security deserves a special position in security policies as blockchain itself is being a catalyst for positive changes in the renewable energy landscape, covering issues related to supply chain management and green investment decision-making[257].

---

[253] Ibid.

[254] IBM, "What is blockchain security?". Accessed August 21st, 2024, https://www.ibm.com/topics/blockchain-security#:~:text=In%20a%20routing%20attack%2C%20blockchain,extracted%20confidential%20data%20or%20currencies.&text=In%20a%20Sybil%20attack%2C%20hackers,network%20and%20crash%20the%20system

[255] Imperva, "Sybil Attack". Accessed August 22th, 2024, https://www.imperva.com/learn/application-security/sybil-attack/#:~:text=A%20Sybil%20attack%20uses%20a,of%20influence%20in%20the%20network

[256] Ibid.

[257] Hamed Taherdoost, "Blockchain Integration and Its Impact on Renewable Energy", *Computers* 13, no. 4 (2024), https://doi.org/10.3390/computers13040107

Blockchain has additionally been used in supply management of critical minerals, to track them throughout international supply chains[258]. As it sits at the convergence of information technology and operational technologies, mining organizations are digital by default. Every asset owned or used by an organization represents another node in the network, which renders the attack surface larger[259].

2.3.5. Manipulation of Artificial Intelligence

AI systems have permeated modern society[260].

AI is a driver of digitalization, now operating in a multitude of capacities, from driving vehicles, interacting with customers as online chatbots, helping doctors diagnose illnesses[261]. Because of its predictive capabilities, AI is revolutionizing the energy industry[262].

AI performs its tasks thanks to the training it has received on vast quantities of data. For instance, autonomous vehicles might be shown images of highways and streets with road signs, chatbots based on a large language model (LLM) might be exposed to record online conversations, data that helps AI predict how to respond in each situation[263]. Data can be processed to optimize production, supply chains, delivery systems, and to identify equipment failures, among other things. Its powerful algorithms are also capable of predicting high-stress and peak demand periods.

---

[258] IEA, "Blockchain Pilot Grants: Critical minerals". Last updated December 12th, 2023. Available at: https://www.iea.org/policies/16651-blockchain-pilot-grants-critical-minerals

[259] Paul Mitchell and Clement Soh, "Cybersecurity in Energy and resources", EY. Accessed August 21st, 2024, https://www.ey.com/en_gl/industries/energy-resources/mining-metals-cybersecurity

[260] Berenice Boutin, "State Responsibility in Relation to Military Applications of Artificial Intelligence", *Leiden Journal of International Law* (2022), https://ssrn.com/abstract=4214292

[261] Ibid.

[262] Ariel Cohen, "The Promise and Peril of AI in the Energy Sector", Forbes, July 3, 2023. Available at https://www.forbes.com/sites/arielcohen/2023/06/29/the-promise-and-peril-of-ai-in-energy/

[263] Tanveer Ahmad et. al, "Artificial intelligence in sustainable energy industry: Status Quo, challenges and opportunities", *Journal of Cleaner Production* 289 (March 2021), https://doi.org/10.1016/j.jclepro.2021.125834

As the energy sector is evolving into a decentralized and diverse landscape, AI emerges as a vital tool to navigate this new frontier[264].

The deliberate manipulation of artificial intelligence (AI) systems and machine learning (ML) to make them malfunction is an equally disruptive vulnerability. There already exists attack technologies and methodologies that consider all types of AI systems[265]. Issues in fact arise when the data itself is not trustworthy.

Malicious actors may corrupt the data, both during an AI's system's training period and afterward[266]. Protecting AI from misdirection still knows no foolproof way in part because of the datasets used to train an AI, being far too large for people to successfully monitor and filter. Four AI attacks have been identified:

1. Evasion attacks: these are attacks that occur after the deployment of an AI system. They use adversarial input data - which may look indistinguishable from regular data from human - to produce a desired model or counter the wishes of the model creator[267]. Their attempt is to alter an input to change how the system responds to it. Examples outside of the energy sector would include adding markings to stop signs; to make an autonomous vehicle misinterpret them as speed limit signs; or create confusing lane markings that would drive the vehicle to veer off the road. Smart meters using AI, which provides data to monitor and manage energy usage, in businesses and in homes, the data reported by these meters may altered to create a false picture of energy consumption, for instance, leading to incorrect billing and distorted energy demand forecasts, in a carefully engineered

---

[264] Ariel Cohen, "The Promise and Peril of AI in the Energy Sector", Forbes, July 3, 2023. Available at https://www.forbes.com/sites/arielcohen/2023/06/29/the-promise-and-peril-of-ai-in-energy/.

[265] Tanveer Ahmad et. al, "Artificial intelligence in sustainable energy industry: Status Quo, challenges and opportunities", *Journal of Cleaner Production* 289 (March 2021), https://doi.org/10.1016/j.jclepro.2021.125834

[266] CESER, *Potential Benefits and Risks of Artificial Intelligence for Critical Energy Infrastructure* (April 2024), https://www.energy.gov/sites/default/files/2024-04/DOE%20CESER_EO14110-AI%20Report%20Summary_4-26-24.pdf

[267] CESER, *Potential Benefits and Risks of Artificial Intelligencce for Critical Energy Infrastructure* (April 2024), https://www.energy.gov/sites/default/files/2024-04/DOE%20CESER_EO14110-AI%20Report%20Summary_4-26-24.pdf

manner that would cause the model - trained to predict energy market prices - to incorrectly overestimate or underestimate prices which in turn can affect the energy supply chain.[268]

2. Poisoning attacks: these attacks occur in the training phase, by introducing corrupted data[269]. Poisoning attacks add, modify, or even alter the data used to train an artificial intelligence model, forcing it to learn the wrong behavior. For instance, an attacker may modify data on energy system operations, so that a model develops an incorrect conception of what "normal operations" look like[270]- for instance, "poisoned" training data would bring the model meant to detect physical wear in energy equipment to never declare such equipment to need maintenance.
3. Privacy attacks: these occur during deployment. They represent attempts to learn sensitive information about or the data that trained the AI, to misuse it.
4. Abuse attacks: these involve inserting incorrect information into a source - such as a web page or online document - which the AI then absorbs. Abuse attacks attempt to give the AI incorrect pieces of information from a legitimate but compromised source, with the goal of repurposing the AI system's intended use.[271]

AI renders the energy system most vulnerable because most of these attacks are easy to mount. In fact, they require minimum knowledge of the AI system and limited adversarial capabilities. Controlling only a few dozen training samples (per sé, a very small percentage of the entire training set), would be enough to mount a poisoning attack[272].

---

[268] Ibid.

[269] Berenice Boutin, "State Responsibility in Relation to Military Applications of Artificial Intelligence", *Leiden Journal of International Law* (2022), https://ssrn.com/abstract=4214292

[270] CESER, *Potential Benefits and Risks of Artificial Intelligencce for Critical Energy Infrastructure* (April 2024), https://www.energy.gov/sites/default/files/2024-04/DOE%20CESER_EO14110-AI%20Report%20Summary_4-26-24.pdf

[271] Ibid.

[272] Ibid.

2.3.5. Man-in-the-Middle Attacks and Denial of Service Attacks

In a man in the middle attack, the attacker positions themselves in a conversation between a user and an application. The aim is to eavesdrop or to impersonate one of the parties, making it appear as if a normal exchange of information is underway[273].

Man-in-the Middle can occur through email hijacking, for instance, if cyber criminals take control of the email accounts of trusted companies and institutions that access to sensitive data and funds, through Wi-Fi eavesdropping, that is, when cyber criminals get victims to connect to a nearby wireless network with a legitimate-sounding name which in reality is a network set up to engage in malicious activity, through Domain Name System (DNS) spoofing, also known as DNS cache poisoning, which occur when manipulated DNS records are used to divert legitimate online traffic to a fake or spoofed website. The latter is built to resemble a website that the user would most likely know and trust, among other techniques.

Though not the same attack, MITM can be used as part of a Denial-of-Service (DoS) attack, which sees an attacker seeking to make a machine or network resource unavailable to its intended users through the temporarily or indefinite disruption of services of a host connected to a network[274]. In its simple form, a Denial-of-service (DoS) attack occurs when legitimate users are unable to access information systems, devices, or other network resources, due to the actions of a malicious cyber threat actor[275].

A distributed denial of service (DDos) attack is a *form* of DoS attack originating from more than one source[276].

---

[273] Imperva, "Man in the middle attack". Accessed August 30th, 2024, https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/

[274] Fortinet, "Man-in-the-Middle Attack: Types and Examples". Accessed August 28th, 2024, https://www.fortinet.com/resources/cyberglossary/man-in-the-middle-attack

[275]

[276] National Cyber Security Center UK, "Denial of service (DoS) guidance". Accessed August 30th, 2024, https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection

2.3.5. Cyber-Physical Attacks: The Future of Warfare?

The real threats ultimately stem from cyberwarfare, hybrid conflict, and cyber-physical attacks, which wield impacts across human security from both a national and global perspective. Is it possible to make near-term predictions about the future of cyberwarfare?[277]

It is argued that computer hacking is becoming more widespread and dangerous, if the most damaging attacks were seen as DoS attacks, large-scale ransomware attacks targeting critical infrastructure operators and public institutions are more common[278].

The inclusion of physical infrastructure - such as power plants - is proof that the targets of opportunity exploited by cyberattacks have expanded. Stuxnet represented the first major cyber-physical attack, as a combination of malware, denial-to-service, and, to a final extent, the disruption of the centrifuges. The two separate attacks on Ukraine's power grid in December 2015 and December 2016 represented, perhaps, the largest cyber physical attacks to date, demonstrating the power and precision of the alleged Russian military cyber war machine[279].

A new trend causing uncertainties concerns the flourishing and now widespread use of artificial intelligence, which, once through the hands of hackers could signal, we are entering the era of the cyber-physical attack. These attacks are those which have the largest potential to directly disrupt critical energy infrastructure, while the main vulnerable elements exploited in the previously mentioned attack types represent energy companies, institutions, service providers, producers, and individuals[280].

---

[277] Studebaker Defense Group, "The Impact of Cyberwarfare in National and Global Human Security" (2024), https://www.studebaker.group/the-impact-of-cyber-physical-warfare-in-national-and-global-human-security/

[278] Studebaker Defense Group, "The Impact of Cyberwarfare in National and Global Human Security" (2024), https://www.studebaker.group/the-impact-of-cyber-physical-warfare-in-national-and-global-human-security/

[279] Studebaker Defense Group, "The Impact of Cyberwarfare in National and Global Human Security" (2024), https://www.studebaker.group/the-impact-of-cyber-physical-warfare-in-national-and-global-human-security/

[280] Kevin Williams, "'Cyber-physical attacks' fueled by AI are a growing threat, experts say", CNBC. March 2rd, 2024, https://www.cnbc.com/2024/03/03/cyber-physical-attacks-fueled-by-ai-are-a-growing-threat-experts-say.html

The cyber-physical nexus has in fact been studied and continues being so, as concerns about physical attacks being the next phase of cybercrime keep growing. Laboratories such as the MIT lab for Cybersecurity at MIT Sloan (CAMS) led by engineering systems professor Stuart Madnick has already simulated cyberattacks in the lab, by hacking computer-controlled motors with pumps and make them incinerate, resulting in explosions[281].

Pressure values to jam, circuits to be circumvented, gauges to malfunction, these are outcomes that would have far-reaching consequences, far more than simply taking the system offline for a while, as it is done by a typical cyber-attack[282].

2.4. Categories of Actors and Motivations

Attributing attacks can be challenging in cyberspace, both due to technical factors and a lack of agreement on basic definitions, namely, on what constitutes an attack or what counts as critical infrastructure[283].

Uncertainties lie around the fact if perpetrators are acting for themselves or as agents of another entity. In current warfare, non-state actors can readily acquire the ability to conduct cyber-attacks, state and non-state actors are more and more attacking other states, businesses, outside and inside of their territories, holding a government responsible even for attacks originating within its borders, proves a difficult task[284].

2.4. States and state-sponsored groups

The belief that cybers warfare is not a viable tool for war is outdated and shortsighted. The recent involvement of state actors as major players in cyber activities has shifted the paradigm from individual, underfunded hackers exploiting systems out of opportunity to a more strategic approach

---

[281] Ibid.

[282] Ibid.

[283] Benjamin Edwards, Alexander Furnas, Stephanie Forrest, and Robert Axelrod, "Strategic aspects of cyberattacks, attribution and blame". *PNAS* 114, no. 11 (March 2017), https://www.pnas.org/doi/pdf/10.1073/pnas.1700442114

[284] Ibid.

driven by state interests. This change has influenced the discourse on the future of cyberwar, which has been overly focused on low-level digital exchanges[285].

A volatile geopolitical scene highlights the issue raised by the cyber challenges of the energy transition. The Russian aggression on Ukraine has been a particular demonstrator of increased strategic state-sponsored cyberattacks on power sector critical infrastructure.

State-sponsored attacks were already taking place before the Russia-Ukraine war. The geopolitical motivation is notably prevalent. It is argued that Russian interests include targeting energy and critical infrastructure facilities across Ukraine to the greatest extent possible to undermine Ukraine's resilience and its ability to respond to military threats. Experts and academicians have equally suggested that Russia's attempts have equally sought to exacerbate a humanitarian crisis to reduce support for the war within Ukraine and create a burden for the international community in terms of financing the post-war reconstruction of the country.[286]

These attacks may be favored by investment in specialized malware, written to target specific equipment or operation processes. Political and strategic purposes may drive state-sponsored hackers to target energy infrastructure[287].

It is alleged that Stuxnet required the cooperation of two presidential administrations, two intelligence agencies and the building of areal-world test site. Any government willing to attempt an attack of a similar scale would have to go to similar lengths. Stuxnet was the outcome of the Operation Olympic Games, the research program inaugurated by President George W. Bush[288].

---

[285] Ibid.

[286] Ibid.

[287] SentinelOne, "The Democratization of Nation-State Actor" (2017), https://go.sentinelone.com/rs/327-MNM-087/images/SEN0202-Democratization_of_Nation_State_Attacks.pdf

[288] Ibid.

Attacks carried out by states fall into the domain of cyber warfare, which involves the actions by a nation-state or an international organization to attempt to damage another's nations computers, infrastructure, or information network through an attack[289].

Critical infrastructure is under constant attack due to the risk posed by the insecurity of the computing systems that operate it most essential services. A nation typically conducts systematic cyber-attacks against the targeted adversary's institutions, to lead to submission to foreign will and intent[290].

Attacks can occur by state-sponsored groups, which backed by governments and funded with important bankrolls, can apply limitless resources to achieve their malicious objectives. Notable state-sponsored cyber groups include Russia's APT28 (Fancy Bear), known for high-profile attacks on political organizations; North Korea's Lazarus Group, infamous for the Sony Pictures hack; Iran's Charming Kitten, which targets academic and diplomatic entities; China's APT10 (Red Apollo), recognized for its extensive cyber-espionage campaigns; and the U.S.'s Equation Group, associated with advanced cyber capabilities and malware development.[291]

Theorists of cyberwarfare assert that even though the international community has yet to witness a full-scale cyberwar, what we have seen are isolated digital incidents that serve specific state agendas. Just as the theory of Mutual Assured Destruction (MAD) has effectively deterred nuclear conflict without any actual mutual destruction occurring, the lack of a past cyberwar does not negate the possibility of one in the future. If we were to claim that cyberwar is impossible simply because it hasn't happened yet, we would also have to dismiss the potential for a nuclear missile exchange since such an event has never occurred[292].

---

[289] Chad Heitzenrater, "Cyber Attacks Reveal Uncomfortable Truths About U.S. Defenses", RAND Corportation. September 21st, 2023, https://www.rand.org/pubs/commentary/2023/09/cyber-attacks-reveal-uncomfortable-truths-about-us.html

[290] Ibid.

[291] Jan Kallberg, "Strategic Cyberwarf Theory – A Foundation for Designing Decisive Strategic Cyber Operations", *The Cyber Defense Review* 1, no. 1 (Spring 2016), https://www.jstor.org/stable/26267302

[292] Ibid.

2.4.2. Terrorists

Defining cyberterrorism assumes that some key questions are addressed. Are cyberterrorism simply terrorist attacks carried out using digital or cyber electronic means, therefore, concerning any actor? Does it involve cyberattacks carried out solely by terrorist or terrorist groups? Can cyberterrorism technically speaking, be done by a state?[293]

An early working definition is provided by Mark Pollitt, special agent for the FBI in 1997, whereby "cyberterrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data, resulting in violence against noncombatant targets by sub national groups or clandestine agents".

The temptation following Pollitt's early and influential attempt at definition is to suggest that only terrorist organizations - that is, non-state actors or "clandestine agents", can commit acts of cyberterrorism. However, another relatively early definition came from James Lewis, scholar, who, in 2022, defined cyberterrorism as the "use of computer network tools to shut down critical national infrastructures, such as energy, transportation, government operations, or to coerce or intimidate a government or civilian population"; like the previous definition, Lewis' clarification leaves open the possibility that state actions might also fall into the category of cyberattacks.

Because of the asymmetric nature of the Internet and its range, terrorism can now affect many systems and create major disruption with limited human resources. Terrorists are not motivated by the same goals that inspire hackers but can follow the hackers' lead to gain sensitive information regarding the operation of crucial services related to critical infrastructure. Having broken into government or private computer systems, their attacks can have the same disrupting events - disabling or crippling the financial and service sectors and advanced economies but also disable the military and create grave consequences to national defense systems, as for instance, air traffic control systems.

---

[293] Kathi Ann Brown, *Critical Path. A Brief Critical Infrastructure Protection in the United States* (Spectrum Publishing Group Inc: Fairfax, Virginia, 2006), https://cip.gmu.edu/wp-content/uploads/2016/06/CIPHS_CriticalPath.pdf

The more technologically advanced a country is and the more vulnerable it comes to cyberattacks against its infrastructure.

Some groups have already expressed their will to engage in cyberterrorism, namely Hezbollah, which showed its increasingly technological sophistication already in 2006 with the launch of over 10,000 cyber-attacks on Israel in retaliation to Israel's bombing of Hezbollah targets in Beirut, and the publishing of a *fatwa* in October 2008 by the Islamic Egyptian Muslim Brotherhood, declaring cyber-attacks against American and Israel websites as allowed by Islamic Law and an acceptable form of Jihad[294].

Driven by political, ideological, and radicalized religious beliefs, the aim of cyberterrorism attacks should result in violence against persons or property, intimate or coerce a government or its people in furtherance of political or social objectives, cause enough harm to generate fear but serious attacks against critical infrastructures, as seen by the intent of Shamoon, would lead to death, bodily injury, explosions, or severe economic loss[295].

2.4.3. Cybercriminals, hacktivists, and individuals

The energy sector attracts several different kinds of threats; cybercriminals are particularly prevalent. Cybercrime is a broad term, used to encompass criminal activities in which computers or networks are used to enable the illicit activity[296].

A crime is broadly speaking a relative phenomenon, universal nature that has touched essentially all societies from ancient to modern times. Political communities ruling over the society have been providing their own description of what constitutes criminal behavior.

---

[294] Mandiant, "Advanced Persistent Threats (APTs)". Accessed August 28th, 2024, https://www.mandiant.com/resources/insights/apt-groups

[295] Ibid.

[296] Ibid.

The most obvious motive is that of financial gain, in which ransomware posits itself as a key player, especially when distributed by phishing scams[297].

Studies pertaining to psychological profiling in the context of cybercrime has also understood the reasons that drive individuals to engage in illicit online activities as an intricate web of motivations, personality traits and behavioral patterns.

Some individuals would broadly be inspired by simply the thrill of outsmarting sophisticated security systems and gaining notoriety within clandestine online communities[298].

Politically motivated attacks on computer systems may carry out by hacktivists, individuals or organizations that oppose certain political views or actions. Pertaining to critical infrastructure, these attacks have been more common in the oil and gas sector, the biggest cyber-attacks being the one on Colonial Pipeline, the United States' largest fuel pipeline, carried out by the hacktivist group Dark Side who created a ransomware that spurred the shutdown of the lines[299].

2.4.3. Insider threats

Insider threats occur when authorized users such as employees, contractors and businesses partners intentionally or accidentally misuse their legitimate access or have their own accounts hijacked by attackers[300].

Disgruntled employees, current or former whose access credentials have not been retired can misuse their access for revenge or financial gain, or both, or work for a malicious outsider, such as a hacker, a competitor, or a nation-state actor to disrupt business operations. Individuals that create security threats through ignorance or carelessness, for instance, falling for a phishing attack,

---

[297] Andrew Newman, "Why Do Hacks Happen? Four Ubiquitous Motivations Behind Cybersecurity Attacks", Forbes. July 13th, 2022, https://www.forbes.com/councils/forbestechcouncil/2022/07/13/why-do-hacks-happen-four-ubiquitous-motivations-behind-cybersecurity-attacks/

[298] Ibid.

[299] Klarian, "Hacktivists Vs The Oil and Gas Industry. Tackling challenges in the new era of cybersecurity, post covid-19". August 24th, 2021, https://klarian.com/blog/tackling-challenges-in-the-new-era-of-cyber-security

[300] IBM, "What are insider threats". Accessed August 21, 2024, https://www.ibm.com/topics/insider-threats#:~:text=IBM-,What%20are%20insider%20threats%3F,their%20accounts%20hijacked%20by%20cybercriminals

bypassing security controls to save time, or losing devices are called negligent insiders. They typically do not have a malicious intent[301].

The most expensive insider threats are those launched through compromise insiders, legitimate users whose credentials have been stolen by outside threat actors. Compromise insiders are often negligent insiders[302].

2.4. New Critical Infrastructure Targets and possible methods of attack

2.4.1. Smart Grids and Distributed Energy Resources: Hydropower, Wind Farms and Solar Farms

A smart grid is composed of both a power grid and a communication network atop of it, which retrieves data essential to facilitate and enable and facilitate the former's functionality.
As shown in Fig. 5, the smart grid communication network is formed on top of the power grid.

The communication network is formed of different nodes, notably smart meters, which sends back the information for feedback to a fusion center (control center), for both data analysis and decision making. These elements are therefore tightly coupled and strongly dependent. Which is precisely what favoring the introduction of new threats on these cyber-physical systems.

Two features are specifically vulnerable to cyber-attacks, notably, communication protocols for their accessibility, and the autonomous features of the smart grid.

One issue that is posed by IoT devices is that of authentication and encryption. These attacks can particularly target operation technology (OT) and industrial control systems (ICS).
What is more, as it can be seen in Figure 12, smart grids interconnect virtually all Distributed Energy Resources, especially hydropower, solar and wind farms.

