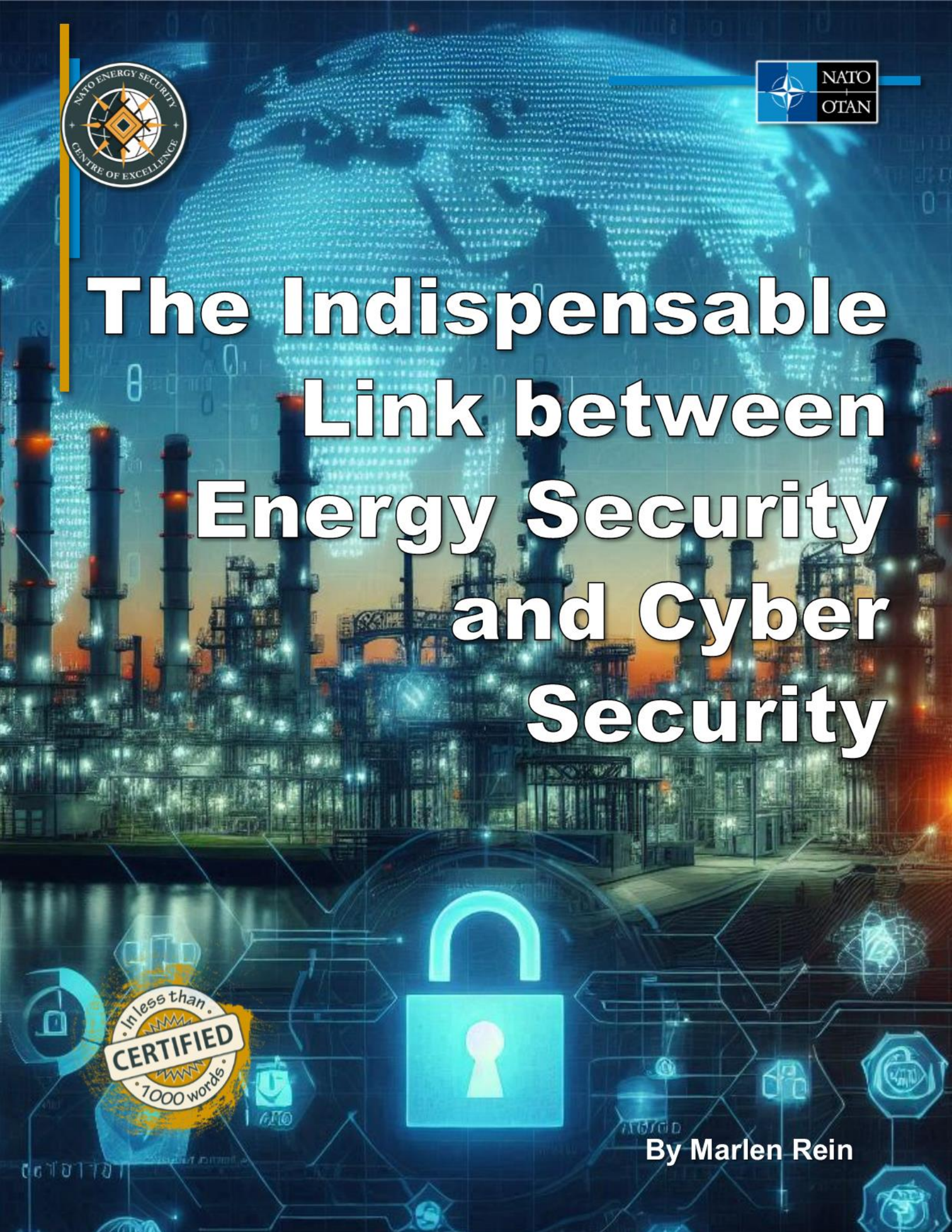
NATO ENERGY SECURITY CENTRE OF EXCELLENCE
NATO OTAN
The Indispensable Link between Energy Security and Cyber Security
In less than CERTIFIED 1000 words
By Marlen Rein

The Indispensable Link between Energy Security and Cyber Security

By Marlen Rein

Ransomware, cyber espionage, phishing, and DDoS attacks are just a few examples of a broad spectrum of possibilities that could harm entire energy systems and cause significant societal disruptions. As many countries are on their path towards the green and digital transition (often referred to as the twin transition), also the energy sector is undergoing rapid and wide-scale digitalization. This, alongside increasing geopolitical tensions, means the interlinkage between energy security and cyber security is getting constantly stronger. This paper highlights some of the key areas of energy security that are impacted by cyber risks to demonstrate the need for a holistic view for ensuring energy security in NATO nations.