[301] Ibid.

[302] Ibid.

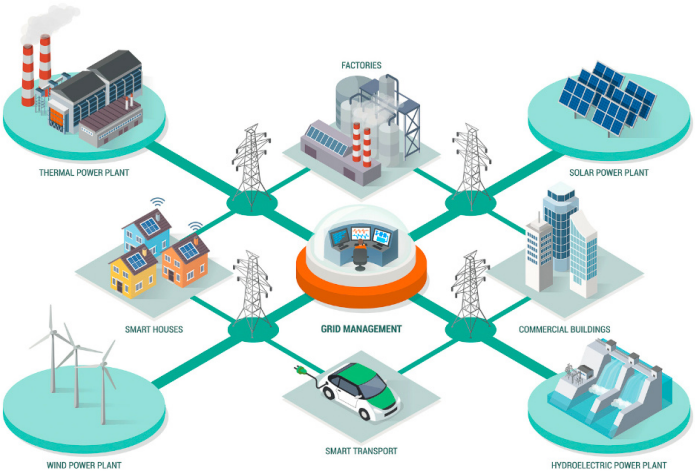


Figure 14: "The Smart Grid and DERs". Source. MemComputing, 2024.

Hydropower is a readily accessible and adaptable resource capable of providing electricity for the evolving grid. Hydropower facilities are quickly being upgraded and modernized[303].

The dam sector faces cybersecurity threats like those which already affect the overall energy sector. In 2013, the controls at Bowman Dam in Rye, New York, were infiltrated in an attack that was attributed to Iranian-government affiliated actors[304].

Cyberattacks targeting dams typically would exploit grid vulnerabilities - as the hydropower and dam sector have been enhanced by the increasing integration of the Internet of things devices and sensors; however, the damage cause would go far beyond power outages, including floods, loss of navigation, and water supplies[305].

---

[303] International Waterpower and Dam Construction Magazine, "Evolving cybersecurity threats to hydropower dams". June 12th, 2024, https://www.waterpowermagazine.com/analysis/evolving-cybersecurity-threats-to-hydropower-dams/

[304] International Water Power and Dam Construction Magazine, "Evolving cybersecurity threats to hydropower dams". June 12th, 2024, https://www.waterpowermagazine.com/analysis/evolving-cybersecurity-threats-to-hydropower-dams/

[305] Ibid.

Hydropower operators must gain visibility on their operational technology (OT) networks' traffic[306]. In fact, the most vulnerable components of digitized energy infrastructure lie at the intersection of information technology (IT) and operational technology (OT)for infrastructures, upon which smart grids, for instance, heavily rely on for both power distribution and efficiency electricity management.

Very similar vulnerabilities apply to wind and solar power.
As power plants that convert wind into electricity, wind farms are composed of wind turbines (various power source that generate energy from wind), substations (which collect the energy produced by wind turbines and feed it into the power grid), SCADA systems and networks (which control the wind turbines and substations) and are a mixture of Incident Command Systems and Information Technologies, other specification which define design, operation, and communication requirements[307].

Cyberattacks can jeopardize national wind energy systems. There are several reasons why offshore and wind parks are vulnerable to attackers. As for the other DERs, the operational technology and industrial control systems of offshore windfarms are most of the time decentralized, wind power generation is associated with systems tracking wind energy generation remotely[308].

A report by the Idaho National Library presented the attack surface of wind energy technologies in the United States. Potential attack vectors are the physical access at the wind turbine, or at the collector substation, or cyber access via remote connections. What are these connections? Wireless connected devices, temporary wireless access points introduced during the construction and

[306] Ibid.

[307] Sarah G. Freeman et. al, "Attack Surface of Wind Energy Technologies in the United States", *Idaho National Laboratory* (January 2024), https://inl.gov/content/uploads/2024/02/INL-Wind-Threat-Assessment-v5.0.pdf?utm_medium=email&utm_source=govdelivery

[308] United States Office of Energy Efficiency & Renewable Energy, "Protecting Wind Energy Systems from Cyberattacks": May 21st, 2024, https://www.energy.gov/eere/wind/articles/protecting-wind-energy-systems-cyberattacks

commissioning phases of a wind plant, individual private networks (VPN) connections of owners, vendors, and assets owners[309].

The hacking of wind assets has a range of impacts, on the assets and on the systems to which they are connected themselves. The larger the wind plant size and the larger the impact will be on the connected power grid.

Finally, solar panels are all the same becoming Internet of Things (devices), in a constany interconnectedness and always-online state and part of a SCADA system. As infrastructure of the energy transition relies on solar panels, a single well-placed cyberattack could cause widespread blackouts. Attacks can affect smart cities, homeowners with solar panels, but also utility-scale power plants and services provided by solar infrastructure often run by government or city entities[310].

2.4.4. Smart cities

Smart cities promise safer, more efficient, and more resilient communities. At the heart of these innovations lie technological and data-driven decision making, an opportunity that introduces potential vulnerabilities and could impact, among other things, urban critical infrastructure operations[311].

Several EU energy policies are for instance promoting sustainable urban proposals and initiatives, including the implementation of smart technologies in buildings to increase their energy efficiency and smart electric vehicles[312].

---

[309] Sarah G. Freeman et. al, "Attack Surface of Wind Energy Technologies in the United States", *Idaho National Laboratory* (January 2024), https://inl.gov/content/uploads/2024/02/INL-Wind-Threat-Assessment-v5.0.pdf?utm_medium=email&utm_source=govdelivery

[310] Zac Amos, "Why Cybersecurity for Solar is Crucial – And Difficult", Hackernoon. March 16th, 2024, https://hackernoon.com/why-cybersecurity-for-solar-is-crucial-and-difficult

[311] Cybersecurity & Infrastructure Security Agency, "Critical Infrastructure Sectors". Accessed August 20th, 2024, https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

[312] European Commission, "In focus: Energy and smart cities", July 13th, 2022, https://commission.europa.eu/news/focus-energy-and-smart-cities-2022-07-13_en

Smart buildings integrate building management technology at the core of complex building automation (BAS) with various monitoring and control solutions, such as heating, ventilation and air-conditioning, lighting, fire, and security, all networked onto a single platform. A smart building also uses data generated by IoT-enabled equipment to allow for energy-saving decision-making[313].

The integrated BAS is for instance vulnerable to intrusions, even from within a corporate network. Electric vehicles charging stations handle all starts of data, from users' financial information to their exact location. Attackers can install malicious software at public charging stations, to theoretically gain information from the car and use the connection between the charging station and the car as an entry point to the vehicle's internal software system[314].

2.5.5. Critical Minerals

The critical minerals and mining sector is additionally part of the energy transition infrastructure. And all the same, it harnesses vulnerabilities for cyberattacks. Billions of dollars are annually spent to identify potential new mining sites. The creation of exploration data is key to any company's growth prospects, which makes it a lucrative target for cyber espionage[315]. Examples of data may include the potential ore reserve of a mine's value - the aim of the cyber attackers would be to devalue the mine and gain insider knowledge.

Because of its criticality and strategic position in the global supply chain, the mining industry is particularly under threat from cyberattacks.
If critical material supply disruptions have minimal impacts on energy security, they have utilized impacts on the energy industry. The risk associated with disruptions in the supply of critical

[313] Johnson Controls, "Smart Buildings". Accessed August 28, 2024, https://www.johnsoncontrols.com/smart-buildings

[314] Michelle Hampson, "Yes, Your Electric Vehicle Could Potentially Be Hacked", Spectrum IEEE, August 24, 2023, https://spectrum.ieee.org/ev-hacks

[315] Australian Critical Minerals, "Information Security & Cybersecurity – Critical Minerals". Accessed August 28, 2024, https://australiancriticalminerals.com/information-security-cybersecurity/

materials is less about energy security and more about the potential slowdown of energy transitions[316].

The processing and mining landscape for critical materials is geographically connected. A selected group[317] of countries play a dominant role, in particular Australia for lithium, Chile for copper and lithium, China for graphite and rare earth elements, the DRC for cobalt, Indonesia for nickel and South AFRICA FOR platinum and iridium. A concentration that is becoming more pronounced in what concerns the processing state, as China currently accounts for 100% of the reading supply chain of natural graphite and a rare earth element called dysprosium, 70% of cobalt, and almost 60% of lithium and manganese[318].

The mining industry can therefore be considered as both a geopolitical and an economic target. foreign Cyber espionage could extend to trying to gain an edge by disrupting the advance of a competitor.

The threat categories related to mining fall into three principal areas: economic factors, theft of pricing information and hacktivists- from environmentally conscious activists protesting the effects of mining on the environment and aiming for attacks that disrupt mining operations.
Once More examples of vulnerabilities are the convergence of OT and IT systems allowing greater access to control systems, and the above - mentioned blockchains.

2.5. Types of security impacts

2.5.1. Societal security

Cyberattacks pose a significant threat to societal security by potentially causing the failure of basic sanitary and life-saving systems. In the event of prolonged power outages, critical infrastructure—

[316] IRENA, "Geopolitics of the Energy Transition", Digital Report (2024), https://www.irena.org/Digital-Report/Geopolitics-of-the-Energy-Transition-Critical-Materials

[317] Russel A. Carter, "Mining is now a cyber-threat target", *Engineering and Mining Journal* (July 2016), https://www.e-mj.com/features/mining-is-now-a-cyber-threat-target/

[318] Ibid.

such as water treatment facilities, hospitals, and emergency services—can be severely disrupted. This can lead to widespread health crises and endanger public safety, highlighting the vulnerability of essential services to cyber threats[319].

2.5.2. Economic Security

The economic impact of cyberattacks can be devastating, particularly when they target critical infrastructure like electricity grids. Recent incidents in the U.S. and Ukraine serve as stark examples, where cyberattacks have led to economic losses amounting to billions of dollars. These disruptions can halt industrial operations, cripple businesses, and create cascading effects across the economy, leading to significant financial instability and economic downturns[320].

The cyberattacks on Ukraine's power grid in 2015 and 2016 caused temporary blackouts affecting hundreds of thousands of people. The economic impact included not just the immediate cost of restoring power, but also the broader economic disruption caused by halting industrial production and daily business activities. The attacks highlighted the economic risks associated with vulnerabilities in critical national infrastructure.

2.5.3. Political Security

Compromise of critical infrastructures can disrupt government operations, undermine national security, and destabilize political systems. Such attacks can weaken a country's defense capabilities, create political instability, and even lead to conflicts, both domestically and internationally. The ability of a state to project power and maintain sovereignty can be severely compromised by cyberattacks, which can embolden adversaries and erode confidence in governmental leadership.

A notable example is the 2015 cyberattack on Ukraine's power grid, which not only caused widespread blackouts but also highlighted vulnerabilities in the country's critical infrastructure.

---

[319] Sapienza, 2019

[320] Sapienza, 2019

This attack was seen as part of a broader strategy to destabilize the Ukrainian government amid ongoing geopolitical tensions. Similarly, the 2020 cyberattack on the U.S. federal government, known as the Solar Winds breach, compromised multiple government agencies and exposed sensitive data. The attack raised concerns about national security and led to increased tensions between the U.S. and Russia, as it was widely attributed to Russian state-sponsored hackers. These incidents illustrate how cyberattacks can undermine political stability, disrupt government operations, and exacerbate international conflicts[321]

2.5.4. Reputational Security

Reputational security is another critical dimension affected by cyberattacks. When a country, organization, or political institution is successfully targeted, its reputation can suffer both domestically and internationally. A damaged reputation can lead to a loss of trust among citizens, allies, and international partners. This loss of credibility can hinder diplomatic relations, reduce political influence, and make it difficult for a nation or organization to assert its interests on the global stage. Moreover, repeated cyber vulnerabilities can brand a country as a soft target, further inviting cyber threats and attacks.

In 2022, Eni, one of the world's largest oil and gas companies, faced a significant cyberattack that targeted its computer systems. Although Eni reported that the attack did not cause major operational disruptions, the incident raised serious concerns about the security of its vast global operations. The attack drew attention to the potential risks associated with cyber vulnerabilities in the energy sector, particularly for a company as prominent as Eni. The breach not only threatened the company's operational integrity but also tarnished its public image, as stakeholders—including governments, investors, and customers—began to question Eni's cybersecurity resilience. The reputational damage from such attacks can lead to a loss of trust, a decline in stock value, and

[321] Dina Temple-Raston, "A 'Worst Nightmare' Cyberattack: The Untold Story of the SolarWinds Hack", NPR. April 16th, 2021, https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack
oky

increased regulatory scrutiny, all of which can have lasting effects on the company's standing in the global energy market[322] .

Concluding remarks

Critical energy infrastructure has become a primary target for cyberattacks due to its significance to national security. Case studies such as the Stuxnet attack on industrial control systems and the Shamoon's virus impact on Saudi Aramco illustrate the complexities of their vulnerabilities.

By categorizing various types of cyber-attacks and their potential consequences, the outcome is that the nature of cyber threats, particularly against new energy infrastructure like smart grids and renewable energy sources, is evermore evolving. The different actors and their motivations further highlight the multifaceted nature of these threats, ranging from state-sponsored attacks to cybercriminals and hacktivists.

Overall, the broader security impacts of cyber-attacks on energy infrastructures extend to social, economic, political, and reputational security. As energy infrastructures have become increasingly digitalized and interconnected, the risk landscape grows more complex, demanding more robust cybersecurity measures.

The stage is hereby set for the subsequent discussion on policies and frameworks needed to protect these critical infrastructures, as an urgent imperative for a coordinated and proactive approach to cybersecurity is required.

[322] Reuters, "Hackers hit Italian oil company's Eni computer networks". September 1st, 2022, https://www.reuters.com/business/energy/hackers-hit-italian-oil-company-enis-computer-networks-bloomberg-news-2022-08-31/

Chapter III: Policies for Cybersecurity of Critical and Digitalized Energy Infrastructure

In an era where information is as valuable as physical assets, the rise of cyber threats has fundamentally transformed security policies worldwide. From small businesses to large governments, the digital landscape has become a battlefield where sensitive data, infrastructure, and even national security are at constant risk. Cyberattacks, ranging from ransomware to state-sponsored espionage, have revealed the vulnerabilities in traditional security frameworks, forcing policymakers to rethink and reshape their approaches. Indeed, cyberthreats have fundamentally changed security policies worldwide. The challenge of invisible adversaries, whose geographical source can often not be determined, renders it essential to secure the Internet for the protection of critical infrastructures, government institutions, personal data, and the protection of individual liberties. Such has been recognized as the key issue in security studies and policies in the 21st century[323].

The primary purpose of a security policy is to establish a set of guidelines and procedures that help protect an organization's, a state, information systems and assets from threats, whether they originate from internal or external sources. Policies provide frameworks intended to mitigate risks, prevent unauthorized access, ensure compliance with legal and regulatory requirements, and promote a culture of security awareness across the organization.

The policies required for cybersecurity of Renewable critical energy infrastructure encompass various essential elements this chapter will delve into, from regulatory and legal frameworks that so far have underpinned cybersecurity efforts, focusing on national strategies and the challenges faced by the European Union in crafting effective cybersecurity. The chapter then oversees the nuances of protecting critical energy infrastructure within the context of global politics, emphasizing the role played by cooperation, international policy guidance, and the role of intelligence and knowledge sharing.

[323] Annegret Bendiek, "European cybersecurity policy", SWP Research Report No. RP 13/2012, Stiftung Wissenschaft und Politik (SWP), Berlin (2012), https://hdl.handle.net/10419/253129

The discussion progresses to the core cybersecurity requirements for energy infrastructure, including risk assessments, incident response management, and the dual considerations of IT and OT network security. Moreover, training and awareness initiatives are also scrutinized as pivotal elements in fortifying defenses against evolving threats.

The chapter additionally touches upon how to address in their specificality the broader spectrum of cyber threats, including cybercrime, cyberterrorism, and cyberwarfare. Then, the importance of public-partnerships in bolstering resilience and preparedness is reminded.
Looking forward, we explore future trends and emerging challenges, such as the security implications of critical minerals – the abovementioned for the nexus with blockchain technology, and the anticipated threats posed by artificial intelligence.

Finally, the chapter concludes with a reflection on the convergence of energy, cyber, and infrastructure diplomacies in shaping a robust security landscape.

3.1. Regulatory and legal frameworks

3.1.1. National Cybersecurity Strategies

The concept of cybersecurity has brought major developments in the roles and responsibility of a State towards its citizens. If traditionally, a State's primary responsibility was to ensure the physical security of its citizens, but the digital age has necessitated a shift in focus. Governments now bear the responsibility of safeguarding their citizens' online presence, ensuring the integrity of national infrastructure, and protecting against cyber threats that can disrupt everything from healthcare systems to financial institutions.[324]
Nonetheless and despite such ‘duty’, there is to this day no universal standard for evaluating cybersecurity policies. However, security experts, practitioners, and researchers have identified common factors that should be examined for successful policy implementation.
These pertain to:

[324] Manuela Tvaronavičienė, Tomas Plėta, Silvia Della Casa, and Juozas Latvys, “Cyber security management of critical energy infrastructure in national cybersecurity strategies: cases of USA, UK, France, Estonia and Lithuania”, *Insights into Regional Development* 24, no. 4 (2020), http://dx.doi.org/10.9770/IRD.2020.2.4(6)

1. Infrastructure,
2. Knowledge and awareness,
3. Frameworks and models,
4. Standards and regulations,
5. Management,
6. Evolution policy,
7. Specialization,
8. Enforcement.

Infrastructure refers in this case to the bolstering of cyber defense in relation to the protection of ICT, management, equipment assets and skills, whereas by knowledge and awareness the aspects that are examined within a policy are its quality, its affordability, and adoption by government, businesses, and individuals alike. Cybersecurity awareness campaigns, training for experts, and formal educational materials are examined to assess this factor. Frameworks and models refer to the procedures, operations, and tools for collecting, analyzing, and using data, including from other disciplines, to set up tactical operating cybersecurity[325].

Moving on, standards and regulations concern the national law and standards that are adopted and created that relate both direct and indirect to cybersecurity and that focus on regulating the standards for cybercrime related statutes and applicable regulations. Managing a cybersecurity that includes a planning process, administration, and cybersecurity operations is associated with a robust management factor.

Then, cybersecurity should be able to adapt, evolve, and tailor to meet new problems and requirements, through specialization professional teams, tasked with maintaining specific cybersecurity acts or law, and enforcement, which are charged with applied punishments or penalties for firms or individuals not following anti-cybercrime laws and regulations.

---

[325] Amos N. Guoria, "Development and implementation of cybersecurity policy", *Cybsersecurity. Geopolitics, Law and Policy*, Routledge (2017). Available on Perlego at https://ereader.perlego.com/1/book/2051556/10?page_number=70n

Promoting international cybersecurity standards can create a consistent and secure approach across borders, making it more difficult for attackers to exploit gaps between different countries' security measures.

Notwithstanding, the achievement of full cybersecurity seems to be an obstacle in particular because of Critical Energy Infrastructure, thus, as it has been seen, strategies focusing not only on IT (Information Technology) environments but also Operational Technology (OT) environments are required[326]

Most members have been providing security and safety measures for their critical infrastructures long before critical infrastructure protection established itself as a policy field on its own[327] . In some cases, State policies could reach a significant level of sophistication and conform to the highest international standards. Many states have decided to implement new strategies in relation to the growing and sophistication phenomenon of cyberattacks[328]. Countries worldwide have begun to publish their National Cybersecurity Strategies (NCSSs), which embody the will of securing the cyber-attacks and ransomware.

Existing cyber strategies include national strategies, addressing civilian and military national cyber defense, digital content, data privacy, and critical infrastructure protection, e-commerce, and cybercrime[329].
A unified database of global and legal policy frameworks was provided by the CSIS to aid the international community to track and harmonize regulations internationally[330].

---

[326] Manuela Tvaronavičienė, Tomas Plėta, Silvia Della Casa, and Juozas Latvys, "Cyber security management of critical energy infrastructure in national cybersecurity strategies: cases of USA, UK, France, Estonia and Lithuania".

[327] United Nations, Office of Counterterrorism, "Cybersecurity and New Technologies". Accessed on August 19th, 2024, https://www.un.org/counterterrorism/cybersecurity

[328] Manuela Tvaronavičienė, Tomas Plėta, Silvia Della Casa, and Juozas Latvys, "Cyber security management of critical energy infrastructure in national cybersecurity strategies: cases of USA, UK, France, Estonia and Lithuania".

[329] Center for Strategic and International Studies, "Global Cyber Strategies Index". Accessed on August 19th, 2024, https://www.csis.org/programs/strategic-technologies-program/archives/cybersecurity-and-governance/global-cyber

[330] Ibid.

The CSIS identified five areas on which States or international organizations can focus their strategy on, namely.

1. National strategy, to guide national deterrents and responses to cyber-change:
2. Military strategies, pertaining to the defensive or offensive cyber capabilities of the military.
3. Strategies regulating digital content.
4. Strategies regulating privacy and personal data.
5. Strategies focused on mitigating and increase resilience to cybersecurity threats to critical infrastructure networks.
6. Strategies governing digital trade and the provision of internet services.
7. Strategies aimed at combating cybercrime[331]

Looking at the index suggests that most countries have strategies or legislation focused on digital trade. Among the 193 countries and 13 territories and organizations listed by the CSIS, 114 have a strategy on digital commerce, while the second most present strategy is the one on Privacy. 91 countries have a strategy for cybercrime, 63 for cyber protection for critical infrastructure, and only 31 have a cyber military strategy[332].

Countries that have all seven strategies or all, but one is France, China, Germany, Russia, Canada (missing a strategy on content), Hungary (missing a strategy on cybercrime), Turkey (missing a strategy on cybercrime). Jamaica (missing a strategy on the military), Japan (missing a strategy for the military), and the United States, which misses a strategy on content[333].

Cyber Strategies can differ in reasons for development - these are defined as infrastructure protection by most states though the EU states more global 'cyberthreats' as the reason behind its strategy[334] .

[331] Ibid.

[332] Ibid.

[333] Ibid.

[334] Amos N. Guoria, "Development and implementation of cybersecurity policy".

According to Tvaronavičienė et. al, the majority of NCCs have yet to address specific plans which include Critical Infrastructure Protection, or even recognize the need of an adequate framework for granting supply chain and aid in case of a cyber-attack[335]. Is CIP a gap in NCCSs? For this reason, a comparison of different NCCSs may prove beneficial.

i. Israel's National Cybersecurity Strategy

As one of the most advanced cybersecurity players in the world, is renowned for its cyber defense and is a constant exporter of cyber-rated products and services, namely to the United States. To position itself in the top five list of global superpower nations, Israel started implementing its cyber security policy by adopting the National Cyber Initiative to defend the nation from cyber-attacks and to ensure that Israel becomes the core for Information Technology, and lastly, by strengthening cooperation between the government, academia[336].

Key events have influenced Israel's threat perception which accordingly have laid out the evolution and various shifts of its cybersecurity and defense policy. Today, it has an intricate but strategic national organizational framework made up of key strategy documents and international and national partnerships. Its geopolitical position has brought the nation to develop and use its sophisticated intelligence and offensive capabilities as the backbone of its conventional military operations and power projections in the region[337]. Moreover, the strive of security has also brought Israel to seek and reinforce strategic partnerships with the United States and engage, somehow, in the international norms building processes for cyberspaces.

Israel established its (Israeli) National Cyber Bureau (INCB) in 2011, as an advising and policy-oriented agency for the Prime Minister, the Israeli government, and its committees, aiming to

---

[335] Manuela Tvaronavičienė, Tomas Plėta, Silvia Della Casa, and Juozas Latvys, "Cyber security management of critical energy infrastructure in national cybersecurity strategies: cases of USA, UK, France, Estonia and Lithuania".
[336] Regner Sabillon, Victor Cavaller and Jeimy Cano, "National Cyber Security Strategies: Global Trends in Cyberspace", *International Journal of Computer Science and Software Engineering* 5, no. 5 (May 2016), https://ijcsse.org/published/volume5/issue5/p1-V5I5.pdf

[337] Jasper Frei, "Israel's National Cybersecurity and Cyberdefense Posture", Cyber Defense Project (CDP), Center for Security Studies (CSS), ETH Zürich, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-09-Israel.pdf

recommend the national cyber field policy[338]. The specific cybersecurity approach adopted by Israel focuses on developing cyber robustness, cyber resilience, and capacity[339]. The tasks of the INCB, as well as the former National Cyber Security Authority (NCSA), which had an operational orientation, are now combined in the Israeli National Cyber Directorate (INCD), which coordinates Israel's' strategic cybersecurity policy from the top[340].

At the operational level, the Mossad, Shin Bet, the Israeli Police and the INCD take care of specific issue areas[341].

Moreover, strengthened cooperation between the government, academia, industry, private sector, and the security community, in particular R&D. Its larger partnership is an innovation park called Cyberpark. As well as incorporating the Military - the Israel Defense Forces (IDF) to protect their cyberspace. The IDF's approach is additionally driven by four of Ben Gurion's doctrinal principles:

1. Deterrence, a rather challenging concept to achieve in cyberspace but according to which aggression must be responded to with sporadic outbreaks of violence, in particular, the IDF has set a precedent when it reacted, in real time, to a cyberattack by bombing Hamas' headquarter.
2. Decisive victory, though none of the various sophisticated cyberattacks, except for support for intelligence collection with Sabotage, have achieved a decisive victory on their own,
3. Early warning, a strategy that proved to be successful through cyberspace means as Unit 8200 provided several early warnings that helped prevent domestic aggressions,

---

[338] Regner Sabillon, Victor Cavaller and Jeimy Cano, "National Cyber Security Strategies: Global Trends in Cyberspace", *International Journal of Computer Science and Software Engineering* 5, no. 5 (May 2016), https://ijcsse.org/published/volume5/issue5/p1-V5I5.pdf

[339] Jasper Frei, "Israel's National Cybersecurity and Cyberdefense Posture", Cyber Defense Project (CDP), Center for Security Studies (CSS), ETH Zürich, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-09-Israel.pdf

[340] Ibid.

[341] Ibid.

4. Alliances, which are not discussed in publicly available documents byt apply some degree of international cooperation between the IDF and the US's cyber agencies, notably during the development of Stuxnet[342].

The IDF established the IDC Cyber Command, Unit 8200 for its offensive cyber operations[343]which works together with the C41 Telecommunications Directorate and the Military Intelligence Directorate (DMI). Other agencies involved with the Israel cybersecurity policy are the Cyber Authority, the General Security Service of Israel (GSS) and the Mossad[344]- Internationally, the country's closest partner remains the US and its NSA[345].

The national cybersecurity structures and initiatives, to sum up, are therefore the Israel National Cyber Directorate (INCD), the Israel Police, The Shin Bet & Mossad, the Unit 2800, and the C41 Directorate. These entities each have their organization, mandate, legal aspects, and operational capabilities. The INCD states the strategic policy to improve Israel's cyber robustness against risks by supporting critical infrastructures and imposing regulations, a strategy which is then implemented at the national level. It additionally facilitates international cooperation and formulates legal framework for cyber activities, domestically and internationally. The INCD is the central and most powerful agency, yet cooperation with other agencies have proved often challenging. Some values and operational approaches differ between Shin Bet and the INCD, while the intelligence community focuses on the protection of Israel's security from domestic threats, with important technical capabilities, if often disregards issues of privacy and legality, which, on the contrary, are stressed by the INCD. Therefore, the latter's reliance on the former can prove to be a double-edged sword (Frei, 2020): if on the one hand the involvement of these agencies into

---

[342] Regner Sabillon, Victor Cavaller and Jeimy Cano, "National Cyber Security Strategies: Global Trends in Cyberspace", *International Journal of Computer Science and Software Engineering* 5, no. 5 (May 2016), https://ijcsse.org/published/volume5/issue5/p1-V5I5.pdf

[343] Jasper Frei, "Israel's National Cybersecurity and Cyberdefense Posture", Cyber Defense Project (CDP), Center for Security Studies (CSS), ETH Zürich, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-09-Israel.pdf

[344] Ibid.

[345] Jasper Frei, "Israel's National Cybersecurity and Cyberdefense Posture", Cyber Defense Project (CDP), Center for Security Studies (CSS), ETH Zürich, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-09-Israel.pdf

its own task allows it to allocate resources to other priorities, it is prone to external influence, notably by the Shin Bet.

ii. Italy's National Cybersecurity Framework

The National Cybersecurity Strategy for 2022-2026 is published by the National Cybersecurity Agency[346], established by decree 82 of 14 June 2021. The strategy seeks to achieve 82 measures by 2026, whose achievement in due time is checked by the very same ACN. The listed challenges include ensuring a cyber resilient digital transformation of the Public Administration (PA) and of the productive system, predicting the evolution of the cyber threats, preventing online disinformation "in a broader context of the hybrid threat", in relation to guaranteeing fundamental freedoms in situations like electoral consultations or during international crisis, managing cyber crises, and pursuing the National and Strategic digital sector autonomy[347].

The objective of the strategy are therefore the protection, of national strategic assets, by using an oriented approach towards risk management and mitigation, consisting of a regulatory framework, measures and control tools; response - through systems for monitoring, detecting, analysis and activation of processes involving the whole national cybersecurity ecosystem and finally the safe development of digital technologies to meet the needs of the market, through tools and initiatives aimed at supporting centers of excellence, research activities and businesses[348].

The definition of adequate cybersecurity strategies is asserted as "one of the duties of the States", aimed at planning, coordinating, and implementing safety and resilience measures. Cybersecurity is additionally linked to achieving national strategic national autonomy, as well as an investment and enabling factor for the development of the national economy and industry. Moreover, the

[346] Agenzia per la cybersicurezza nazionale, "Strategia Nazionale di Cybersicurezza 2022 – 2026". Available at: https://www.acn.gov.it/portale/strategia-nazionale-di-cybersicurezza

[347] Ibid.

[348] Ibid.

Strategy strives towards a security-oriented cultural approach, which must go in parallel with ensuring the security of infrastructures, systems, and information from a technical point of view[349]. These goals have been pursued through the adoption of the national cyber ecosystem, enacted by the adoption of the Law Decree of June 14, 2021, no. 82.

The National Cybersecurity Agency is designed as the exclusive competent national authority and single point of contact for the purposes referred to in the legislation on the security of networks and information systems, national cybersecurity certification authority, and National Coordination Centre with reference to the European Cybersecurity Industrial, Technology and Research Competence Centre, as well as central element of the National Security Perimeter for Cyber (PSNC), competences previously attributed to a plurality of institutional actors[350].

The national cybersecurity architecture according to Law Decree No. 82/2021 include the following technical operational pillars: cybersecurity and resilience (carried forward by the ACN), prevention and combating of cybercrime (provided by law enforcement agencies, State Police (Polizia di Stato), the Financial Police (Guardia di Finanzia), and the national gendarmerie (Carabinieri); military defense and security of the State, ensured by the military; and finally Intelligence, carried forward by the domestic and the foreign security agencies, respectively AISI and AISE, overview by the Dipartimento delle informazioni per la sicurezza[351].

The Strategy is complemented by a set of implementation strategies, concerning, notably technological screening - with measures including the development of the Assessment Centres of the Ministry of Interior and the Ministry of Defence accredited by the ACN, or activated a centraò inspection team at the AGENCY, i.e.; the definition and maintenance of coherent national legal cybersecurity framework, in-depth knowledge of the cyber threat scenario, enhancement of the Public Administration's cyber capabilities, among other things[352].

---

[349] Ibid.

[350] Ibid.

[351] Ibid.

[352] Ibid.

The documents cite the responsible entities for each measure and other interested parties.

A relevant contribution before the publishing of the Strategy was the Cyber Security Report 2015 realized by CIS-Sapienza and by the Cyber Security National Laboratory of the National inter university Consortium which introduced the National Cyber Security Framework[353]. Italy's National Cybersecurity Framework has been deeply tied to risk analysis rather than technical standards, in a generalization of the US NIST Framework for Improving Critical Infrastructure Cybersecurity. It has been realized in alignment with the very same NIST and adopted by the Italian government[354].

iii. European Cyber Security Policy

The basis of the approach in the EU has been the aboev- mentioned 2008 Directive on European Critical Infrastructures, through which the EU has reinforced its approach to cybersecurity through legislation and standards[355].

In the European Union, cyber security policy is linked to both international and national regulatory processes, in what is referred to as a global multi-level and multi-stakeholder governance[356]. Because threats can be of varied geographical origin and impact, increasing level of cooperation between authorities and institutions responsible for different policy fields is required[357].

---

[353] Roberto Baldoni and Luca Montanari, "2015 Italian Cybersecurity Report: Un Fraework Nazionale per la Cyber Security", Research Center of Cyber Intelligence and Information Security Center, Sapienza Univeristà di Roma, Laboratorio Nazionale CINI di Cyber Security Consorzio Interuniversitario Nazionale per l'Informatica (Febbraio 2016), https://www.cybersecurityframework.it/sites/default/files/CSR2015_web.pdf

[354] Ibid.

[355] European Parliament, " Directive 2008/115/EC of the European Parliament and the Council of 16 December 2008 on common standards and procedures in Member States for returning illegally staying third-country nationals", https://eur-lex.europa.eu/eli/dir/2008/115/oj

[356] Annegret Bendiek, "European cybersecurity policy", SWP Research Report No. RP 13/2012, Stiftung Wissenschaft und Politik (SWP), Berlin (2012), https://hdl.handle.net/10419/253129

[357] Ibid.

The European cyber security policy is gradually evolving[358]. An essential feature in any security policy is the establishment of minimum standards about prevention and resilience. In the EU there are to be established in all member states which also cater to international cooperation. European security policy aims to foster national security without compromising democratic principles, or unduly violating individual liberties so to speak[359]

An operational guidance implemented by the EU Cyber Capacity Building Network (EUCyberNet), under the supervision of the Service for Foreign Policy Instruments and in cooperation with units of the Commission (DG INTPA, DG NEAR) and the European External Action Service in 2023, titled "Stability and Peace - Global and Transregional Threats and Challenges". According to the Network, the first steps into external capacity building are selecting the policy areas, defining the objective, and choosing the targets[360].

As such, does the EU build its policies on cyber capacity? The cornerstone of the EU's policy is the 2013 Cybersecurity strategy, which "aims to make the EU's digital environment the safest in the world", (European Court of Auditors, 2018). It focuses on five core objectives - (i) increasing cyber resilience; (ii) reducing cybercrime; (iii); developing cyber defense policies and capabilities; (iv) developing industrial and technological cybersecurity resources; (v) establishing an international cyberspace policy aligned with core EU values. A new EU Cybersecurity Strategy was presented by the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy at the end of 2020[361], covering the security of essential services such as energy grids, railways, and hospitals as well as increasingly connected objects in individuals' homes, offices, and factories. The focus of the Strategy is to build collective capabilities to respond

[358] Ibid.

[359] Ibid.

[360] EU Cyber Capacity Building Network (EU CyberNet), "The EU's International Cooperation on Cyber Capacity Building" (2023), https://www.eucybernet.eu/wp-content/uploads/2023/11/operational-guidance-for-the-eu-international-cooperation-on-ccb-1-1.pdf

[361] European Commission, "The Cybersecurity Strategy". Accessed August 21st, 2024, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

to major cyberattacks and work with worldwide partners to ensure international security and stability in cyberspace.

The Strategy outlines how a Joint Cyber Unit can ensure the most effective response to cyber threats, using the collective resources and expertise available to the EU and its Member States. Concerning specific legislation and certification, the Directive on security of network and information systems (NIS Directive), reviewed at the end of 2020, which has been implemented by all countries, ensures the creation and cooperation of government bodies as the ENISA.

In fact, a pivotal role is also played by the European Agency for Network and Information Security (ENISA), taking on coordinating and operational roles in cybersecurity. ENISA has a permanent mandate empowered to contribute to step up both operational cooperation and crisis management across the European Union. It Provides support to Member States, EU institutions, and businesses in key areas, including the implementation of the NIS2 Directive (Directive on measures for a high common level of cybersecurity across the Union) Commission[362], the EU-wide legislation on cybersecurity which provides legal measures to boost the overall level of cybersecurity in the EU[363].

The NIS2 Directive came into force in 2023, updating cybersecurity rolls introduced in 2016 and expanding the scope of the cybersecurity rules to new sectors and entities.

Other legislation includes the Cyber Resilience Act, which bolsters cybersecurity rules and requirements for products with digital elements to ensure a more secure hardware and software product, the Cybersecurity Act, which strengthens the role of ENISA, and the EU Cyber Solidarity Act, which aims to improve the response to cyber threats across the EU through a European Cyber

[362] European Commission, "Cybersecurity Policies". Accessed August 21st, 2024, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies

[363] European Commission, "Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)", https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

Security Shield and a comprehensive Cyber Emergency Mechanism to create a better cyber defense method[364].

3.3.2. Cybersecurity in policy making and decision-making process: challenges in effective EU Cybersecurity Policy

Concerning the case of the European Union's cybersecurity, and thus critical infrastructure protection strategy, it is relevant to highlight some limits pertaining to the questions that EU measures raise about the democratic implications of European cyber security whether the institutional structures and instruments of European cyber security policy's compatibility with the criteria of democratic governance[365].

Other challenges concern the blurring of boundaries between international and external policies. It is difficult, if not impossible, to identify the sources of an attack even though it originates in another country. The boundaries between justice and home affairs policy and foreign policy are therefore continuously blurred[366]

In this matter, the EU strives for a shift towards performance culture to ensure meaningful accountability and evaluation. In fact, as existing legislation is not consistently transposed by Member States, some gaps in the law remain, making it difficult for legislation to reach its full potential. Moreover, as the EU and its Member States do not have a clear overview of EU spending in cybersecurity, there are reported constraints concerning the alignment of investment levels with the strategic goals which call for the scaling up of investment levels and its impact. The adequate resourcing of the EU's cyber-relevant agencies also faces difficulties to attract and retain talent[367].

---

[364] European Commission, "The EU Cyber Solidarity Act". Accessed August 21st, 2024, https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity

[365] Annegret Bendiek, "European cybersecurity policy", SWP Research Report No. RP 13/2012, Stiftung Wissenschaft und Politik (SWP), Berlin (2012), https://hdl.handle.net/10419/253129

[366] Ibid.

[367] European Court of Auditors, "Challenges to effective EU cybersecurity policy", Briefing Paper (March 2019), https://www.eca.europa.eu/lists/ecadocuments/brp_cybersecurity/brp_cybersecurity_en.pdf

Moreover, the rapid evolution of cyber threats outpaces the development of legislative and regulatory frameworks. The EU faces difficulties in ensuring that its cybersecurity legislation keeps up with emerging threats, as the process of drafting, negotiating, and implementing legislation is inherently slow. This challenge is compounded by the inconsistent transposition of existing legislation by Member States, which creates gaps in the legal framework and hinders the EU's ability to respond effectively to cyber threats. The slow pace of legislative development can also result in outdated policies that are ill-suited to address current and future cybersecurity challenges.

3.3.3. Critical Energy Infrastructure Protection in International Politics: Intelligence and Knowledge Sharing

In addition to National Security Strategies, knowledge and intelligence sharing, whether done through military organizations, networks, and intergovernmental organizations, is a crucial element in cybersecurity strategy, specifically in the energy sector, as effects of cyberattacks are cascading and in most cases have cross-border impacts.

Focused on cybersecurity, the European Network, and Information Security (ENISA) is an EU-based platform that may have relevant frameworks for threat intelligence sharing, which can be expanded or mirrored in other regions worldwide. Dedicated to achieving a high common level of cybersecurity across Europe, ENISA was established in 2004. Headquartered in Athens, with offices in Heraklion and Brussels, it cooperates with EU countries and bodies to help them prepare for future cyber challenges, in particular to the EU'S cyber policy (ENISA, 2024): it does so by sharing knowledge, developing staff and structures, and raising awareness. The agency's work was strengthened by the abovementioned EU Cybersecurity Act as it works principally for the benefit of public organizations - EU countries' authorities, institutions, and decentralized bodies and agencies, as well EU institutions, agencies, and bodies, and extends its support to the IT industry, the business community, cybersecurity experts such as cybersecurity incident response teams, the public and academia.

It can be noted that the agency has already been at the frontline of initiatives related to critical energy infrastructure cyber protection. For instance, it organized seven editions of "one of the

largest cybersecurity exercises in Europe", *Cyber Europe,* which, in its last edition in June 2024, focused on a scenario that involved cyber threats aiming at the EU energy infrastructure in relation to geopolitical tension between the European Union and a fictitious foreign nation.
Other relevant international organizations then exist to promote the adoption of international standards for cybersecurity, in the energy sector, such as those developed by the International Electrotechnical Commission (IEC), and the International Organization for Standardization (ISO), both headquartered in Geneva, which develop these to help ensure consistency in protection levels. Countries working to align their national regulations on cybersecurity to avoid regulatory gaps and ensure a unified approach to security energy infrastructure can cater to these organizations to harmonize their relevant legislation.

Moving on, as one of the recognized international authorities in the global energy sector, the International Agency (IEA), headquarter in Paris can support technical programs helping countries improve their cybersecurity infrastructure and policies, and, in addition, engage in diplomatic efforts to develop and promote international normal for responsible state behavior in cyberspace, particularly regarding the non-targeting of critical infrastructure.

For instance, various reports were published pertaining to cybersecurity of green critical energy infrastructure, in particular, a 2022 study titled *Electricity Grids and Secure Energy Transitions,* which offers insights, for instance, on security gaps related to the internet access router and lack of encrypted VPN connection usage[368], and its updated web page and database on Smart Grids, through which it provides recommendations.
Finally, NATO endorsed its Comprehensive Cyber Defense Policy at its 2021 Summit in Brussels, through which it recognized that the impact of significant malicious cumulative cyber activities might, in certain circumstances, be considered an armed attack that could lead the North Atlantic Council to invoke Article 5 of the North Atlantic Treaty, on a case-by-case basis. Two years later, at its 2023 Summit in Vilnius, Allies endorsed a new concept to strengthen the contribution of cyberdefense to the organization's overall deterrence and defense posture, a concept that will

[368] IEA, Electricity Grids and Secure Energy Transitions. Enhancing the foundations of resilient, sustainable and affordable power systems (2022), https://iea.blob.core.windows.net/assets/ea2ff609-8180-4312-8de9-494bcf21696d/ElectricityGridsandSecureEnergyTransitions.pdf

further integrate NATO's three cyber defense levels through political, military, and technical, always ensuring civil-military cooperation, engagement with the private sector as appropriate, during crisis and conflict.

The NATO Cyber Security Centre (NCSC) based at Supreme Headquarters Allied Powers Europe (SHAPE) in Mons, Belgium, protects the Organizations' own networks by providing centralized and round-the-clock cyber defense support.

As such, updating cybersecurity regulations to mandate robust protection measures for critical infrastructure sectors can ensure that industries like energy, healthcare, and transportation are better equipped to defend against cyber threats.

3.2. Cybersecurity imperatives for Critical Energy Infrastructure Policies

While political frameworks and regulatory policies are essential in shaping the cybersecurity landscape for critical energy infrastructure, it is equally important to identify and prioritize the fundamental cybersecurity elements that require the most investment. Identifying key cybersecurity areas is crucial to protect these infrastructures from evolving threats.

3.2.1. Risk assessments for Smart Grids

Firstly, a risk-based approach to security is such that identifies the critical assets and seeks appropriate controls based on risk levels[369] There exists several risk assessment models. These estimate overall risk exposure, adding in risk mitigation and prioritization. Examples include the National Institute of Standards and Technology (NIST) Cybersecurity Framework (or ISO/IEC 27005), which quantifies risks and impacts by evaluating threats and vulnerabilities[370].

---

[369] Adrian Booth, Aman Dhingra, Sven Heiligtag, Mahir Nayfeh, and Daniel Wallance, Critical infrastructure companies and the global cybersecurity threat. How the energy, mining and materials industries can meet the unique challenges of protecting themselves in a digital world (McKinsey & Company, 2019), https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/Critical%20infrastructure%20companies%20and%20the%20global%20cybersecurity%20threat/Critical-infrastructure-companies-and-the-global-cybersecurity-threat-vF.pdf

[370] Ibid.

Risk assessments can also be focused on the economic assessment, that is, models that assess the financial consequences of cybersecurity, including reputation damage.

For smart grids, Bouramdane proposes the following to include in a risk assessment (cybersecurity smart grid

1. Availability and reliability metrics, concerning the meantime between failures (MTBF), the mean time to repair (MTTR), among other things, which help evaluate the impact on performance and customer service,
2. Incident Response Metrics, which assess the response efficiency to incidents and guide improvements in incident management capabilities, namely through the mean time to detect (MTTD) and the mean time to respond, and mean time to recover.
3. User awareness and training metrics to evaluate and measure the effectiveness of cybersecurity education programs through completion rates, campaign frequency, and policy adherence.
4. Compliance Metrics, that cover security controls, audits, patch management and vulnerability assessments and that assess adherence to the cybersecurity standards,
5. Resilience Metrics, which evaluate the system's ability to withstand and recover from incidents, including redundancy, backup`, recovery capabilities, and service restoration time[371].