There are multiple concepts of energy security, but in this paper, the definition and criteria of energy security used by the NATO Energy Security Centre of Excellence (ENSEC COE) is adopted, which refers to energy security as "a stable and reliable supply of required energy forms and quantities, enabling NATO's capabilities, operational effectiveness, and resilience." The article is structured around the key terms of this definition, i.e., stable and reliable supply, NATO's capabilities, operational effectiveness, and resilience, by highlighting some of the main cyber threats related to these aspects in the broader civil-military framework.

There is a vast array of alarming information about the vulnerability of the energy sector to cyber threats; for instance, the IEA, NATO, and the European Commission have warned about the increase of cyber-attacks in the energy sector, Financial Times has referred to the rising number of cyber-attacks on industrial targets, to name just a few. Moreover, many national authorities have also underlined the increasing security risk. Table 1 shows the growing cyber-attack trend in recent years in different industries, including gas and electricity infrastructure. The risks posed to the critical energy infrastructure are especially worrisome, as they could cause significant disruptions and diminish the stable and reliable supply of energy sources, aside from the possible negative economic and reputational impact. Ukraine's energy sector has been one of the most prominent recent targets of several cyber-attacks. Still, there are many other examples and incidents around the globe, including many NATO members.

The energy sector, just like any other key sector, could be vulnerable to different types of risks, such as ransomware, DDoS attacks, data-related threats, malware, social engineering, or supply chain attacks. The cyber threats could negatively impact the stable and reliable supply of energy sources for a shorter or longer period, depending on the attack's difficulty level and the sector's preparedness. The targets in the energy sector could be very diverse. The ransomware attack on the US' largest refined products pipeline, Colonial Pipeline, is one of the most famous recent examples and has had a significant disruptive effect. Some other cases highlighted in the list of cyber incidents compiled by the CSIS are, for instance, the cyber-attack on Italy's energy agency GSE, by compromising servers and blocking access to systems; the DDoS attack on Lithuania's energy group Ignitis; cyber espionage campaigns against different private companies,

including energy businesses; ransomware attacks against multiple European oil terminals and Norwegian energy technology company Volue. Additionally, the renewable energy infrastructure, especially solar and offshore wind farms, smart grids, and energy storage systems, as indispensable parts of the clean energy transition, are increasingly popular targets for cyber-attacks. For example, in 2022, several wind farms in Germany suffered from different types of cyber-attacks, and the Dutch Government Inspectorate for Digital Infrastructure warned about the vulnerability to the hacking of solar panel converters.