Implementing cyber security measures in smart grids has brought multi-faced implications, across various timeframes and aspects. Cyber security measures extend far beyond the technical and economic benefits as they enhance smart-grid resilience, reliability, and sustainability, by countering evolving cyberthreats.

A first step in smart grid security regards network security, which, as it has been seen, are the biggest obstacle to maintain: the attacker can target different network layers of the Open Systems Interconnection model, a reference model from the International Organization for Standardization

[371] Ayat-Allah Bouramdane, "Cyberattacks in Smart Grids: Challenges and Solving the Multi-Criteria Decision-Making for Cybersecurity Options, Including Ones That Incorporate Artificial Intelligence, Using an Analytical Hierarchy Process", *J. Cybersecurity Priv. 3*, no. 4 (2023), https://doi.org/10.3390/jcp3040031

(OSI-model)[372]. A solution proposed by Faquir et. al is encrypting smart grids. Encryption refers to the process of scrambling information and data so that it can't be ready. If cybercriminals would get access to the data, the latter would be hardly accessible.
Moreover, assessing and monitoring third-party risk in the supply chain can identify potential weaknesses early, allowing organizations to address them before they can be exploited by attackers.

It is crucial to secure information assets, notably through confidentiality, integrity, and availability, also referred to as the CIA triad. The CIAD triad is a foundational concept in information security across various domains, including smart grids. It offers a framework that is comprehensive for security strategies aiming to safeguard assets against cyber threats, breaches, and unauthorized access. Confidentiality refers to the guarantee of authorized access, by safeguarding data from unauthorized exposure using encryption, access controls, and secure communication protocols.

Integrity ensures that data accuracy is maintained through the prevention of unauthorized alterations. The tools used are data validation, checksums, digital signatures, and audit trails.

Finally, availability guarantees that system and data access despite disruptions with redundancy, backup systems, disaster recovery, and network resilience techniques.

The integration of these principles into systems and processes may allow organizations to mitigate cyber risks.

In the evolving decentralized landscape of renewable energy, robust cybersecurity also has social benefits, as it cultivates consumer trust, and privacy, shielding personal information, maintaining energy data confidentiality, and upholding privacy rights[373].

---

[372] Dharmesh Faquir et. al, "Cybersecurity in smart grids, challenges and solutions", AIMS Electronics and Electrical Engineering 5, no. 1 (2020), https://www.aimspress.com/aimspress-data/electreng/2021/1/PDF/ElectronEng-05-01-002.pdf

[373] Ibid.

3.2.1. Incident response management

Incident responses refer to an organization's processes and technologies for detecting and responding to cyberthreats, and formal incident plans enable cybersecurity teams to limit, or prevent damage. According to IBM, in 2022, organizations with incident response teams, and regularly tested incident response plans, had an average data breach cost USD 2.66 million lower than that of organizations without incident response teams and plans. (IBM, 2024). Intrusion detection can have an impact on the physical impacts to the power system following a cyberattack, in because, if successful, it can result in the termination of the adversary kill chain. Once programmed, intrusion detection systems can detect attacks. Complemented by security, orchestration, automation, and response (SOAR) tools, the adversary can effectively and autonomously quarantine prior to power system impact (McCarthy et. al, 2023).

Situation awareness is also essential to maintain system resilience, which is enabled by cyber and physical metrics indicated network and endpoint visibility (McCarthy et. al, 2023).

Typically, incident response plans are created and executed by a computer security incident response team (CSIRT) made up of stakeholders from across the organization, including the chief information security officer (CISO), security operations center (SOC), and IT staff, as well as representatives from executive leadership, legal, human resources, regulatory compliance, and risk management[374]. Most Plans follow a general incident response framework based on incident models developed by the SANS Institute, the National Institute of Standards and Technology (NIST), the National Institute for Standards and Technology (NIST), and the Cybersecurity and Infrastructure Agency.

Incident response plans consist of six typical steps:

1. Preparation
2. Detection and Analysis
3. Containment
4. Eradication

[374] IBM, "What is incident response?". Accessed August 30, 2024, https://www.ibm.com/topics/incident-response

5. Recovery,
6. Post-incident review.

Preparation is a phase that consists in assuring that the competent computer security incident response team (CSIR) has always the best possible procedures in place to avoid minimal (business disruptions). This phase therefore consists in identifying and assessing risks.

Then, detection and analysis consist of monitoring the network for suspicious activity, and potential threats - in particular, data, notifications, and alerts analysis, gathered from device logs, and from various security tools such as anti-virus softwares and installed firewalls.

Containment, then, is a strategy used to stop the beach from provoking further damage to the network. Containment strategies are split into short term containment measures, focused on preventing the current threats' spread. The affected systems are isolated with strategies including for instance taking the infected devices offline. Long term containment measures focus instead on protecting unaffected systems.

Eradication refers to the identification and removal of the underlying cause of the incident to prevent it from recurring. This might include removing malware, closing vulnerabilities, or addressing exploited weaknesses in the system.

Finally, the post-incident review is a critical process that takes place after a cybersecurity incident has been resolved. Its purpose is to evaluate the entire incident response, understand what occurred, and improve future responses. Here's what this involves:

Ultimately, building cyber-resilience frameworks that enable systems to operate in a degraded state during an attack can ensure that essential services continue to function, minimizing disruption to critical infrastructure.

3.2.3. Network Security: Information Technology (IT) and Operation Technology (OT) Security

Operational technology (OT) and information technology (IT) differ. While the first constitutes the hardware and software that monitors and controls devices, processes, and infrastructures, used in industrial settings, the latter combines technologies for data, cloud systems, networking, and information processing. It can therefore be said that devices therefore control the physical while IT systems manage data and applications[375]. Securing IoT devices used in critical infrastructure can prevent these devices from becoming entry points for cyber attackers, safeguarding the broader network.

OT cybersecurity is a key component of protecting the security and safety of critical infrastructure and industrial environments. Securing OT has become an imperative, however, OT devices had traditionally been kept separate from the public internet and often internal networks, which meant they could only be accessed by authorized employees. The issue of cybersecurity is relatively new and goes hand in hand with the digital revolution, since, as it has been seen for smart grids and smart cities, IT systems control and monitor OT systems[376].

It is in fact safe to say that OT and traditional IT have converged becoming the so-called cyber-physical systems, which enable real-time data exchange but create a much larger attack surface into the bargain. The cybersecurity awareness toward OT has been growing since the Stuxnet incident[377]. As mentioned, OT environments now boast distributed, large, and decentralized governance structures, which do not lend themselves readily to traditional cybersecurity controls[378]

---

[375] CISCO, "How Do OT and IT Differ?". Accessed August 30, 2024, https://www.cisco.com/c/en/us/solutions/internet-of-things/what-is-ot-vs-it.html

[376] Fortinet, "Information Technology (IT) vs. Operational Technology (OT) Cybersecurity". Accessed August 30, 2024, https://www.fortinet.com/resources/cyberglossary/it-vs-ot-cybersecurity

[377] Muammer Semih Sonkor, Borja García de Soto, "Operational Technology on Construction Sites: A Review from the Cybersecurity Perspective", Journal of Construction Engineering and Management 147, no. 12 (2021), https://doi.org/10.1061/(ASCE)CO.1943-7862.0002193

[378] Adrian Booth, Aman Dhingra, Sven Heiligtag, Mahir Nayfeh, and Daniel Wallance, Critical infrastructure companies and the global cybersecurity threat. How the energy, mining and materials industries can meet the unique challenges of protecting themselves in a digital world (McKinsey & Company, 2019), https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/Critical%20infrastructure%20companies%20and%20the%20global%20cybersecurity%20threat/Critical-infrastructure-companies-and-the-global-cybersecurity-threat-vF.pdf

Blockchain technology, when secure, can help resolve security issues since it can provide a shared and encrypted leger immutable to changes made by malicious nodes attackers, it can verify identities, and authorize access by storing and recording transactions in the immutable ledger[379]. Utilizing blockchain or similar technologies for data integrity measures can help maintain the accuracy and authenticity of critical data, preventing tampering and ensuring trust in information systems.

Moreover, adopting zero trust architecture with strict identity and access management (IAM) controls can ensure that every user and system is continuously verified, thereby minimizing the risk of unauthorized access to critical systems.

3.3.4. Training and Awareness

The paths for information sharing have been in place for several years. For instance, the US Department of Homeland Security has developed various information sharing programs, one of these being the Cyber Information Sharing and Collaboration Program (CISCP). Information sharing networks allow the public and private sector to provide each other with any cyber threat, incident and vulnerability information faced and to work in a collaborative environment. In the United States there are six other information sharing programs overshadowed by the Department for Homeland Security. Ultimately, all these programs share their agendas: to create partnerships and to have a means to share valuable information companies and stakeholders can act on[380] .

Experts have suggested that governments fund programs that increase incentives and decrease barriers as they relate to cyber threat information sharing. It is crucial for users to have self-

---

[379] Dharmesh Faquir et. al, "Cybersecurity in smart grids, challenges and solutions", *AIMS Electronics and Electrical Engineering* 5, no. 1 (2020), https://www.aimspress.com/aimspress-data/electreng/2021/1/PDF/ElectronEng-05-01-002.pdf

[380] Jason F. Clemente, "Cybersecurity for critical energy infrastructure", (Thesis), *Calhoun: The NPS Institutional Archive* (September 2018), https://upload.wikimedia.org/wikipedia/commons/0/08/CYBER_SECURITY_FOR_CRITICAL_ENERGY_INFRASTRUCTURE_%28IA_cybersecurityfor1094560378%29.pdf

awareness regarding the risk to cyber-attacks in Smart Grids and mitigate them through risk assessments and case studies[381].

The success of some attacks can often be determined by user unawareness and lack of formal training of staff. Chowdhury and Gkioulos (2021) assert, based on a 2015 study that 31% security breaches in industrial firms during the year were attributed to human errors. In another study it was reported that 80% of data breaches had their root cause in stolen data, which is often obtained through social engineering attacks such as e-mail phishing. A key factor in countering cyberattacks is therefore an adequate user awareness and training, coupled with a culture for cybersecurity[382]. As a matter of fact, ensuring continuous education and training for employees operating critical infrastructure can enhance their ability to recognize and respond to cybersecurity threats, reducing the risk of human error.

Several frameworks and initiatives around the world have sought to counter the issue of human unpreparedness to cyberattacks. Notably, the National Institute of Standards and Technology (NIST) through its contribution as a developer of the National Initiative for Cybersecurity Education (NICE) and the Cybersecurity Workforce Framework (Nice Framework), has developed an adequate framework used as the basis for later national frameworks. The former has been instrumental to the development of many different awareness programs, tools, and modules for cybersecurity personnel, though criticism regarding the comprehensiveness and accuracy of the information given in the NICE document was raised by multiple researchers[383].

The cybersecurity skills and knowledge requirements towards the workforce will evolve continuously and rapidly in parallel to the spread of digitalization and its constant influence on an increasing number of occupations. Concerning the energy sector, authors have suggested that a

---

[381] Dharmesh Faquir et. al, "Cybersecurity in smart grids, challenges and solutions", *AIMS Electronics and Electrical Engineering* 5, no. 1 (2020), https://www.aimspress.com/aimspress-data/electreng/2021/1/PDF/ElectronEng-05-01-002.pdf

[382] Nabin Chowdhury, and Vasileios Gkioulos, "Cyber security training for critical infrastructure protection: A literature review", *Computer Science Review* 40 (May 2021), https://doi.org/10.1016/j.cosrev.2021.100361

[383] Nabin Chowdhury, and Vasileios Gkioulos, "Cyber security training for critical infrastructure protection: A literature review", *Computer Science Review* 40 (May 2021), https://doi.org/10.1016/j.cosrev.2021.100361

focus should be paid on workforce management, to specifically address organizational training and awareness of staff. A company should establish and maintain plans, procedures, technologies, and controls to ensure personnel competence.

Promoting a cybersecurity culture within organizations can encourage all employees to be vigilant and proactive in protecting against potential threats, creating a stronger overall defense.
Maturity indicator levels should be used to evaluate the training and of any security-related activities that are to take place, going, for instance, to an initial evaluation level corresponding to a *not performed activity,* to a fourth and final level of *management*[384].

Types of training include awareness training, for all employees; technical training, for system engineers and cybersecurity technicians, specialized cybersecurity training, for cybersecurity technicians and for the cybersecurity incident response team; and finally incident response and recovery training for the cybersecurity incident response team and for system engineers.

3.4. Countering cybercrime, cyberterrorism, and cyberwarfare

The Internet is a "double-edged source". Addressing cyberattacks on critical energy infrastructure also means developing effective cross-national policing of cybercrime, and defense in relation to cyberterrorism and cyberwarfare, to ultimately secure the Internet from providing a gateway for offenders and attackers.

The costs of cybercrime are increasing in scale and gravity as malicious software (or crime-ware) is increasing a true "industrialization"[385].

An urgent and integrated response must be mounted according to UNODC. Cybercrime is to be seen as an evolving form of transnational crime; due to its complex nature, it takes place in the

---

[384] Ibid.

[385] Roderic Broadhurst Ph.D., and Lennon Y. C. Chang Ph.D., "Cybercrime in Asia: Trends and Challenges" in *Handbook of Asian Criminology* (eds. Liu, J., Hebenton, B., Jou, S), (Springer: New York, 2012), https://link.springer.com/chapter/10.1007/978-1-4614-5218-8_4#citeas

border-less realm of cyberspace, compounded by the increasing involvement of organized crime groups. As most cybercrimes are transnational in character, can take place in different regions and can have ripping effects through societies around the world.

This very same transnational nature is what has rendered laws and regulations across country borders to be inconsistent and especially difficult for countries to cooperate when investigating cross-border cybercrimes. All the elements of a cybercrime offense are rarely found in the same jurisdiction. Harmonizing cyber-laws and regulations and the building of cooperation and comity among nations is a vital countermeasure against cybercrime[386].

A problem concerns when the offender, the victim, and even the evidence is in different jurisdictions, thus requiring a higher degree of cooperation between the law enforcement agencies to investigate and prosecute.

The first international instrument in this direction was represented by the Convention on Cybercrime, proposed by the Council of Europe of 2001, referred to as the *Budapest Convention,* which provided a legal framework on cybercrime[387].

International organizations such as UNODC play a role in suggesting drawing upon its specialized expertise on criminal justice systems response to provide technical assistance in capacity by building, prevention, and awareness training, international cooperation, data collection, research, and analysis on cybercrime.[388]

Moreover, scholars and experts are gaining more interest if testing various theories of crime, including traditional criminological theories such as routine activities theory and social theory, can be applied to various forms of crime. Today there exist a significant and growing number of cybercrime-related conferences, national and international, in a year. For instance, the European Society of Criminology (established 2000) (ESC) established its Working Group on Cybercrime

[386] Ibid

[387] Ibid
[388] Ibid.h

in the last several years. The American Society of Criminology (ASC) approved its Division of Cybercrime. The first annual Conference on the Human Factor in Cybercrime was held at the Hebrew University in Jerusalem, Israel, in October 2018 while the second was held in October 2019 in the Netherlands[389].

Moving on, there exists a limited but robust among of academicians highlighting a fundamental gap in the existing literature base on the nexus between the climate crisis and the different aspects of finance, including those that cover financial crime. There is no known research on clean energy and net-zero emissions goals and the proceeds of crime. As such organized crime groups are potentially sentenced to profit from proposed policies to encourage and support decarbonization[390]. Clean energy infrastructure object is in fact inherently linked to global plans to improve society's wellbeing at the international level. These 'utilitarian' actions on behalf of governments are therefore vulnerable to organized crime: economies which invest in energy can attract both legitimate and criminal entrepreneurs[391].

Concerning terrorism, the landmark in this field was resolution 1373 (2001), which provides for a comprehensive set of criminal justice requirements such as the obligations to criminalize the collection or provision of funds in relation to the commission of terrorist acts, deny haven to all those who plan, support, or commit terrorist acts and bring them to justice, and establish terrorists act as serious criminal offenses in domestic laws[392].

---

[389] Adam M. Bossier and Tamar Berenblum, "Introduction: new directions in cybercrime research", *Journal of Crime and Justice* 42, no. 5 (2019), https://doi.org/10.1080/0735648X.2019.1692426

[390] Mary Alice Young and Deborah Adkins, "Editorial: The ascent of green crime: exploring the nexus between the net zero transition and organized crime", *Journal of Financial Crime* 29, no. 3 (2022), http://dx.doi.org/10.1108/JFC-07-2022-277

[391] Ibid.

[392] United Nations Office of Counter-Terrorism, *The Protection of Critical Infrastructure Against Terrorist Attacks. Compendium of good practices* (2022), https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2225521_compendium_of_good_practice_web.pdf

The universal legal framework against terrorism is given by Security Council Resolution 2341 (2017), whereby a distinctive feature consists in its call upon Member States to specifically criminalize acts against critical infrastructure. This sets forth general requirements for Member states in terms of bringing to justice perpetrators of terrorist attacks and facilitators[393].
Finally, crippling impact to critical national infrastructure has established the role of cyberwarfare in modern conflicts[394]. Any actor, whether a country or a non-governmental body, following its objectives in cybersecurity, requires cooperation from a wide range of international partnerships.

The need for cooperation between states, international and regional organizations, and other entities in the context of cybersecurity is emphasized by the borderless increasingly sophisticated nature of cyberthreats. International cooperation and collaboration logic lies on why, when, and how to collaborate[395].

Cyberwarfare is difficult to detect a priori. It is generally understood that States engaging in it lay the groundwork for potential cyber conflict by hacking the networks of adversaries and allies alike. A potent weapon in political conflicts, espionage, and propaganda, national strategies of several cyberpower including Russia, China and the United States feature gaining offensive capability on the cyber battlefield as a prominent goal in their national strategies[396].

3.5 Public-Private Partnerships

It can be said that there is a jointly and mutually actively supported strategy reflecting a convergence of underlying interests: on the one hand, public policy success is assumed to depend on private actor participation, according to governments; on the other hand, private actors consider

---

[393] Ibid.

[394] Sanjay Goel, "Cyberwarfare: connecting the dots in cyber intelligence", *Communications of the ACM* 54, no. 8 (2011), https://doi.org/10.1145/1978542.1978569

[395] Anna-Maria Talihärm, "Towards Cyberspace: Managing Cyberwar Through International Cooperation", *UN Chronicle,* Vol. L. Security, no. 2 (August 2013), https://www.un.org/en/chronicle/article/towards-cyberpeace-managing-cyberwar-through-international-cooperation

[396] Sanjay Goel, "Cyberwarfare: connecting the dots in cyber intelligence", *Communications of the ACM* 54, no. 8 (2011), https://doi.org/10.1145/1978542.1978569

their contribution to reaching policy goals to be beneficial in achieving their own goals such as profit gain. Active involvement of private actors to achieve energy cybersecurity policy goals is essential. They can contribute by providing financial resources, technical expertise, by enhancing social support and by providing entrepreneurship[397].

However, in the private sector, a report by McKinsey stated that the investment gap leaves most heavy industrials insufficiently prepared for the mounting cyber threat[398]. Knowledge-sharing initiatives have been emerging across heavy industrial sectors[399]. Ultimately, there needs to be more conversation on reconceptualizing critical energy infrastructure governance to the shift to a sustainable cybersecurity.

How can companies transform their cybersecurity capabilities? What investments will address the most risks? As a matter of fact, there are some companies leading their way into the shaping of their cybersecurity organizations and governance models[400].

Developing shared responsibility models between the public and private sectors can ensure that both parties are equally invested in the protection of critical infrastructure, leading to more comprehensive security measures.

Example of Eni's Integrated Risk Management Model (IRM)

Companies have recognized the importance of risk assessment and their subsequent impact on the energy transition. Eni's strategy, for instance, consists of an Integrated Risk Management Model

---

[397] Michiel A. Heldeweg, Maurits Sanders, and Marc Harmsen, "Public-private or private-private energy partnerships? Toward good energy governance in regional and local green gas projects", *Energy, Sustainability and Society* 5, no. 9 (2015), https://doi.org/10.1186/s13705-015-0038-8

[398] Adrian Booth, Aman Dhingra, Sven Heiligtag, Mahir Nayfeh, and Daniel Wallance, Critical infrastructure companies and the global cybersecurity threat. How the energy, mining and materials industries can meet the unique challenges of protecting themselves in a digital world (McKinsey & Company, 2019), https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/Critical%20infrastructure%20companies%20and%20the%20global%20cybersecurity%20threat/Critical-infrastructure-companies-and-the-global-cybersecurity-threat-vF.pdf

[399] Ibid.

[400] Ibid.

(IRM), based on a system of methodologies and skills that leverages on criteria consistency of the evaluations of risks in the short, medium, and long term, within the framework of an organic, comprehensive, and prospective vision. A central role is attributed to the Board of Directors (BoD) by Risk Governance, which defines the nature and level of risk in line with strategic targets, with the support of the Control and Risk Committee. Through the IRM processes, the CEO presents a review of Eni's main risks to the Board of Directors every three months, with risks specific to each business area401.

The main risks areas are financial (market risks, liquidity risk, etc.); strategic (climate change, fall in demand due to a competitive environment, and commodity price scenario); external (geopolitical; country-related risks, energy sector regulation, relationships with stakeholders); and finally operational (cybersecurity, accidents, investigations and HSE proceedings[402]).

Every risk has its own set of treatment measures. For cybersecurity, the company proposes a centralized governance model of Cyber Security with units dedicated to cybering intelligence and prevention responsible of monitoring and managing of cyber-attacks; the strengthening cyber security operation infrastructures, the enhancement safeguards at subsidiaries outside Italy and industrial sites; and the promotion of a corporate security culture[403].

Concerning the collaboration with the public sector, the company seeks to increase its detection capacity by implementing specific IoC (Compromise Indicators) from institutional sources, and Cyber Threat Intelligence providers, and to stronger monitor security events[404].
Expanding the use of cyber insurance to cover critical infrastructure can help organizations manage the financial impact of cyber-attacks, providing a safety net that encourages investment in security measures.

---

[401] Eni, "Main financial risks". Accessed August 22, 2024, https://www.eni.com/en-IT/investors/risk-management/principal-financial-risks.html

[402] Ibid.

[403] Ibid.

[404] Ibid.

3.6. Future trends for Critical Energy Infrastructure

3.6.1. Critical minerals and critical energy infrastructure: blockchain security

Central to critical energy infrastructure will be the role of mining and processing of minerals, crucial in maintaining the military's technological edge, securing manufacturing supply chains, and pursuing sustainable development practices. For this reason, the United States Geological Survey (USGS) has designated 50 critical minerals "essential to the economic and national security of the U.S."[405]. The US Department of Defense (DOD) has identified more than 250 "strategic and critical materials" defined as "those that support military and essential civilian industries".

The Western Hemisphere is emerging as a key source of some of these minerals: Latin America currently supplies 40% of the world's copper and 35 percent of the world's lithium. The United States has lost its lining, becoming import dependent, for instance, for its supply or rare earth oxides since the early 2000s.

Minerals are crucial in energy transition infrastructure. The types of mineral resources used vary by technology. Rare earth elements are essential for permanent magnets that are vital for wind turbines and EV motors. Electricity-related technologies rely on huge amounts of copper and aluminum, as copper is a cornerstone for all electricity-related technologies. Lithium, nickel, cobalt, manganese, and graphite are crucial to battery longevity and performance and energy density[406].

The energy sector is emerging as a major force in mineral markets. The shift to a clean energy system is expected to drive a huge increase in the requirements for these minerals, as energy technologies are becoming the fastest-growing segment of demand, a change compared to the

[405] Daniel F. Runde and Austin Hardman, "Elevating the Role of Critical Minerals for Development and Security", Center for Strategic & International Studies, September 1, 2023, https://www.csis.org/analysis/elevating-role-critical-minerals-development-and-security

[406] IEA, *The Role of Critical Minerals in Clean Energy Transitions* (May 2021), https://www.iea.org/reports/the-role-of-critical-minerals-in-clean-energy-transitions

period until the mid 2010s, when for most minerals the energy sector represented only a small part of total demand[407].

However, security and resilience-wise, minerals offer their distinct and different set of challenges, concerns about price vitality and security of supply do not disappear in an electrified, renewables rich energy system. Their rising importance in a decarbonizing energy system will require energy policy makers to expand their horizons and consider potential new vulnerabilities, including blockchain cybersecurity.

3.6.2. Anticipating AI emerging threats

Developing systems that can detect and respond to threats in real time, using AI and machine learning to analyze patterns and predict potential attacks will be crucial in mitigating risks and ensuring that critical infrastructure remains secure. Leveraging AI and machine learning allow the critical energy infrastructure to evolve and adapt to emerging threats, providing a dynamic defense that is both proactive and resilient against sophisticated cyber-attacks.

It remains crucial to address the advances and challenges associated with the role of AI-based algorithms and approaches in advancing a wide range of renewables. To recall some AI utilizations in renewable energy, various AI simulation techniques have been used, for instance, in solar energy to substitute traditional physical modeling approaches, requiring less computational work and no knowledge of internal system parameters. The function of AI techniques in simulation, control, decision-making continues to be explored[408].

The world's first comprehensive AI law is the EU AI act, which regulates the use of artificial intelligence in the European Union[409]. The act aims to regulate artificial intelligence while

---

[407] Ibid.

[408] Aseel Bennagi. Obaida AlHousrya, Daniel T. Cotfas, Petru A. Cotfas, "Comprehensive study of the artificial intelligence applied in renewable energy", *Energy Strategy Reviews* 54 (July 2024), https://www.sciencedirect.com/science/article/pii/S2211467X24001536#sec6

[409] European Parliament, "EU AI Act: first regulation on artificial intelligence", June 18, 2024, https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

ensuring better conditions for the development and use of the innovative technology. The creation of cheaper and more sustainable energy is a cited benefit among those that can be created by AI. Article 5 of the EU act prohibits certain AI Practices, namely "subliminal techniques beyond a person's consciousness", or "purposefully manipulative or deceptive techniques, with the objective or the effect of materially distorting the behavior of a person or a group of persons by appreciably impairing their ability to make an informed decision"[410].

In the United States, President Biden's Executive Order on the Safe, Secure, and Trustworthy Development Use of Artificial Intelligence (2023), directed the actions needed to mitigate the potential risks of AI systems, namely:

1. The requirement that developers of the most powerful AI systems share their safety test results and other critical information with the U.S. government,
2. The development of standards, tools, and tests to help that AI systems are safe, secure, and trustworthy, issued by the National Institute of Standards and Technology,
3. The protection against the risks of using AI to engineer biological materials,
4. The establishment of standards and best practices to detect AI-generated content and authentication official content, with watermarking to clearly label AI-generated content,
5. The establishment of an advanced cybersecurity program to develop AI tools to find and fix vulnerabilities in critical software,
6. The development of a National Security Memorandum that directs further actions on AI and security, to be developed by the National Security Council and White House Chief of Staff[411].

Dealing with AI itself brings with it a tidal wave of "unknowns", ranging from highly beneficial to harmful. The decisions about the construction and operation of AI models are what determine

---

[410] EU Artificial Intelligence Act. Date of entry into force: 2 February 2025, https://artificialintelligenceact.eu/article/5/

[411] The White House, "FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence", October 30, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/

both near- and long-term consequences of those models and these are made by humans. Regulating these models therefore comes with the imperative of core principles, namely a Duty of Care, transparency, safety, and responsibility[412].

This challenge will require collaboration between the public and AI companies to navigate the regulatory and legal landscape efficiently to ensure the security of infrastructure[413].

3.6.3. Energy, Cyber and Infrastructure Diplomacies

Engaging in diplomatic efforts to establish norms and agreements that deter state-sponsored cyber-attacks on critical infrastructure will help create a more stable and secure global environment. In fact, by fostering international cooperation and establishing clear guidelines for acceptable behavior in cyberspace, these diplomatic efforts can reduce the likelihood of conflicts escalating due to cyber incidents. Additionally, such agreements can facilitate collaboration on threat intelligence sharing, joint response efforts, and the development of global standards for cybersecurity, ultimately contributing to the protection of critical infrastructure on a worldwide scale.

To address these challenges, a multifaceted approach combining cyber, energy, and infrastructure diplomacy may prove relevant. In fact, the intersection of these three forms of diplomacy merges insights from international relations, energy policy, and cybersecurity and can help develop strategies that protect the critical infrastructure on which our sustainable future depends.

Cyber Diplomacy involves international efforts to address the challenges posed by cyber threats. It includes negotiations, treaties, and cooperative measures aimed at reducing cyber risks and building trust among nations. It encompasses how countries, groups, or people behave in cyberspace to protect and advance their cultural, economic, scientific, or political interests, all while maintaining peaceful relations[414].

---

[412] Tom Wheeler, "The three challenges of AI regulation", Brookings, June 15, 2023, https://www.brookings.edu/articles/the-three-challenges-of-ai-regulation/

[413] Jane Accomando et. al, "The Intersection of Energy and Artificial Intelligence: Key Issues and Future Challenges", Morgan Lewis, August 12, 2024, https://www.morganlewis.com/pubs/2024/08/the-intersection-of-energy-and-artificial-intelligence-key-issues-and-future-challenges

[414] IE, UncoverIE, "Cyber diplomacy and cybersecurity: guardians of the digital realm", July 16, 2024, https://www.ie.edu/uncover-ie/cyber-diplomacy-and-cybersecurity-guardians-of-the-digital-realm/

Energy Diplomacy refers to the strategic use of diplomatic relations to secure energy resources, ensure stable energy supplies, and promote sustainable energy initiatives. With the rise of renewable energy, energy diplomacy now encompasses efforts to facilitate international collaboration on clean energy projects and protect these investments from external threats, including cyberattacks.

According to Griffiths, multilateral energy diplomacy is expected to play a key role in determining the ultimate extent and scale of the energy transition and its impact on groups of countries and organizations that share common interests. Bilateral energy diplomacy can support long-term energy security and economic well-being of individual nations through the fostering of firing relationships concerning energy supply and demand[415].
Finally, concerning infrastructure diplomacy, national and international efforts have brough limited results[416]

A potential answer lies in the creation of a global cyber treaty specifically aimed at safeguarding critical infrastructure. As an approach that could overcome the limitations of current frameworks, the treaty would establish binding obligations to enhance cybersecurity by States, provide a focused and clear legal structure and promote international cooperation. Building upon existing efforts such as the UN's framework for responsible State behavior in cyberspace and the EU's robust legal framework on cybersecurity - including the directives NIS and NIS II - the treaty would concretely *narrow the scope* to a manageable level, rendering the reach of a consensus among States easier[417]

---

[415] Steven Griffiths, "Energy diplomacy in a time of energy transition", *Energy Strategy Reviews* 26 (November 2019), https://doi.org/10.1016/j.esr.2019.100386

[416] Patrick Pawlak and Aude Géry, "Why the World Needs a New Cyber Treaty for Critical Infrastructure, Carnegie Endowment, March 28, 2024, https://carnegieendowment.org/research/2024/03/why-the-world-needs-a-new-cyber-treaty-for-critical-infrastructure?lang=en&center=europe

[417] Ibid.

The effectiveness of such a measure goes hand in hand with mechanisms for accountability, such as reporting requirements, dispute resolution procedures, and possibly a permanent secretariat to oversee implementation[418]

Ultimately, in the transition era, a global treaty on the protection of critical infrastructure could significantly enhance global cyber resilience, reduce the risk of cyber conflicts, and provide a clearer legal basis for international cooperation in responding to and preventing cyberattacks[419]

Concluding remarks

Efficient and straightforward policy and regulatory frameworks are required to safeguard critical and digitalized energy infrastructures against the growing threat of cyberattacks. In this context, an essential role is played by national cybersecurity strategies as well as the implementation of effective policies and coordination at a regional and ultimately global level.

International collaboration, particularly in intelligence and knowledge sharing, proves to be essential components in the fight against cyber threats. Still, a comprehensive approach to securing energy infrastructures. As such it should be ensured that cybersecurity policies follow guidelines including risk assessments, incident response management, and an integral approach to information and operational technology security.

Both the digital and the energy transition are yet to be completed as they continue to evolve, leaving gaps that cyberthreats can exploit. For this reason, a discussion on future trends, such as the implications of AI in emerging threats, the increasing integration of critical minerals, the importance of public-private partnerships among others highlights the need for adaptative and forward-looking policies.

Cybersecurity is a strategic concern that must evolve alongside these transitions, as such ongoing efforts are essential to ensure that critical energy infrastructures remain resilient and secure as the global energy landscape its path to sustainability.

---

[418] Ibid.

[419] Ibid.

Analytical Assessment of Benefits & Risks of Corresponding Security Policies

The cybersecurity strategies explored in the third chapter encompass a range of approaches. From international cooperation through cyber diplomacy, to the regulations stemming from National Security Strategies and international frameworks, efforts to combat cyber terrorism and crime, investment in technological cyber security strategies and the role of public-private partnerships, each of these measures is designed to address specific aspects of the cybersecurity challenge, with varying degrees of emphasis on prevention, mitigation, response, and recovery.

While distinct in their focus, these policies are interconnected and mutually reinforcing to form a comprehensive strategy to safeguard critical energy infrastructure from the growing and evolving landscape of cyber threats, a critical evaluation of each measure on its own terms can ensure that they collectively contribute to a robust and resilient cybersecurity framework. It is therefore crucial to ponder each policy individually to fully assess its effectiveness, risks, and benefits.

Policy 1: Improving National Security Strategies

During both peace and war time national security strategies that incorporate cybersecurity strategies are crucial for a cohesive defense against cyber threats. However, the lack of several critical aspects can hinder their effectiveness.

Policy strengths & benefits

- Increases private sector responsibilities and tackles unregulated cyber markets.
- Prioritization of collaboration with other countries.
- Allocation of dedicated budget and resources.
- Development of an implementation plan.
- Identify common methodologies.
- Creation of a national security agency.

Policy weaknesses & challenges

- **Integration of the private sector.** The private sector owns and operates a significant portion of critical infrastructure, notably concerning energy. National security

frameworks that over rely on governmental and military responses may not adequately integrate the expertise and resources of the private sector.

- Insufficient emphasis on multi-sectoral collaboration.
- **Lack of engagement with non-governmental actors**, which can result in coverage and missed opportunities for resilience and innovation building.
- **Risk of abstract strategies**. The attempt to encompass different sectors can cause these strategies to outline goals and objects that are sometimes too broad, without providing clear, actionable steps for achieving them.
- **Gap between strategic planning and implementation.** Can leave organizations and agencies uncertain about how to operationalize these strategies effectively.
- Lack of focus on and lack of identification of the main actors of cyber-attacks and espionage.
- **Lack of focus on geopolitical risks,** which can have a profound impact on national security strategies especially in the context of cybersecurity for critical infrastructure like energy systems. These seem to be scarcely addressed in existing strategies.

Limits

- **Choosing offensive vs. defensive cyber response strategies.** Defensive strategies are often reactive, responding to threats after they occur, which can leave critical infrastructures vulnerable to new or unexpected cyber threats. On the other hand, engaging in offensive cyber operations can trigger retaliatory actions, leading to a tit-for-tat escalation that can spiral out of control, potentially leading to broader conflicts.
- Is collaboration, especially international, feasible to implement?
- Lack of centralized command.
- **Prioritization.** Overall, prioritizing cybersecurity within these strategies remains a significant challenge as, despite the growing awareness of cyberthreats, cybersecurity often competes with other pressing national issues for attention and resources, which can lead to inconsistent implementation and a lack of sustained focus on developing and enhancing cybersecurity measures. For examples of National Cybersecurity Strategies

that are stalling because of lack of prioritization, see Carnegie's reports on Mexico[420], Brazil[421], and South Africa[422].

Policy applications & main actors

- States
- States in collaboration with the private sector, international organizations, non-governmental organizations, and other States.

Focus

- Cyber tangible and intangible knowledge
- Protection of critical infrastructure
- Regulation and legal frameworks

Final reflection & recommendations

- There needs to be a decisive jump ahead from strategy to practice which could be achieved by the development and implementation of Key Performance Indicators (KPIs) that translate strategic objectives into measurable outcomes, providing concrete benchmarks for assessing progress and ensuring that cybersecurity initiatives are not only planned but actively pursued and evaluated.

---

[420] Joe Devanny and Russell Buchan, "Mexico's National Cybersecurity Policy: Progress Has Stalled Under AMLO", Carnegie Endowment for International Peace, May 28, 2024 https://carnegieendowment.org/research/2024/05/mexicos-national-cybersecurity-policy-progress-has-stalled-under-amlo?lang=en

[421] Joe Devanny and Russell Buchan, "Brazil's Cyber Strategy Under Lula: Not a Priority, but Progress is Possible", August 8, 2023, https://carnegieendowment.org/research/2023/08/brazils-cyber-strategy-under-lula-not-a-priority-but-progress-is-possible?lang=en

[422] Joe Devanny and Russell Buchan, "South's Africa Cyber Strategy Ramaphosa: Limited Progress, Low Priority", January 12, 2024, https://carnegieendowment.org/research/2024/01/south-africas-cyber-strategy-under-ramaphosa-limited-progress-low-priority

- **National Strategies must be flexible and adaptable** to respond effectively to these dynamic risks, balancing the need for strong defense with the complexities of international relations and the potential for escalation in cyberspace.

Policy 2: Cyber Diplomacy

The effectiveness of cyber diplomacy depends on the ability of nations to align their interests, which can be a complex and challenging process. Differences in national priorities, legal frameworks, and levels of cyber maturity can create obstacles to achieving meaningful agreements. Furthermore, the risk of diplomatic breakdowns, especially in the context of geopolitical tensions, poses a significant challenge to the success of cyber diplomacy.

Policy strengths & benefits

- Appointing *tech* ambassadors
- Progressing a cyber diplomacy COP
- Development of global norms and standards for cybersecurity, essential for fostering a cohesive international response to cyberthreats.
- Enhance threat intelligence sharing, reducing the risk of conflicts, and fostering a more unified global approach to cybersecurity.
- Potential to build trust between nations and promote stability in cyberspace is a critical asset in the fight against cyber-threats.
- Improving international regulations and standards for the identification and designation and protection of (common) critical infrastructure.
- Mitigate attracts from rival or adversarial countries through negotiations, sanctions, or international agreements.

Policy weaknesses & challenges

- **Lack of global consensus,** leading, for instance, to disagreements over key issues like internet governance, data sovereignty, and the acceptable use of cyber capabilities.
- **Vague and non-binding norms** which can lead to different interpretation and selective adherence by states: what is more is that many cyber norms that have been proposed or agreed upon are non-binding and lack clear definitions.

- **There are limited enforcement mechanisms for cyber norms and agreements.** Even when norms are violated, there is often no clear or effective way to hold states accountable.
- Inconsistent participation
- **Regional conflicts of interests;** what might be seen as a security measure in one region could be perceived as a threat in another, complicating international diplomatic efforts.

Limits

- **Difficulties** in decision-making and agreement for coordinated cybersecurity policies.

Policy applications & main actors

- **National governments** and allied nations through foreign ministries, and likewise cybersecurity agencies
- International and Regional Organizations and regional alliances
- **Advocacy groups**, civil society, and non-governmental organizations
- **Academic** and research institutions
- **International coalitions**, networks, and partnerships

Focus

- Rival or adversarial countries.
- Private sector entities and representatives
- Transnational cybercriminal groups and terrorist organizations.

Final reflections & recommendations

- Integrating tech experts and digital tools in diplomacy and peace-building actions.
- The promotion of global norms
- Advancing a global cybersecurity COP

Policy 3: Harmonization of international standards and norms and international cooperation

The effectiveness of cyber diplomacy depends on the ability of nations to align their interests, which can be a complex and challenging process. Differences in national priorities, legal frameworks, and levels of cyber maturity can create obstacles to achieving meaningful agreements. Furthermore, the risk of diplomatic breakdowns, especially in the context of geopolitical tensions, poses a significant challenge to the success of cyber diplomacy.

Policy strengths & benefits

- Development of global norms and standards for cybersecurity, essential for fostering a cohesive international response to cyberthreats.
- Enhance threat intelligence sharing, reducing the risk of conflicts, and fostering a more unified global approach to cybersecurity.
- Potential to build trust between nations and promote stability in cyberspace is a critical asset in the fight against cyber-threats.
- Improving international regulations and standards for the identification and designation and protection of (common) critical infrastructure.

Policy weaknesses & challenges

- **Variations in legal and regulatory frameworks,** countries can have different legal traditions and regulatory environments which can make it challenging to harmonize standards. For instance, data protection laws vary widely, with some countries emphasizing privacy more than others.
- **Resource constraints in developing countries** may signify a lack of resources and technical expertise for them to implement and comply with international standards.
- **Rapid technological change** can outstrip the ability of international bodies to develop and update standards.

Limits

- Diverse national priorities and interests and sovereignty issues if nations are reluctant.
- Implementation and enforcement,

Policy applications & main actors

- United Nations and affiliated relevant international organizations and agencies
- International Standard Organizations
- Regional organizations
- Global and regional alliances
- Industry and sectoral organizations such as the WEF and the IEA

Focus

- Nation-states and Private Sector Representatives, Critical Infrastructure Operators

Final reflections & recommendations

- **Capacity building and technical assistance,** wealthier nations along with international organizations should provide technical assistance to developing countries to help them build their cybersecurity infrastructure and capabilities.
- **Establish Regional Cybersecurity Centers of excellence,** that can offer training, resources, and support to countries with limited capabilities.
- **Financial support mechanisms such as** a cybersecurity fund, or subsidies for ompliance.

Policy 4: Intelligence Sharing

This collaborative effort enables organizations to better anticipate, detect, and respond to cyber incidents by pooling resources and knowledge. Intelligence sharing can occur within industries (between companies in the energy sector), across different sectors, or between governments and private entities. Effective intelligence sharing is essential for improving overall cybersecurity resilience and minimizing the impact of cyber threats.

Policy strengths & benefits

- Effective intelligence sharing can enhance early warning capabilities, enabling faster detection and response to cyber-incidents.

Policy weaknesses & challenges

- Limits of the different laws and regulations on data sharing, privacy, and liability from different jurisdictions, making cross-border threat intelligence sharing frameworks difficult to implement.
- Challenge of analyzing data efficiently across several organizations
- Challenge of choosing the appropriate level of classification and sensitivity for shared threat intelligence
- Organizations may lack sufficient incentives to share threat intelligence particularly if there are not tangible benefits or rewards for participation.
- **Ensuring** intelligence sharing is timely, relevant, and actionable while also protecting sensitive information and respecting legal and ethical boundaries.

Limits

- In intelligence sharing, organizations that hesitate to disclose sensitive cyber threat intelligence due to concerns about trusts and the possible risks of disclosing vulnerabilities to others.

Policy applications & main actors

- States and Intelligence Agencies
- National Cybersecurity Agencies
- Regulatory bodies
- Law enforcement, through cybercrime units.
- International law enforcement, organizations like INTERPOL or EUROPOL.
- States and Intelligence Agencies in collaboration with companies and international organizations and bodies like the IEA.
- Private sector entities (security vendors, industry consortiums).

Focus

- **Critical infrastructure operators** (energy companies notably renewable energy providers which need to be aware of emerging threats to protect their operations, grid operators i.e., organizations responsible for managing national or regional power grids, utility companies i.e., electricity, gas, and water).
- **Threat actors** (nationstates, criminal organizations, hacktivists, insider threats).
- **Indicators of compromise** (technical indicators i.e., IP addresses, file hashes, domain names, and behavioral indicators i.e., unusual behaviors or patterns within networks such as unusual login attempts, unexpected data transfers and changes in system configurations).

Final reflections & recommendations

- **The success of intelligence sharing** depends on trust, transparency, and the establishment of standardized protocols for information exchange.
- **Geopolitical tensions** and differing national priorities can complicate intelligence sharing potentially leading to gaps in information that adversaries might exploit, therefore fostering a culture of collaboration and trust is essential to maximizing the benefits of intelligence sharing in the fight against cyber threats.

Policy 5: Global anti-crime and anti-terrorism efforts

These measures often involve advanced surveillance, intelligence gathering, and law enforcement cooperation, as well as global awareness, educational and anti-radicalisation training programmes.

Policy strengths & benefits

- **Comprehensive legal frameworks** for the criminalization of cyber-offenses.
- Deterrence of criminal activity
- Collection of evidence from surveillance
- **Quick-incident response,** from real-time monitoring responses to emergencies, such as crimes, accidents, or security breaches

Policy weaknesses & challenges

- Sustaining a balance between ensuring security and protecting civil liberties (legal privacy issues and potential for abuse).
- Strategies must adapt to evolving cyberthreats therefore require significant investment in both technology and training.