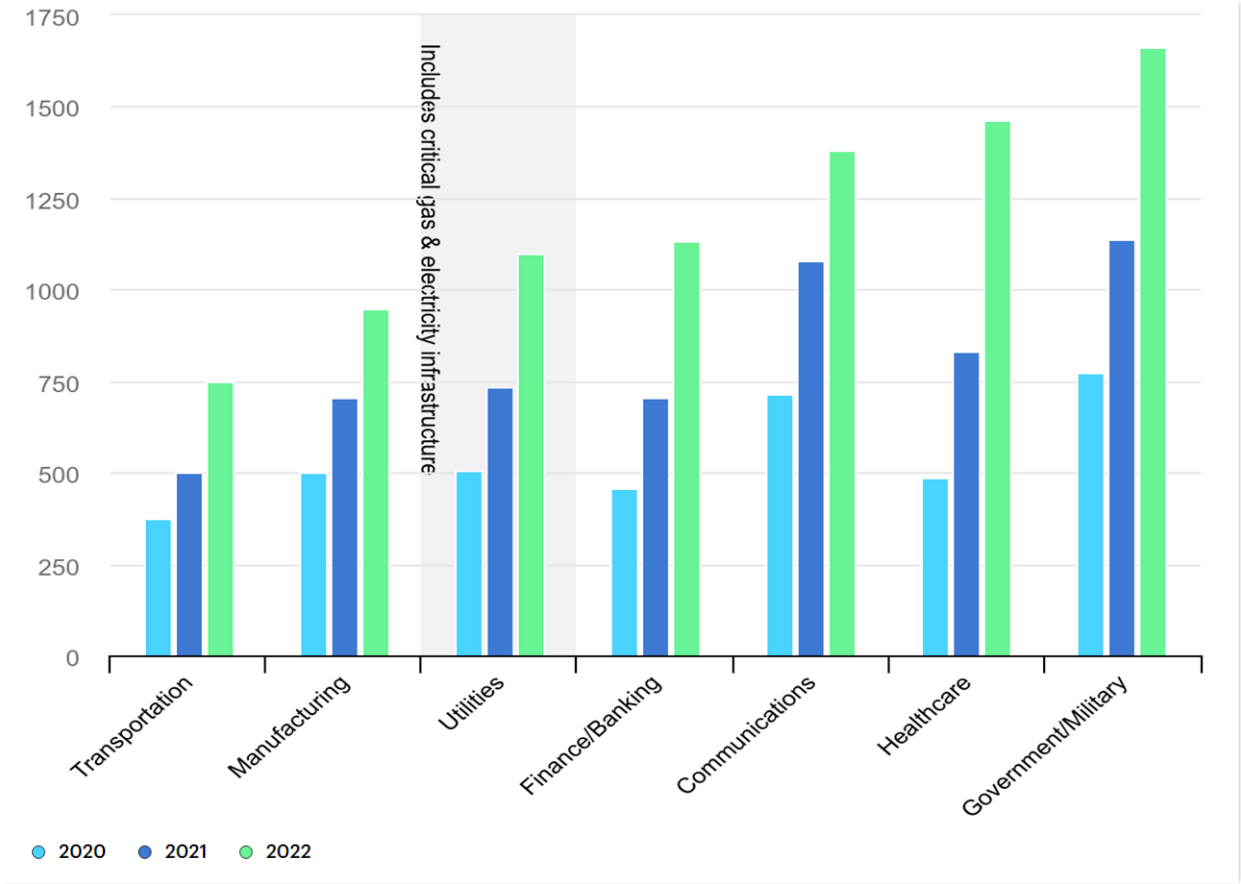

Table 1: Average number of weekly cyberattacks per organisation in selected industries, 2020-2022, (IEA, 2023). Licence: CC BY 4.0.

As the previously mentioned examples indicate, cyber-attacks are very diverse and could pose a risk to different components of our energy systems. As military forces depend largely on civilian energy infrastructure, disruption to the integral elements of the energy system also considerably impacts NATO's capabilities, operational effectiveness, and resilience. Therefore, energy sector preparedness and cyber resilience through the whole supply chain - from the generation and transmission to the distribution, storage, and consumption - need to be considered to build up and ensure resilience. A considerable amount of work has already been done at different levels, including regulatory, educational, and awareness-raising activities. Still, the growing risks and more intensive attacks require every one of us to be alert and ready constantly. For instance, the Office

of Cybersecurity, Energy Security, and Emergency Response (CESER) of the US Department of Energy uses the concept of cyber-informed engineering to integrate cybersecurity into the conception, design, development, and operation of any system. Also, the IEA emphasizes collective responsibility as key for cyber resilience in the electricity sector.

Another relevant phenomenon related to NATO's resilience in this regard is the increasing usage of predominantly Chinese technology in renewables, such as solar and wind parks. For instance, the Estonian Foreign Intelligence Service has highlighted in its annual report "International Security and Estonia 2024" the widespread use of Chinese technology in critical infrastructure, especially the electrical grid, solar and wind firms, as a threat to Estonia's security. It thereby refers primarily to the risk of manipulation of the inverters used in solar and wind farms and energy storage systems. Other NATO nations have occasionally raised similar warnings, pointing to a broader problem.

The green and digital transition are key enablers for a more sustainable world and are relevant for the energy security. At the same time, the associated cyber risks need to be taken into account throughout the energy systems. This includes integrating cybersecurity into the early system design, but also backing it up with the awareness of the end-users, in order to provide a stable and reliable supply of required energy forms and quantities as enablers for NATO's capabilities, operational effectiveness, and resilience. Energy security and cyber security are, therefore, increasingly interlinked. Integrating a holistic view is an essential daily duty of every NATO member, but is particularly critical during crisis situations, as has been evident in Ukraine throughout Russia's war of aggression. The NATO ENSEC COE has a crucial role to play in this regard by raising awareness, ensuring an accurate overview of essential emerging trends and threats, and offering solutions and knowledge to enhance the energy efficiency of NATO military forces and the resilient functioning of the energy systems of NATO, its members, and partners.