Limits

- The issue of attribution in cybercrime for holding perpetrators accountable and identifying the responsible party without causing unintended consequences, whether legal, diplomatic, or political: attributing cyber threats to individual actors - or entities such as groups or entities - can be difficult leading to uncertainty and possibly intelligence misinterpretation.
- The issue of liability.

Policy applications & main actors

- Law enforcement agencies
- Intelligence agencies
- INTERPOL, UNODC

Focus

- Cybercriminals
- Terrorist organizations

Final reflections & recommendations

- **Continuous adaptation** to the issue of cyber-radicalization and the evolving cyber threats
- **Discrepancies in national laws** and varying levels of cybersecurity capabilities can hinder effective collaboration.
- Balancing security with civil liberties

Policy 6: Public-Private Partnerships

Policy strengths & benefits

- **Ownership.** Many critical infrastructures, such as energy, finance, and healthcare, are owned and operated by private entities. Private-public partnerships ensure that these critical sectors are adequately protected by aligning private security measures with national security priorities.
- **PPPs can drive cybersecurity awareness and education initiatives.** The public sector can reach broad audiences with educational campaigns, while the private sector can provide specific training and tools to help businesses and individuals through their cybersecurity practices.
- **The private sector can provide input** on the feasibility and impact of cybersecurity regulations helping to shape policies that are both effective and practical, a collaboration that leads to more balanced regulations that protect national security without unduly burdening businesses.
- **Public-private partnerships can drive** joint research and development efforts leading to the creation of new cybersecurity tools, techniques, and protocols. This collaboration can accelerate the pace of innovation and ensure that cybersecurity measures remain on the cutting edge.
- **Access to vast amounts of data and threat intelligence** from the private sector which can be beneficial and invaluable to government agencies.
- **Facilitation of sharing of this information** from the private sector which enables faster detection and response to emerging threats.

Policy weaknesses & challenges

- Dependence on private sector expertise
- Data sharing risks
- **Lack of coordination and communication** with fragmented efforts and information sharing issues

Limits

- Regulatory, interest and legal challenges
- Security of shared information
- **Scope of collaboration:** PPPs may have limited scope in addressing the full spectrum of cybersecurity focusing primarily on specific aspects or sectors rather than a comprehensive approach.
- Cost sharing disputes and funding limitations.

Policy applications & main actors

- Energy companies, utilities companies
- Government agencies
- Technology and security vendors
- Critical Infrastructure Operators

Focus

- Tools and technology needed to promote cybersecurity.
- Training programmes
- Industry groups

Final reflection & recommendations

- **Improve Information Sharing** through secure data sharing mechanisms, and build trust between partners through transparency, regular updates, and collaborative efforts to address shared risks.
- **Increase funding** for cybersecurity initiatives both public and private to support the implementation of advanced technologies and comprehensive risk management strategies.

Concluding remarks

These cybersecurity policies do not operate in isolation but are deeply interdependent. For instance, effective cyber diplomacy can enhance national security strategies by establishing international norms, which in turn, support efforts to combat cyber terrorism and crime. However, managing these interdependencies requires careful coordination to avoid potential conflicts. For

example, strict national security measures might inadvertently strain international cooperation, or private sector interests might clash with public regulatory frameworks. Therefore, a holistic integration of these policies is necessary, ensuring they reinforce rather than undermine each other.

The operational complexity of implementing these diverse policies simultaneously cannot be understated. Coordinating efforts between different government agencies and private sector stakeholders is a significant challenge. Furthermore, the allocation of resources across these areas requires careful consideration, especially given the varying levels of maturity and different demands of each policy. Prioritizing cybersecurity within these national strategies remains a significant challenge, as cybersecurity often competes with other pressing national issues for attention and resources, which can lead to inconsistent implementation and a lack of sustained focus on developing and enhancing cybersecurity measures.

The effectiveness of these cybersecurity strategies is also influenced by global and regional factors. Regional differences in cyber maturity, legal frameworks, and threat landscapes can affect how these policies are implemented and their overall effectiveness. Moreover, global coordination is essential in combating cross-border cyber threats. The success of national strategies often depends on the broader international context, making global collaboration a key component of any robust cybersecurity framework.

What is evident is that while the national and international public sectors play a crucial role in setting out regulations and frameworks for cybersecurity, these efforts cannot be effective without the active involvement of the private sector. As the primary operators of critical infrastructure and developers of innovative technologies, private companies possess the expertise, resources, and agility necessary to implement and enforce these regulations. Public-private collaboration is essential to ensure that cybersecurity measures are practical, comprehensive, and capable of addressing the dynamic challenges of the digital age.

Cyber threats are dynamic, constantly evolving in complexity and sophistication. As such, these strategies must be flexible and adaptable to remain effective. This includes being responsive to

new threats and technological advancements, such as artificial intelligence and quantum computing, which have significant implications for the future of cybersecurity.

It is true that there has been a paradigm shift from the adoption of specific measures aimed at protecting critical infrastructures from cyberthreats towards a holistic approach aligned with a more significant national effort. The institutionalization of a centralized architecture through the creation of a central authority to coordinate all national efforts in securing the national cyber space. National strategies ensure continuity and cohesiveness in the long run: the creation of a robust and efficient system at the institutional level is crucial.

However, raising cyber hygiene, notably, by strengthening cyber ecosystems play a key role in cyber defense success and will be a continuous challenge. A national ecosystem must support the development of innovative security technologies. Investments in technological research and development and notably through the development of educational programmes enable the creation of a dynamic cyber ecosystem. There is a necessity to invest in the cyber-job-market to develop more secure technologies. Countries who suffer from chronic cyber investments in this case still fall short. The digital gaps, over-dependence on foreign information technology and an overall lack of digital competences among the population are factors that will negatively affect cybersecurity.

No implementation of these cybersecurity strategies would be complete without it addressing important societal and ethical considerations. Measures like surveillance and intelligence gathering, while effective in countering cyber threats, must be balanced against the protection of civil liberties. Ensuring this balance is delicate but essential to maintaining public trust and avoiding potential abuses of power. Moreover, public-private partnerships rely heavily on the trust and cooperation of all parties involved, including the public.

Looking ahead, ongoing assessment and refinement of these policies are necessary to address emerging risks and opportunities. The development and implementation of Key Performance Indicators (KPIs) could be instrumental in translating strategic objectives into measurable

outcomes, providing concrete benchmarks for assessing progress. Additionally, continued investment in research and innovation is critical to staying ahead of cyber threats.

In conclusion, while the current cybersecurity strategies for protecting critical energy infrastructure lay a strong foundation, they must be continuously evaluated and improved to address the evolving landscape of cyber threats. Voluntary improvements in cybersecurity and data privacy are no longer adequate. Businesses must rethink their approach to cybersecurity in alignment with National Cybersecurity Strategies. The government needs to introduce new standards and regulatory frameworks while shifting liability to ensure companies are held accountable for not fulfilling their responsibilities. Supply chain vulnerabilities must be tackled by fostering information sharing through new public/private partnerships, addressing known vulnerabilities, offering cybersecurity training to employees, and developing critical incident response plans.

By critically assessing each policy on its own terms and understanding the broader interconnections, stakeholders can ensure that these strategies collectively contribute to a resilient and robust cybersecurity framework. The future of cybersecurity depends not only on the strategies we adopt today but also on our ability to adapt, innovate, and collaborate in the face of new challenges. Therefore, a call to action is necessary for all involved to commit to continuous improvement, ensuring that cybersecurity measures are not only planned but actively pursued, evaluated, and refined.

Final figures

Respectively,

Figure 15: Strengths of National Cyber Security Stratregies, Own Work.

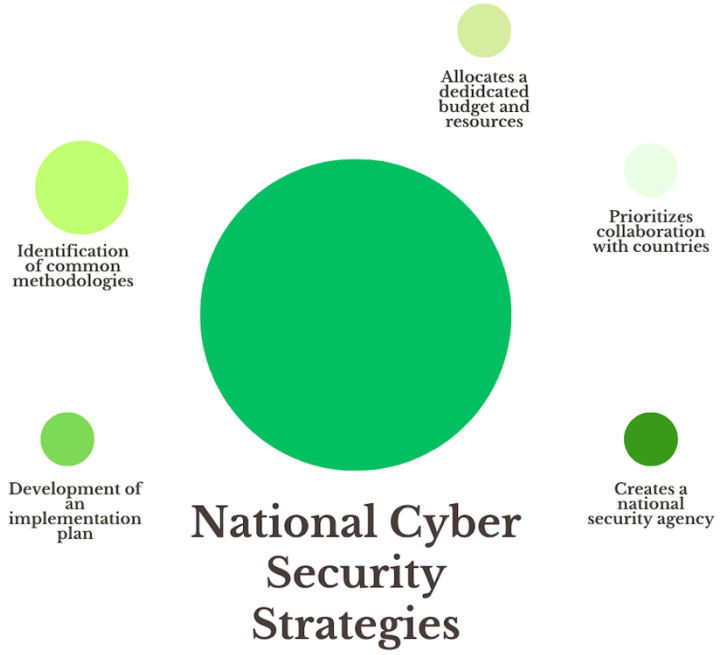
Figure 16: Strengths of Cyberdipomacy, Own Work.

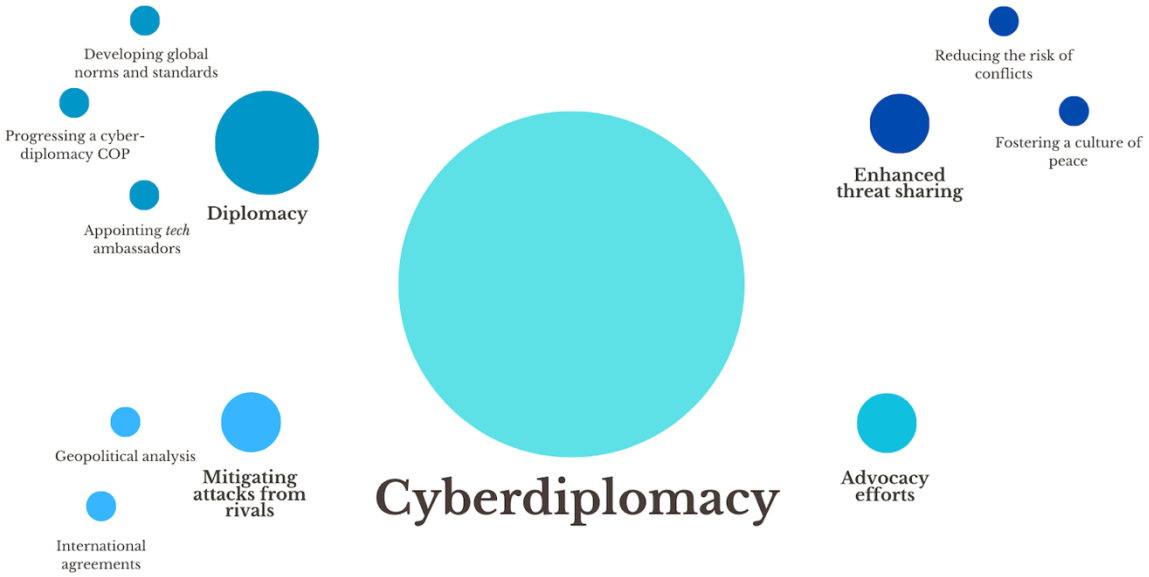
Figure 17: Strengths of Public-Private Partnerships, Own Work.

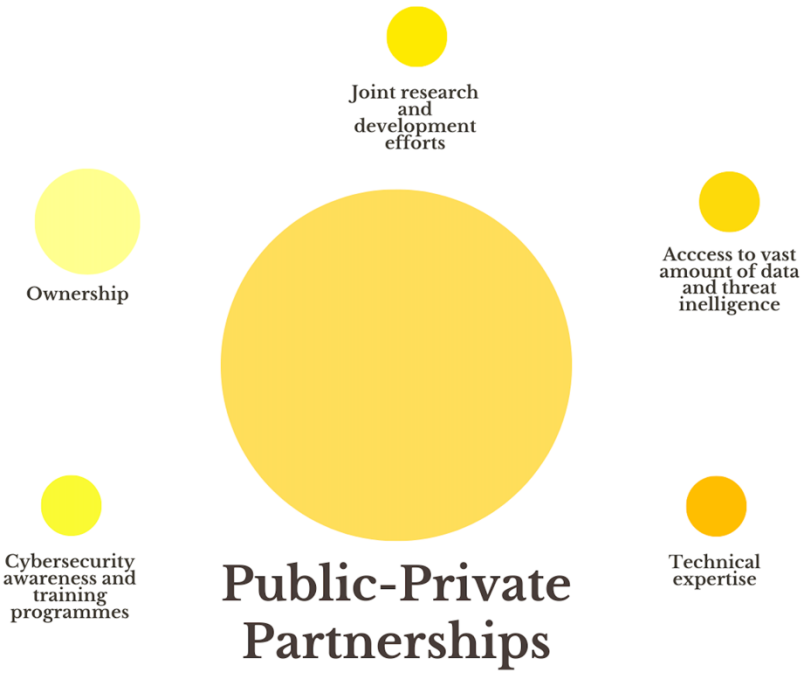
Figure 18: Challenges of National Cyber Security, Own Work.

Figure 19: Challenges of Cyberdiplomacy, Own Work.

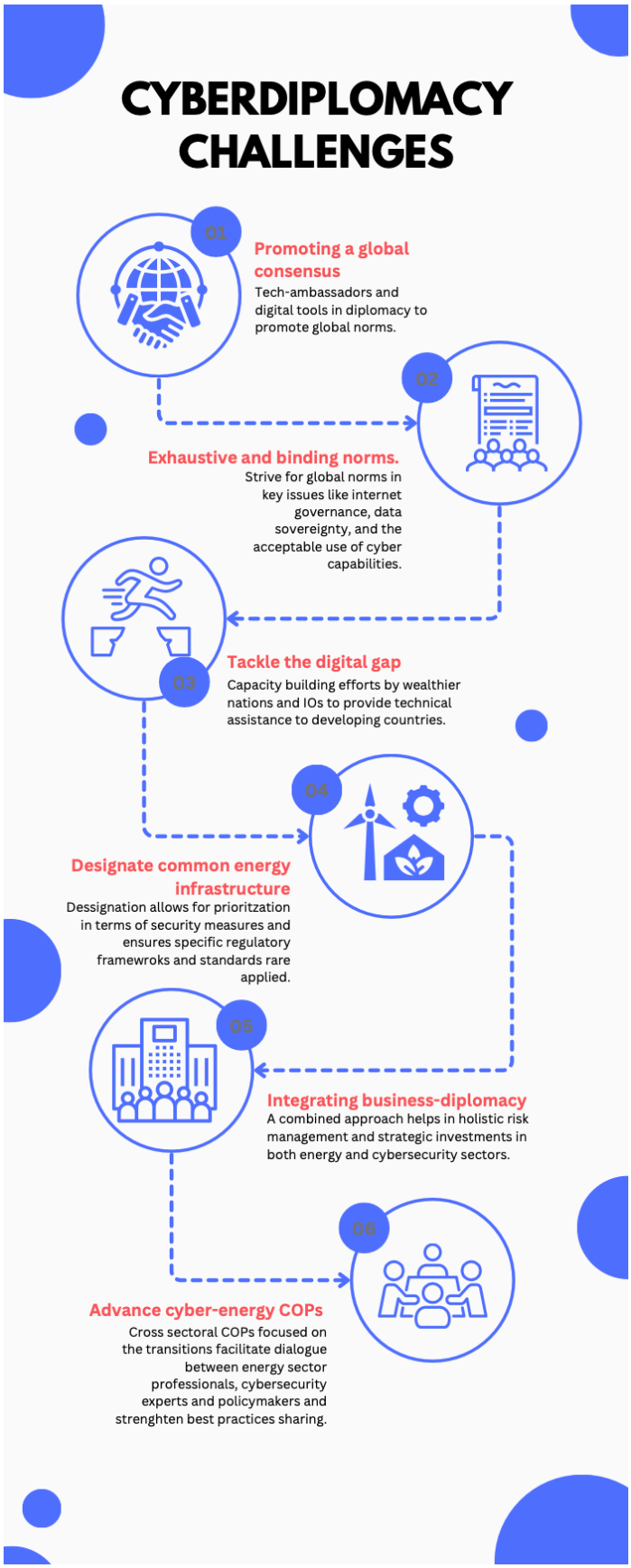
Figure 20: Challenges of Public-Private Partnerships, Own Work.

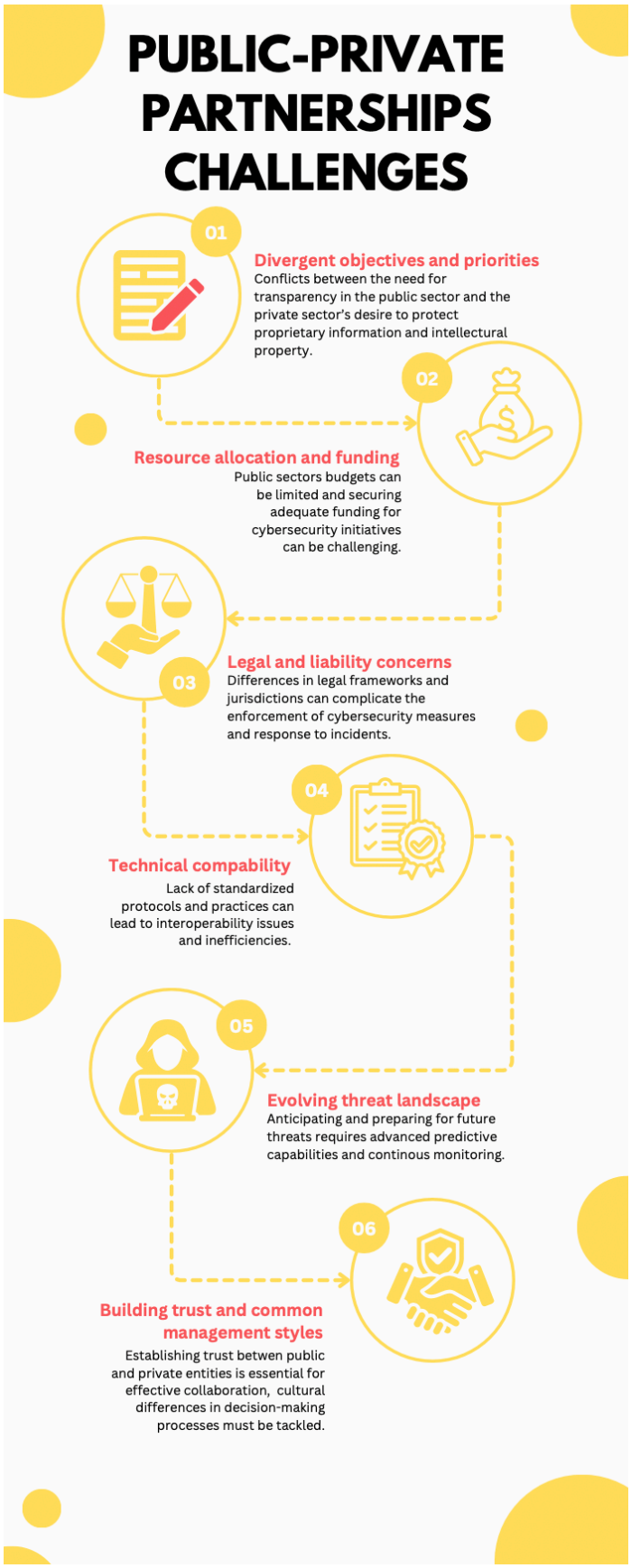



Developing global norms and standards
Progressing a cyber-diplomacy COP
Diplomacy
Appointing *tech* ambassadors
Reducing the risk of conflicts
Fostering a culture of peace
Enhanced threat sharing
Geopolitical analysis
Mitigating attacks from rivals
International agreements
Advocacy efforts
Cyberdiplomacy


Joint research and development efforts
Ownership
Acccess to vast amount of data and threat inelligence
Cybersecurity awareness and training programmes
Technical expertise
Public-Private Partnerships


NATIONAL CYBER SECURITY CHALLENGES
01
Engaging with non-governmental actors
Promote resource pooling among non-governmental entities to bring additional resources including financial investements, tech assets.
02
Risk of abstract strategies
Outlining goals and objectives too broad without providing clear actionable steps for achieving them such as KPIs.
03
Identifying the main threat groups and actors
For tailored defenses, risk assessment and prioritization and strategic planning.
04
Considering geopolitical risks and scenarios
Prioritizing collaborations with other countries and cross-border strategies.
05
Integrating the public sector
Avoiding an overreliance on governmental and military responses which may not adequately integrate the expertise and resources of the private sector.
06
Promoting a centralized architecture
That prioritizes cybersecurity avoiding an inconsistent implementation and a lack of sustained focus on developing and enhancing cybersecurity measures.


CYBERDIPLOMACY CHALLENGES
01
Promoting a global consensus
Tech-ambassadors and digital tools in diplomacy to promote global norms.
02
Exhaustive and binding norms.
Strive for global norms in key issues like internet governance, data sovereignty, and the acceptable use of cyber capabilities.
03
Tackle the digital gap
Capacity building efforts by wealthier nations and IOs to provide technical assistance to developing countries.
04
Designate common energy infrastructure
Dessignation allows for prioritzation in terms of security measures and ensures specific regulatory framewroks and standards rare applied.
05
Integrating business-diplomacy
A combined approach helps in holistic risk management and strategic investments in both energy and cybersecurity sectors.
06
Advance cyber-energy COPs
Cross sectoral COPs focused on the transitions facilitate dialogue between energy sector professionals, cybersecurity experts and policymakers and strenghten best practices sharing.


PUBLIC-PRIVATE PARTNERSHIPS CHALLENGES
01
Divergent objectives and priorities
Conflicts between the need for transparency in the public sector and the private sector's desire to protect proprietary information and intellectural property.
02
Resource allocation and funding
Public sectors budgets can be limited and securing adequate funding for cybersecurity initiatives can be challenging.
03
Legal and liability concerns
Differences in legal frameworks and jurisdictions can complicate the enforcement of cybersecurity measures and response to incidents.
04
Technical compability
Lack of standardized protocols and practices can lead to interoperability issues and inefficiencies.
05
Evolving threat landscape
Anticipating and preparing for future threats requires advanced predictive capabilities and continous monitoring.
06
Building trust and common management styles
Establishing trust betwen public and private entities is essential for effective collaboration, cultural differences in decision-making processes must be tackled.

Conclusion

Critical energy infrastructure has become a primary target for cyberattacks due its significance to national security. From the Stuxnete attack on Iranium nuclear plants in 2010, to the Shamoon's virus impact on Saudi Aramco's facilities in 2012, and the ongoing conflict between Russia and Ukraine demonstrate the complexities of our energy systems' vulnerabilities.
As the critical infrastructure of the energy transition undergoes a profound transformation, driven by the rapid advancements in digitalization and technology, this evolution brings numerous benefits including enhanced efficiency, better resource management, and a significant boost in our ability to integrate renewable energy sources seamlessly.

Digitalized energy shifts empower consumers with detailed insights into their energy consumptions and digitalization supports the development of new business models, fostering a more decentralized and democratized energy market, from peer-to-peer energy trading to virtual power plants.

As countries and regions will continue to invest in and adopt these digital solutions in the energy sector, therefore increasing the potential for significant reductions in carbon emissions and improvements in energy efficiency, the global transition towards a greener and more sustainable future is therefore made increasingly attainable, some key challenges need to be addressed.

A categorization of various types of cyber-attacks and their potential consequences on the new energy infrastructure as smart grids and distributed energy resources show, highlighted by the different possible actors and their motivations, highlight the multifaceted nature of these threats, ranging from state-sponsored attacks to cybercriminals and hacktivists.
Incorporating digital technologies will be a key factor in shaping the industry's future, and adoption, while also reducing costs, yet it is crucial to identify the challenges the energy transition faces today. The risk landscape is growing more complex, demanding more robust cybersecurity measures.

Cybersecurity is a strategic concern that must evolve alongside these transitions, as such, ongoing efforts are essential to ensure that critical energy infrasrtuctures remain resilient and secure as the

global energy landscape reaches its path to sustainability. Policies and frameworks are urgently needed to protect these critical infrastructures, as an urgent imperative, for a coordinate and proactive approach to cybersecurity and to protect critical and digitalized energy infrastructures against the growing threat of cyberattacks.

Cybersecurity policies do not operate in isolation but are deeply interdependent.
International collaboration, particularly in intelligence and knowledge sharing proves to be an essential component in the fight against cyber threats, but it still requires investments and concrete prioritization.

Effective cyber diplomacy can enhance national security strategies by establishing international norms, which in turn, can support efforts to combat cyber terrorism and crime. Managing these interdependencies, however, requires, careful coordination to avoid potential conflicts. Strict national security measures might inadvertently strain international cooperation, or private sector interests might clash with public regulatory frameworks.

What is evident is that while the national and international public sector are fundamental players especially, when it comes to setting out regulations and frameworks for cybersecurity, the active involvement of the private sector is essential for these efforts to be effective.

In the energy sector, the private sector remains a main operator of critical infrastructure and developer of innovative technologies. Private companies possess the expertise, resources, and agility necessary to implement these regulations. Public-privte collaboration is essential to ensure that cybersecurity measures are practical, comprehensive, and capable of addressing the dynamic challenges of the digital age.

Overall, the broader security impacts of cyber-attacks on energy infrastructures touch upon many levels of security - social, economic, political, and reputational security. Still, while this thesis primarily focuses on the cybersecurity aspects of critical energy infrastructures, it is crucial to recognize that these systems remain vulnerable to physical attacks, particularly as the energy sector transitions to renewable sources. The resilience of critical infrastructure cannot be ensured by

cybersecurity measures alone; physical security is equally important in safeguarding against a comprehensive range of threats.

Both the digital and the energy transition are yet to be completed as they continue to evolve, leaving gaps that cyberthreats can exploit. The discussion on future trends in cybersecurity of the energy sector, notably the implication of AI in emerging threats, the increasing integration of critical minerals and the importance of public-private partnerships among others, highlights the neede for adaptation and forward-looking policies.

Bibliography

Accomando, Jane et al., "The Intersection of Energy and Artificial Intelligence: Key Issues and Future Challenges", *Morgan Lewis*, August 12, 2024, https://www.morganlewis.com/pubs/2024/08/the-intersection-of-energy-and-artificial-intelligence-key-issues-and-future-challenges

Agency for the Cooperation of Energy Regulators (European Union) and Council of European Energy Regulators, "Energy Retail and Consumer Protection. 2023 Market Monitoring Report" (September 2023), https://www.acer.europa.eu/sites/default/files/documents/Publications/2023_MMR_Energy_Retail_Consumer_Protection.pdf

Agenzia per la cybersicurezza nazionale, "Strategia Nazionale di Cybersicurezza 2022 – 2026". Available at: https://www.acn.gov.it/portale/strategia-nazionale-di-cybersicurezza

Ahraf, Muqsit and Roberto Bocca, "Fostering Effective Energy Transition: 2023 Edition", *World Economic Forum* (June 2023), https://www3.weforum.org/docs/WEF_Fostering_Effective_Energy_Transition_2023.pdf

Albano, Kevin and Limor Kessem, "The Full Shamoon: How the Devastating Malware Was Inserted Into Networks", *Security Intelligence*, February 15th, 2017, https://securityintelligence.com/the-full-shamoon-how-the-devastating-malware-was-inserted-into-networks/

Alsaaed, Alaa, "The Cyber Attack on Saudi Aramco in 2012", *Asian Journal of Engineering and Technology* 10, no. 2 (2021), https://doi.org/10.51983/ajeat-2021.10.2.3057

Amos, Zac, "Why Cybersecurity for Solar is Crucial – And Difficult", *Hackernoon*, March 16th, 2024, https://hackernoon.com/why-cybersecurity-for-solar-is-crucial-and-difficult

Ang, B.W. and T.S. Ng, "Energy security: Definitions, dimensions and indexes", *Renewable and Sustainable Energy Reviews* 42 (February 2015), https://doi.org/10.1016/j.rser.2014.10.064

Australian Critical Minerals, "Information Security & Cybersecurity – Critical Minerals". Accessed August 28, 2024, https://australiancriticalminerals.com/information-security-cybersecurity/

Baezner, Marie and Patrice Robin, "Stuxnet", *CSS Cyber Defense Project*, ETH Zurich (February 2018), https://www.researchgate.net/publication/323199431_Stuxnet

Baidya, Sanghita, Vidyasagar Potdar, Partha Pratim Ray, Champa Nandi, "Reviewing the opportunities, challenges and future directions for the digitalization of energy", *Energy Research & Social Science* 81 (2021), https://doi.org/10.1016/j.erss.2021.102243

Baldoni, Roberto and Luca Montanari, "2015 Italian Cybersecurity Report: Un Framework Nazionale per la Cyber Security", Research Center of Cyber Intelligence and Information Security Center, *Sapienza Università di Roma, Laboratorio Nazionale CINI di Cyber Security Consorzio Interuniversitario Nazionale per l'Informatica* (Febbraio 2016), https://www.cybersecurityframework.it/sites/default/files/CSR2015_web.pdf

Balzani, Vincenzo, "Saving the planet and the human society: renewable energy, circular economy, sobriety", *Substantia: An International Journal of the History of Chemistry* 3, no. 2 (2019), https://doi.org/10.13128/Substantia-696

Banco Santander, "Ransomware". Accessed August 30th, 2024, https://www.bancosantander.es/en/glosario/ransomware

Bendiek, Annegret, "European cybersecurity policy", *SWP Research Report No. RP 13/2012*, Stiftung Wissenschaft und Politik (SWP), Berlin (2012), https://hdl.handle.net/10419/253129

Bennagi, Aseel, Obaida AlHousrya, Daniel T. Cotfas, Petru A. Cotfas, "Comprehensive study of the artificial intelligence applied in renewable energy", *Energy Strategy Reviews* 54 (July 2024), https://www.sciencedirect.com/science/article/pii/S2211467X24001536#sec6

Booth, Adrian, Aman Dhingra, Sven Heiligtag, Mahir Nayfeh, and Daniel Wallance, "Critical infrastructure companies and the global cybersecurity threat. How the energy, mining and materials industries can meet the unique challenges of protecting themselves in a digital world", *McKinsey & Company* (2019), https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/Critical%20infrastructure%20companies%20and%20the%20global%20cybersecurity%20threat/Critical-infrastructure-companies-and-the-global-cybersecurity-threat-vF.pdf

Bossier, Adam M. and Tamar Berenblum, "Introduction: new directions in cybercrime research", *Journal of Crime and Justice* 42, no. 5 (2019), https://doi.org/10.1080/0735648X.2019.1692426

Bouramdane, Ayat-Allah, "Cyberattacks in Smart Grids: Challenges and Solving the Multi-Criteria Decision-Making for Cybersecurity Options, Including Ones That Incorporate Artificial Intelligence, Using an Analytical Hierarchy Process", *J. Cybersecurity Priv*. 3, no. 4 (2023), https://doi.org/10.3390/jcp3040031

Boutin, Berenice, "State Responsibility in Relation to Military Applications of Artificial Intelligence", *Leiden Journal of International Law* (2022), https://ssrn.com/abstract=4214292

Broadhurst, Roderic Ph.D., and Lennon Y. C. Chang Ph.D., "Cybercrime in Asia: Trends and Challenges" in *Handbook of Asian Criminology* (eds. Liu, J., Hebenton, B., Jou, S), (Springer: New York, 2012), https://link.springer.com/chapter/10.1007/978-1-4614-5218-8_4#citeas

Bronk, Christopher and Eneken Tikk-Ringas, "The Cyber Attack on Saudi Aramco", *Survival. Global Politics and Strategy* 55, no. 2 (2013), https://doi.org/10.1080/00396338.2013.784468

Brown, Kathi Ann, *Critical Path. A Brief Critical Infrastructure Protection in the United* States (Spectrum Publishing Group Inc: Fairfax, Virginia, 2006), https://cip.gmu.edu/wp-content/uploads/2016/06/CIPHS_CriticalPath.pdf

Bilge, Leyla, Tudor Dumitraş, "Before we knew it: an empirical study of zero-day attacks in the real world", *CCS Proceedings of the 2012 ACM Conference on Computer and Communications Security,* https://doi.org/10.1145/2382196.2382284

Cambers, Joseph, Caitlin Robinson, and Matthew Scott, "Digitalization without detriment: A research agenda for digital inclusion in the future energy system", *People, Place and Policy Online* 16, no. 2 (2023), https://www.researchgate.net/publication/364626784_Digitalisation_without_detriment_A_research_agenda_for_digital_inclusion_in_the_future_energy_system

Carter, Russel A., "Mining is now a cyber-threat target", *Engineering and Mining Journal* (July 2016), https://www.e-mj.com/features/mining-is-now-a-cyber-threat-target/

CESER, Potential Benefits and Risks of Artificial Intelligence for Critical Energy Infrastructure (April 2024), https://www.energy.gov/sites/default/files/2024-04/DOE%20CESER_EO14110-AI%20Report%20Summary_4-26-24.pdf

Cherp, Aleh and Jessica Jewell, "The concept of energy security: Beyond the four As", *Energy Policy* 75 (December 2017): 416, https://doi.org/10.1016/j.enpol.2014.09.005

Chowdhury, Nabin, and Vasileios Gkioulos, "Cyber security training for critical infrastructure protection: A literature review", *Computer Science Review* 40 (May 2021), https://doi.org/10.1016/j.cosrev.2021.100361

Cisco, "How Do OT and IT Differ?". Accessed August 30, 2024, https://www.cisco.com/c/en/us/solutions/internet-of-things/what-is-ot-vs-it.html

Cisco, "What Is a Worm?". Accessed August 30, 2024, https://www.cisco.com/c/en/us/products/security/what-is-a-

worm.html#:~:text=A%20worm%20is%20a%20type,files%20or%20introduce%20other%20malware

Clemente, Jason F., "Cybersecurity for critical energy infrastructure", (Thesis), Calhoun: The NPS Institutional Archive (September 2018), https://upload.wikimedia.org/wikipedia/commons/0/08/CYBER_SECURITY_FOR_CRITICAL_ENERGY_INFRASTRUCTURE_%28IA_cybersecurityfor1094560378%29.pdf

Cohen, Ariel, "The Promise and Peril of AI in the Energy Sector", *Forbes*, July 3, 2023. Available at https://www.forbes.com/sites/arielcohen/2023/06/29/the-promise-and-peril-of-ai-in-energy/

Cybersecurity & Infrastructure Security Agency, "Critical Infrastructure Sectors". Accessed August 20, 2024, https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

Cassotta, Sandra and Roman Sidortsov, "Sustainable cybersecurity? Rethinking approaches to protecting energy infrastructure in the European High North", *Energy Research & Social Sciences* 51 (May 2019), https://vbn.aau.dk/en/publications/sustainable-cybersecurity-rethinking-approaches-to-protecting-ene-2

Ceser, "CyOTE Case Study: Crashoverride/Industroyer", February 7, 2022, https://cyote.inl.gov/cyote/wp-content/uploads/2022/11/CRASHOVERRIDE-CyOTE-Case-Study_508_FINAL.pdf

Center for Strategic and International Studies, "Global Cyber Strategies Index". Accessed August 19, 2024, https://www.csis.org/programs/strategic-technologies-program/archives/cybersecurity-and-governance/global-cyber

Daricili, A. Burak and Soner Çelik, "National Security 2.0: The Cyber Security of Critical Infrastructure", *Perceptions* 26, no. 2 (2021), https://dergipark.org.tr/en/download/article-file/2181981

Devanny, Joe and Russell Buchan, "Mexico's National Cybersecurity Policy: Progress Has Stalled Under AMLO", *Carnegie Endowment for International Peace*, May 28, 2024, https://carnegieendowment.org/research/2024/05/mexicos-national-cybersecurity-policy-progress-has-stalled-under-amlo?lang=en

Dyagileva, Olena et al., "The use of the mechanism of public-private partnership in the investment processes management in the context of digitalization", *Cuestiones Politicas* 40, no. 72 (2022), https://produccioncientificaluz.org/index.php/cuestiones/article/view/37767

European Commission "In focus: Energy and smart cities", July 13, 2022, https://commission.europa.eu/news/focus-energy-and-smart-cities-2022-07-13_en

European Commission, "Questions and Answers: EU action plan on digitalizing the energy system", October 18, 2022, https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_6229

European Commission and Joint Research Centre, *Clean Energy Technology Observatory, smart grids in the European Union: status report on technology development, trends, value chains and markets* (2022), https://data.europa.eu/doi/10.2760/276606

European Commission, "Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)", https://digital-strategy.ec.europa.eu/en/policies/nis2-directive (Came into force January 16th, 2023).

European Commission EU-NATO Task Force, *Final assessment report on strengthening our resilience and protection of critical infrastructure*, June 29, 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3564

European Commission, "EU Adaptation Strategy". Accessed August 17, 2024, https://climate.ec.europa.eu/eu-action/adaptation-climate-change/eu-adaptation-strategy_en#:~:text=The%20European%20Commission%20adopted%20its,become%20climate%20resilient%20by%202050.

European Commission, "Cybersecurity Policies". Accessed August 21, 2024, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies

European Commission, "Energy communities". Accessed August 21, 2024, https://energy.ec.europa.eu/topics/markets-and-consumers/energy-consumers-and-prosumers/energy-communities_en#:~:text=Energy%20communities%20allow%20local%20communities,field%20with%20other%20market%20actors.

European Commission "The Cybersecurity Strategy". Accessed August 21, 2024, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

European Commission "The EU Cyber Solidarity Act". Accessed August 21, 2024, https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity

European Council and Council of the European Union "Fit for 55". Accessed August 22, 2024, https://www.consilium.europa.eu/en/policies/green-deal/fit-for-55/#:~:text=for%2055%20package%3F-,What%20is%20the%20Fit%20for%2055%20package%3F,Council%20and%20the%20European%20Parliament.

European Parliament, *Directive 2008/115/EC of the European Parliament and the Council of 16 December 2008 on common standards and procedures in Member States for returning illegally staying third-country nationals*, https://eur-lex.europa.eu/eli/dir/2008/115/oj

European Parliament "EU AI Act: first regulation on artificial intelligence", June 18, 2024, https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

Elmaghraby, Adel S. and Michael M. Losavio, "Cyber security challenges in Smart Cities: Safety, security and privacy", *J Adv Res* 5, no. 4 (July 2014), https://doi.org/10.1016/j.jare.2014.02.006

El Zein Musadag, and Girma Gebrensenbet "Digitalization in the Renewable Energy Sector", *Energies* 17, no. 9 (2024), https://doi.org/10.3390/en17091985

Enel "Blockchain, a permanent revolution", February 7, 2018, https://www.enel.com/company/stories/articles/2018/02/blockchain-energy-focus-on-santiago-chile

Eni A Just Transition (Report) (2023), https://www.eni.com/content/dam/enicom/documents/eng/sustainability/2023/eni-for-2023-just-transition-eng.pdf

Eni "Main financial risks". Accessed August 22, 2024, https://www.eni.com/en-IT/investors/risk-management/principal-financial-risks.html

Entezari, Ashkan, Alireza Aslani, Rahim Zahedi, Younes Noorollahi "Artificial intelligence and machine learning in energy systems: A bibliographic perspective", *Energy Strategy Reviews* 45 (2023), https://doi.org/10.1016/j.esr.2022.101017

ESCAP "Smart Cities in Southeast Asia: A Landscape Review" (2022), https://www.zotero.org/yasminadionisi/search/escap

EU Artificial Intelligence Act. Date of entry into force: 2 February 2025, https://artificialintelligenceact.eu/article/5/

EU Cyber Capacity Building Network (EU CyberNet) "The EU's International Cooperation on Cyber Capacity Building" (2023), https://www.eucybernet.eu/wp-content/uploads/2023/11/operational-guidance-for-the-eu-international-cooperation-on-ccb-1-1.pdf

EU Science Hub "Critical infrastructure protection". Accessed August 28, 2024, https://joint-research-centre.ec.europa.eu/scientific-activities-z/critical-infrastructure-protection_en

Farwell James P. and Rafal Rohozinski, "Stuxnet and the Future of Cyber War", *Survival* 53, no. 1 (2011): 24-40, https://cyberdialogue.ca/wp-content/uploads/2011/03/James-Farwell-and-Rafal-Rohozinski-Stuxnet-and-the-Future-of-Cyber-War.pdf

Faghani Mohammed Reza and Uyen Trang Nguyen, "A Study of Malware Propagation via Online Social Networking" in *Mining Social Networks and Security Informatics* (eds. Tansel Özyer et. al) (Springer: New York, 2013), https://link.springer.com/chapter/10.1007/978-94-007-6359-3_13

Faquir Dharmesh et. al, "Cybersecurity in smart grids, challenges and solutions", *AIMS Electronics and Electrical Engineering* 5, no. 1 (2020), https://www.aimspress.com/aimspress-data/electreng/2021/1/PDF/ElectronEng-05-01-002.pdf

Fazle Rabbi Mohammad, József Popp, Domicián Máté, and Sándor Kovács, "Energy Security and Energy Transition to Achieve Carbon Neutrality", *Energies* 15, no. 21 (October 2022), https://doi.org/10.3390/en15218126

Fortinet, "Information Technology (IT) vs. Operational Technology (OT) Cybersecurity". Accessed August 30, 2024, https://www.fortinet.com/resources/cyberglossary/it-vs-ot-cybersecurity

Fortinet, "Malware vs Viruses vs Worms". Accessed August 30, 2024, https://www.fortinet.com/resources/cyberglossary/malware-vs-virus-vs-worm#:~:text=What%20is%20the%20difference%20between%20a%20virus%20and%20a%20worm,a%20user%20or%20via%20software

Fortinet, "Man-in-the-Middle Attack: Types and Examples". Accessed August 28, 2024, https://www.fortinet.com/resources/cyberglossary/man-in-the-middle-attack

Freeman Sarah G. et. al, "Attack Surface of Wind Energy Technologies in the United States", Idaho National Laboratory (January 2024), https://inl.gov/content/uploads/2024/02/INL-Wind-Threat-Assessment-v5.0.pdf?utm_medium=email&utm_source=govdelivery

Frei Jasper, "Israel's National Cybersecurity and Cyberdefense Posture", *Cyber Defense Project* (CDP), Center for Security Studies (CSS), ETH Zürich, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-09-Israel.pdf

Gallais C. and E. Filiol, "Critical Infrastructure. Where do We Stand Today?", Journal of Information Warfare 16, no. 1 (Winter 2017), https://www.jstor.org/stable/2650287

Giuli Marco, "Bringing Paris into the EU'S Energy Infrastructure Policy: What Future for Gas?", IAI Commentaries (2020), https://www.iai.it/it/pubblicazioni/bringing-paris-eus-energy-infrastructure-policy-what-future-gas

Hamed Taherdoost, "Blockchain Integration and Its Impact on Renewable Energy", *Computers* 13, no. 4 (2024), https://doi.org/10.3390/computers13040107

Hampson Michelle, "Yes, Your Electric Vehicle Could Be Hacked", *IEEE Spectrum*, August 24th, 2023, https://spectrum.ieee.org/ev-hacks

Heitzenrater Chad, "Cyber Attacks Reveal Uncomfortable Truths About U.S. Defenses", *RAND Corporation*, September 21st, 2023, https://www.rand.org/pubs/commentary/2023/09/cyber-attacks-reveal-uncomfortable-truths-about-us.html

Heldeweg Michiel A., Maurits Sanders, and Marc Harmsen, "Public-private or private-private energy partnerships? Toward good energy governance in regional and local green gas projects", *Energy, Sustainability and Society* 5, no. 9 (2015), https://doi.org/10.1186/s13705-015-0038-8

Hove Anders, Michal Meidan, and Philip Andrews-Speed, "Software versus hardware: How China's institutional setting helps and hinders the clean energy transition", *OIES Paper:CE No. 2*, The Oxford Institute for Energy Studies, Oxford (2021), https://www.econstor.eu/handle/10419/253276

Ince Matt and Erin Sikorsky, "The Uncomfortable Geopolitics of the Clean Energy Transition", Lawfare, December 13th, 2023, https://www.lawfaremedia.org/article/the-uncomfortable-geopolitics-of-the-clean-energy-transition

Iberdrola, "How can blockchain be used to certify the source of green energy?". Accessed August 21st, 2024, https://www.iberdrola.com/innovation/blockchain-energy#:~:text=We%20believe%20blockchain%20is%20a,consumption%20of%20100%20%25%20renewable%20energy

Iberdrola, "Smart grids, intelligent electricity networks". Accessed August 21st, 2024, https://www.iberdrola.com/about-us/what-we-do/smart-grids#:~:text=The%20traditional%20electricity%20grid%20is,increasing%20efficiency%20and%20energy%20savings.

IBM, "What are insider threats". Accessed August 21, 2024, https://www.ibm.com/topics/insider-threats#:~:text=IBM-

,What%20are%20insider%20threats%3F,their%20accounts%20hijacked%20by%20cybercriminals

IBM, "What is blockchain security?". Accessed August 21st, 2024, https://www.ibm.com/topics/blockchain

IBM, "What is incident response?". Accessed August 30, 2024, https://www.ibm.com/topics/incident-response

IE, UncoverIE, "Cyber diplomacy and cybersecurity: guardians of the digital realm", July 16, 2024, https://www.ie.edu/uncover-ie/cyber-diplomacy-and-cybersecurity-guardians-of-the-digital-realm/

Imperva, "Social Engineering". Accessed August 21st, 2024, https://www.imperva.com/learn/application-security/social-engineering-attack/

Imperva, "Sybil Attack". Accessed August 22nd, 2024, https://www.imperva.com/learn/application-security/sybil-attack/#:~:text=A%20Sybil%20attack%20uses%20a,of%20influence%20in%20the%20network

Imperva, "Man in the middle attack". Accessed August 30th, 2024, https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/

International Energy Agency, Energy and Climate Change. World Energy Outlook Special Report (2015), https://www.iea.org/reports/energy-and-climate-change

International Energy Agency, The Role of Critical Minerals in Clean Energy Transitions (May 2021), https://www.iea.org/reports/the-role-of-critical-minerals-in-clean-energy-transitions

International Energy Agency, Electricity Grids and Secure Energy Transitions. Enhancing the foundations of resilient, sustainable and affordable power systems (2022), https://iea.blob.core.windows.net/assets/ea2ff609-8180-4312-8de9-494bcf21696d/ElectricityGridsandSecureEnergyTransitions.pdf

International Energy Agency, Unlocking the Potential of Distributed Energy Resources – Analysis (2022), https://www.iea.org/reports/unlocking-the-potential-of-distributed-energy-resources

International Energy Agency (IEA), OECD, World Energy Outlook (2023), https://www.oecd-ilibrary.org/energy/world-energy-outlook-2023_827374a6-en

International Energy Agency, "Blockchain Pilot Grants: Critical minerals". Last updated December 12th, 2023. Available at: https://www.iea.org/policies/16651-blockchain-pilot-grants-critical-minerals

International Hydropower Association, “World’s largest hydro-PV station now operating in China”, July 28, 2023, https://www.hydropower.org/news/worlds-largest-hydro-pv-station-now-operating-in-china

International Labor Organization, Green jobs, green economy, just transition and related concepts: A review of definitions developed through intergovernmental processes and international organizations (June 2023), https://www.ilo.org/publications/green-jobs-green-economy-just-transition-and-related-concepts-review

International Waterpower and Dam Construction Magazine, “Evolving cybersecurity threats to hydropower dams”. June 12th, 2024, https://www.waterpowermagazine.com/analysis/evolving-cybersecurity-threats-to-hydropower-dams/

International Renewable Energy Agency, A New World: The Geopolitics of the Energy Transition (2019), https://www.irena.org/publications/2019/Jan/A-New-World-The-Geopolitics-of-the-Energy-Transformation

International Renewable Energy Agency, Renewable energy and jobs: Annual review 2023 (September 2023), https://www.irena.org/Publications/2023/Sep/Renewable-energy-and-jobs-Annual-review-2023

International Renewable Energy Agency, Geopolitics of the Energy Transition, Digital Report (2024), https://www.irena.org/Digital-Report/Geopolitics-of-the-Energy-Transition-Critical-Materials

International Telecommunications Union, “Digital inclusion of all”. Accessed August 22, 2024, https://www.itu.int/en/mediacentre/backgrounders/Pages/digital-inclusion-of-all.aspx

Johnson Controls, “Smart Buildings”. Accessed August 28, 2024, https://www.johnsoncontrols.com/smart-buildings

Judson E. et al., “The centre cannot (always) hold: Examining pathways towards energy system de-centralisation”, *Renewable and Sustainable Energy Reviews* 118 (2020), https://doi.org/10.1016/j.rser.2019.109499

Jixuan Zheng and Lin Li, “Smart Meters in Smart Grid: An Overview”, *IEEE Green Technologies Conference* (2013), https://ieeexplore.ieee.org/document/6520030

Kallberg Jan, “Strategic Cyberwarf Theory – A Foundation for Designing Decisive Strategic Cyber Operations”, *The Cyber Defense Review* 1, no. 1 (Spring 2016), https://www.jstor.org/stable/26267302

Kaspersky, “What’s the Difference between a Virus and a Worm?”. Accessed August 30, 2024, https://www.kaspersky.com/resource-center/threats/computer-viruses-vs-worms

Khalid Mohammed, “Smart grid and renewable energy systems: Perspectives and grid integration challenges”, *Energy Strategy Reviews* 51 (2024), https://doi.org/10.1016/j.esr.2024.101299

Klarian, “Hacktivists Vs The Oil and Gas Industry. Tackling challenges in the new era of cybersecurity, post covid-19”. August 24, 2021, https://klarian.com/blog/tackling-challenges-in-the-new-era-of-cyber-security

Kumar Gupta Krishna et al., “The role of cyber security in advancing sustainable digitalization: Opportunities and challenges”, *Journal of Decision Analytics and Intelligent Computing* 3, no. 1, DOI: 10.31181/jdaic10018122023g

Kaspersky, “ATT&CK for ICS: Industroyer”. Accessed August 30, 2024, https://www.kaspersky.com/enterprise-security/mitre/industroyer

Kushner David, “The real story of Stuxnet. How Kaspersky Lab tracked down the malware that stymied Iran’s nuclear-fuel enrichment program”, *IEEE Spectrum*, February 26, 2013, updated May 21, 2024, https://spectrum.ieee.org/the-real-story-of-stuxnet

Lefèvre Laurent and Anne-Cécile Orgerie, “Designing and evaluating an energy efficient Cloud”, *The Journal of Supercomputing* 51 (2010), https://doi.org/10.1007/s11227-010-0414-2

Lemieux Frederic, *Current and Emerging Trends in Cyber Operations* (London: Palgrave Macmillan UK, 2015).

Li Shancang and Li Da Xu, “The internet of things: a survey”, *Information Systems Frontiers* 17, no. 2 (2015), https://doi.org/10.1007/s10796-014-9492-7

Li Yuchong and Qinghui Liu, “A comprehensive review of cyber-attacks and cyber security; Emerging trends and recent developments”, *Energy Reports* 7, no. 8 (2021), https://doi.org/10.1016/j.egyr.2021.08.126

Lindsörm Madeleine and Stefan Olsson, “The European Programme for Critical Infrastructure Protection” in *Crisis Management in the European Union. Cooperation in the Face of Emergencies* (Springer, 2009).

Lombard Odier, “The countries leading the energy transition”. Accessed July 12, 2024, https://www.lombardodier.com/contents/corporate-news/responsible-capital/2024/april/picking-the-winners-in-the-energ.html

Mandiant, “Advanced Persistent Threats (APTs)”. Accessed August 28th, 2024, https://www.mandiant.com/resources/insights/apt-groups

Manea Andrei, “Enhancing cyber security in the energy transition”, DNV (February 2023), https://www.dnv.com/article/enhancing-cyber-security-in-the-energy-transition-249155/

Metzger Jan, "The concept of critical infrastructure protection" in *Business and Security. Public-Private Sector relationships in a New Security Environment* (Stockholm: Sipri, 2004), https://doi.org/10.1093/oso/9780199274505.003.0018

Mitchell Paul and Clement Soh, "Cybersecurity in Energy and resources", EY. Accessed August 21st, 2024, https://www.ey.com/en_gl/industries/energy-resources/mining-metals-cybersecurity

Moomaw William and Mihaela Papa, "Creating a mutual gains climate regime through universal clean energy services", *Climate Policy* 12, no. 4 (January 2012), https://doi.org/10.1080/14693062.2011.644072

Mosavi Amir et al., "State of the Art of Machine Learning Models in Energy Systems, a Systematic Review", *Energies* 12, no. 7 (2019), https://doi.org/10.3390/en12071301

Moteff John, Claudia Copeland, John Fischer, "Critical Infrastructures: What Makes an Infrastructure Critical?", Defense Technical Information Center (2015), http://www.fas.org/sgp/crs/homesec/RL30153.pdf

Motlagh Naser Hossein, Mahsa Mohammadrezaei, Julian Hunt, and Benham Zaker, "Internet of Things (IoT) and the Energy Sector", *Energies* 13, no. 2 (2020), https://doi.org/10.3390/en13020494

National Cyber Security Center UK, "Denial of service (DoS) guidance". Accessed August 30th, 2024, https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection

National Research Council, *Terrorism, and the Electric Power Delivery System* (Washington D.C.: National Academies Press, 2012).

Newman Andrew, "Why Do Hacks Happen? Four Ubiquitous Motivations Behind Cybersecurity Attacks", *Forbes*, July 13th, 2022, https://www.forbes.com/councils/forbestechcouncil/2022/07/13/why-do-hacks-happen-four-ubiquitous-motivations-behind-cybersecurity-attacks/

Nexus Integra, *Digital transformation in 4 large industrial sectors: water, ceramics, oil and energy* (2024), https://nexusintegra.io/ebook-digital-transformation-4-large-industrial-sectors/

NASA Science, "Responding to Climate Change". Accessed August 17th, 2024, https://science.nasa.gov/climate-change/adaptation-mitigation/

Organization for Security and Co-Operation in Europe (OSCE), Energy Security (2017) https://www.osce.org/resources/factsheets/energy-security

Pant R., S. Thacker, J.W. Hall, S. Barr, and D. Alderson, "Building an integrated assessment methodology for critical infrastructure risk assessment", *Society for Risk Analysis Annual Meeting, Maryland,* US, 8-11 December 2013, https://www.itrc.org.uk/itrcpublications/building-an-integrated-assessment-methodology-for-critical-infrastructure-risk-assessment/

Pasquazzi Simone and Adriano Savarino Morelli, "Cyber-attacks, geopolitica e settore energetico" in *Europea* 1 (June 2023), DOI: 10.53136/97912218086436

Pawlak Patrick and Aude Géry, "Why the World Needs a New Cyber Treaty for Critical Infrastructure", *Carnegie Endowment*, March 28, 2024, https://carnegieendowment.org/research/2024/03/why-the-world-needs-a-new-cyber-treaty-for-critical-infrastructure?lang=en&center=europe

Pourmirza Zoya, *Cybersecurity in Centralised vs Decentralised Energy Systems*, Supergen Energy Networks (2023), https://www.ncl.ac.uk/media/wwwnclacuk/supergenenergynetwork/files/Cyber%20Security%20in%20Centralised%20vs%20Decentralised%20Energy%20Systems%20(2).pdf

Primetica Branko and Joe Helfrich, "Enabling the SmartGrid through Cloud Computing", *EGlobal Tech* (2012), https://www.energy.gov/sites/prod/files/Friday_Trinity_Ballroom_3_0855_Primetica_final.pdf

Qi Junjan and Adam Hahn, and Cheng-Chiang Liu," Cybersecurity for distributed energy resources and smart inverters", IET Cyber-Physical Systems: Theory & Applications 1, no. 1 (2016), https://doi.org/10.1049/iet-cps.2016.0018

Renewable Energy Institute, "Blockchain for the Renewable Energy Industry". Accessed August 21st, 2024, https://www.renewableinstitute.org/blockchain-for-the-renewable-energy-industry/

R. Kane Bridget et al., "Threats to Critical Infrastructure. A Survey", *RAND*, June 11th, 2024, https://www.rand.org/pubs/research_reports/RRA2397-2.html

Repsol, "What are smart or digital meters?", September 11, 2023, https://www.repsol.com/en/energy-and-the-future/technology-and-innovation/smart-meters/index.cshtml

Reuters, "Hackers hit Italian oil company's Eni computer networks". September 1, 2022, https://www.reuters.com/business/energy/hackers-hit-italian-oil-company-enis-computer-networks-bloomberg-news-2022-08-31/

Rinaldi Gianmario, Michele Cucuzella, Prathyush P. Menon, Antonella Ferrara, Christopher Edwards, "Load Altering Attacks Detection, Reconstruction and Mitigation for Cyber-Security in Smart Grids with Battery Energy Storage Systems", *European Control Conference (ECC)*, IEEE (2023), https://ieeexplore.ieee.org/abstract/document/9838515/authors#authors

Rundee Daniel F. and Austin Hardman, "Elevating the Role of Critical Minerals for Development and Security", *Center for Strategic & International Studies*, September 1, 2023, https://www.csis.org/analysis/elevating-role-critical-minerals-development-and-security

Rydén Sonesson Tove, "Governance and interdependencies of critical infrastructures: Exploring mechanisms for cross-sector resilience", *Safety Science* 142 (October 2021), https://www.sciencedirect.com/science/article/pii/S0925753521002277

Sabillon Regner, Victor Cavaller, and Jeimy Cano, "National Cyber Security Strategies: Global Trends in Cyberspace", *International Journal of Computer Science and Software Engineering* 5, no. 5 (May 2016), https://ijcsse.org/published/volume5/issue5/p1-V5I5.pdf

Schmitt N.M., "Peacetime Cyber Responses and Wartime Cyber Operations under International Law. An Analytical Vade Mecum", *Harvard National Security Journal* 8 (2017), https://www.scirp.org/reference/referencespapers?referenceid=2476198

Semih Sonkor Muammer, Borja García de Soto, "Operational Technology on Construction Sites: A Review from the Cybersecurity Perspective", *Journal of Construction Engineering and Management* 147, no. 12 (2021), https://doi.org/10.1061/(ASCE)CO.1943-7862.0002193

SentinelOne, "The Democratization of Nation-State Actor" (2017), https://go.sentinelone.com/rs/327-MNM-087/images/SEN0202-Democratization_of_Nation_State_Attacks.pdf

Siddarth Sareen, "Digitalisation and social inclusion in multi-scalar smart energy transitions", *Energy Research & Social Science* 81 (2021), https://www.sciencedirect.com/science/article/pii/S2214629621003443

Sims Ralph E.H., "Can Energy Technologies Provide Energy Security and Climate Change Mitigation?", *Energy and Environmental Challenges to Security* (2009), https://doi.org/10.1007/978-1-4020-9453-8_19

Smart Energy International, "A guide to France's Linky smart meter", December 27, 2018, https://www.smart-energy.com/features-analysis/smart-meters-101-frances-linky-electricity-meters/

Singh Udayan and Samarth Singh, "Future research directions to facilitate climate action and energy transitions", *Energy and Climate Change* 4 (December 2023), https://doi.org/10.1016/j.egycc.2022.100092

Staggs Jason, David Ferlemann, and Sujeet Shenoi, "Wind farm security: attack surface, targets, scenarios and mitigation", *Information Journal of Critical Infrastructure Protection* 17 (June 2017), https://doi.org/10.1016/j.ijcip.2017.03.001

Studebaker Defense Group, "The Impact of Cyberwarfare in National and Global Human Security" (2024), https://www.studebaker.group/the-impact-of-cyber-physical-warfare-in-national-and-global-human-security/

Światowiec-Szczepańska Justyna and Stepién Beata, "Drivers of Digitalization in the Energy Sector – The Managerial Perspective from the Catching Up Economy", *Energies* 15, no. 4 (2022), https://www.mdpi.com/1996-1073/15/4/1437

Tabanski, Lior. "Critical Infrastructure Protection against Cyber Threats." *Military and Strategic Affairs* 3, no. 2 (2011). https://www.inss.org.il/wp-content/uploads/2017/02/FILE1326273687-1.pdf

Temple-Raston, Dina. "A 'Worst Nightmare' Cyberattack: The Untold Story of the SolarWinds Hack." *NPR*, April 16, 2021. https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack

Talihärm, Anna-Maria. "Towards Cyberspace: Managing Cyberwar Through International Cooperation." *UN Chronicle*, Vol. L. Security, no. 2 (August 2013). https://www.un.org/en/chronicle/article/towards-cyberpeace-managing-cyberwar-through-international-cooperation

Tennet. "TenneT Unlocks Distributed Flexibility via Blockchain." May 2, 2017. https://netztransparenz.tennet.eu/tinyurl-storage/detail/tennet-unlocks-distributed-flexibility-via-blockchain/

Tuballa, Maria Lorena, and Michael Lochinvar Abundo. "A Review of the Development of Smart Grid Technologies." *Renewable and Sustainable Energy Reviews* 59 (2016). https://doi.org/10.1016/j.rser.2016.01.011

Tvaronavičienė, Manuela, Tomas Plėta, Silvia Della Casa, and Juozas Latvys. "Cyber Security Management of Critical Energy Infrastructure in National Cybersecurity Strategies: Cases of USA, UK, France, Estonia and Lithuania." *Insights into Regional Development* 24, no. 4 (2020). http://dx.doi.org/10.9770/IRD.2020.2.4(6)

United Nations, Division for Sustainable Development Goals Department of Economic and Social Affairs. *Leveraging Energy Action for Advancing the Sustainable Development* (2021). https://sdgs.un.org/sites/default/files/2021-06/2021-POLICY%20BRIEFS_3.pdf

United Nations, United Nations Framework Convention on Climate Change. *Concluded at New York on 9 May 1992*. https://treaties.un.org/doc/source/RecentTexts/unfccc_eng.pdf

United Nations Office of Counter-Terrorism. *The Protection of Critical Infrastructure Against Terrorist Attacks: Compendium of Good Practices* (2022). https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2225521_compendium_of_good_practice_web.pdf

United Nations Office of Counter-Terrorism. "Opening Remarks by Vladimir Voronkov: High-Level Hybrid Event to Launch the Updated United Nations Compendium of Good Practices on the Protection of Critical Infrastructure against Terrorist Attacks", June 5, 2023. https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/230605_usg_opening_remarks_cip_launch_madrid_as_delivered.pdf

United Nations Office of Counter-Terrorism. "Cybersecurity and New Technologies." Accessed August 19, 2024. https://www.un.org/counterterrorism/cybersecurity

United States Office of Energy Efficiency & Renewable Energy. "Protecting Wind Energy Systems from Cyberattacks." May 21, 2024. https://www.energy.gov/eere/wind/articles/protecting-wind-energy-systems-cyberattacks

US Department of Energy – Office of Cybersecurity, Energy Security, and Emergency Response (CESER). *Potential Benefits and Risks of Artificial Intelligence for Critical Energy Infrastructure* (April 2024). https://www.energy.gov/sites/default/files/2024-04/DOE%20CESER_EO14110-AI%20Report%20Summary_4-26-24.pdf

Van de Graaf Thijs and Hans Kribbe, Energy diplomacy: Europe's new strategic mission, Brussels Institute for Geopolitics (March 2024), https://big-europe.eu/publications/big003-energy-diplomacy

Wells, Emily M., Mariel Boden, Ilana Tseytlin, Igor Linkov. "Modeling Critical Infrastructure Resilience under Compounding Threats: A Systematic Literature Review." *Progress in Disaster Science* 15 (October 2022). https://doi.org/10.1016/j.pdisas.2022.100244

Wheeler, Tom. "The Three Challenges of AI Regulation." *Brookings*, June 15, 2023. https://www.brookings.edu/articles/the-three-challenges-of-ai-regulation/

White House (The). "FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence." October 30, 2023. https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/

White House Administrative Office. "The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets." February 1, 2003. https://rosap.ntl.bts.gov/view/dot/33977/titleCreatorYear/items/E8WZ6ZVR/item-details

Williams, Kevin. "'Cyber-Physical Attacks' Fueled by AI Are a Growing Threat, Experts Say". *CNBC*, March 2, 2024. https://www.cnbc.com/2024/03/03/cyber-physical-attacks-fueled-by-ai-are-a-growing-threat-experts-say.html

Woetzel, Lola et al. "Smart Cities: Digital Solutions for a More Livable Future." *McKinsey Global Institute*, June 5, 2018. https://www.mckinsey.com/capabilities/operations/our-insights/smart-cities-digital-solutions-for-a-more-livable-future

Yadav G. and Kolin Paul, "Architecture and security of SCADA systems: A review", International *Journal of Critical Infrastructure Protection* 34 (September 2021), https://doi.org/10.1016/j.ijcip.2021.100433

Young Mary Alice and Deborah Adkins, "Editorial: The ascent of green crime: exploring the nexus between the net zero transition and organized crime", *Journal of Financial Crime* 29, no. 3 (2022), http://dx.doi.org/10.1108/JFC-07-2022-277

Executive Summary

The energy infrastructure of the contemporary energy transition has become a primary target for cyberattacks. Digitalization in the energy sector has brought forward the integration of digital technologies - from advanced analytics, Internet of Things (IoT) devices, artificial intelligence, and notably smart grid technologies. The transformative process is not only transforming how the energy sector is generated, distributed, and consumed, but it is equally facilitating the seamless integration of renewable. With decentralization, the reorganization of a single concentrated, energy-generation facility into smaller and more autonomous energy generation units - distributed generations - through rooftop solar panels, electric vehicles, and battery storage showcases significant opportunity for sustainable energy growth.

The creation of these digitalized energy assets however, created key challenges still need to be addressed. This dissertation focuses on the challenge of cybersecurity threats to this new critical energy infrastructure.

Cyber-threats are unique threats that must be distinguished from traditional national security threats. As critical energy infrastructure is deemed, by virtually every jurisdiction, as an object of national security, with risks heightened due to critical infrastructure cross-sectoral and cross-broder interdependencies a study of the main threats, actors, and motivation is essential for developing adequate and efficient cyber strategies and policies. As shown from different case studies, cyberthreats can be perpetrated by different actors - from nation-states, terrorist groups and individuals, hackers, and can also be delivered from insider threats. Different attackers can have diverse motivations, as different methods of attacks can have different targets.

Types of attacks include malware, social engineering, blockchain-related attacks, manipulation of artificial intelligence and machine learning, and finally, main-in-the-middle and denial of service attacks targeting communication infrastructure.

To mitigate these attacks, security policies worldwide are transforming, in an era in which information is as valuable as physical assets. The primary purpose of a security policy is to

establish a set of guidelines and procedures that help protect an organization, state, information systems and assets from threats, whether they originate from internal or external sources.

Cybersecurity policies include international collaboration, intelligence, and knowledge sharing, cyberdiplomacy, national security strategy, investments, and public-private partnerships. Yet all of them do not operate in isolation but are deeply interdependent.
Ultimately, investments and public-private partnerships will determine the success of efforts to counter cyberattacks, but these will require fundamental national and international regulations, standards, and guidelines to efficiently operate.