Dependency on Chinese Clean Energy Technology:

Risks and Challenges for Energy and Cyber Security

By Marlen Rein

Dependency on Chinese Clean Energy Technology: Risks and Challenges for Energy and Cyber Security

By Marlen Rein

Abstract

Renewable energy is breaking its records globally, and the share of electricity produced from clean power sources is predicted to increase even more in the coming years. On the one hand, many governments face strong pressure from society to decarbonize and tackle the climate crisis. Furthermore, investments in renewables have surged as a reaction to the growing energy security concerns. At the same time, the remarkable Chinese dominance in the solar and wind power market has increased Western dependency on its clean energy technology. Smart technology used in solar photovoltaic and wind power systems offers numerous opportunities for conveniently measuring and monitoring our energy consumption in a user-friendly way. The cyber security risks are often underestimated or even neglected, albeit the number of cyber-attacks is on the rise. Moreover, unpredictable geopolitical challenges, competition, and contradictory political interests bring additional uncertainty. The risk perception about solar and wind power systems' vulnerabilities and the countermeasures applied to protect them is relatively variable among the NATO nations and partners. Often, the opposing challenges and dilemmas also hinder decision-making. At the same time, concerns about cybersecurity and overreliance on Chinese technology are growing in many countries, emphasizing the need for implementing well-coordinated and risk-minimizing measures.

Introduction

Renewable energy is one of the key drivers for reaching climate targets and securing sustainable and efficient energy use. The share of renewable energy in global energy consumption has increased remarkably during the last decades, and according to the IEA forecast, renewable energy consumption in the power, heat, and transport sectors will increase by about 60% over the years 2024-2030 [1]. Renewable energy sources are also pivotal players in the NATO energy transition; for example, the NATO Strategic Concept adopted at the NATO Summit in Madrid in 2022 highlights the need to invest in the transition to clean energy sources and leverage green technologies [2]. Renewable energy is progressively tested and used in the military context, including in various NATO exercises. Furthermore, as the military depends largely on civilian energy infrastructure, the increased use of renewables in countries' energy mix also influences the military sector.

At the same time, there are growing concerns about the vulnerabilities of some renewable energy systems, especially about the cyber security risks related to solar and wind power. On the one hand, China's dominance in the solar and wind supply chain, including several crucial smart technology components is on the rise. At the same time, the NATO Allies have stated in their latest Strategic Concept [2] that the People's Republic of China's malicious hybrid and cyber operations harm Alliance security. Consequently, these interlinked risk factors require thorough consideration by the Allies, especially in their critical energy infrastructure protection measures.

This paper focuses on the two commonly used and increasingly important clean energy sources, i.e., solar and wind. Relying on desk-based research, it describes the principal vulnerabilities of these two energy sources, concentrating mainly on solar inverters and wind turbines, but not excluding other interrelated components. The paper also gives a brief overview of different types of warnings issued by the governments, industry, or other key stakeholders from NATO nations or partners, as well as some risk mitigation measures taken by the nations and organizations. The paper ends with a brief analysis of the main challenges and dilemmas faced by the NATO nations, partners and China related to this topic.

Solar power

The rapid growth of solar power in recent years allows us to speak about the boom of the renewable energy installations. In 2023, solar energy was the largest source of renewable capacity at 36.7% (1418 GW) [3]. According to the IEA forecast [1], by 2030, renewable energy sources will be used for 46% of global electricity generation, whereby wind and solar photovoltaics (PV) will make up 30% of this. Significantly, the share of solar PV will increase remarkably, i.e. it is forecasted to triple. There is one country that particularly stands out in statistics and predictions: China. The IEA foresees that China's predominant role will continue in the coming years, i.e., by 2030, China will maintain over 80% of global manufacturing capacity for all PV manufacturing segments.

There are numerous benefits regarding the use of solar power. The surging appetite to install a small solar PV system on the roof of residential buildings or using this in larger, industrial or utility-scale is a good example of its popularity. Even the military sector is increasingly interested in the use of solar power in different installations. Solar power is thereby often seen as an appropriate and increasingly available method to improve energy efficiency and bolster energy security. However, solar PV systems include several components that could pose cyber security risks, when proper protection mechanisms are not implemented. In this case, they could potentially have a negative impact on energy security.

The inverter is a key component of the solar PV system that is often considered as one of the most vulnerable parts for cyber-attacks. There are several types of inverters, but generally, it is possible to talk about two main categories - a string inverter and a micro inverter. Their main function is similar, i.e. to convert direct current (DC) electricity to alternating current (AC) electricity, but the difference lies in their structure. The string inverters connect several panels as a wired system, but micro inverters are placed separately on every individual panel. The string inverters are the most classical ones and also more affordable than the micro inverters. Nevertheless, they do not offer the possibility to monitor the panels individually and as they operate as a single unit, the efficiency of every individual panel has the impact on the overall production. Sometimes, also the central inverters that are usually used in large installations are considered as a separate type of inverter. It is also possible to distinguish inverters based on grid connection methods, such as grid-tied, off-grid or hybrid inverters.

Modern inverters are constantly getting more sophisticated by providing the users many useful benefits for ensuring efficient energy use and a good real-time overview with its monitoring capabilities. Often the term “smart inverter” is thereby used to refer to the inverters that next to their primary role of converting DC into AC, also provide the users with many smart technology features to optimize the performance. Some common functions of smart inverters include the following: remote control and monitoring (e.g. supporting Wi-Fi, 4G, 5G or

Bluetooth connection), built-in sensors, real-time data collection, tracking with smartphone applications and web-based platforms, performance analysis, bidirectional power flow and communication, voltage and frequency regulation etc. The abovementioned features are just a few examples gathered by different solar PV manufacturer's webpages.

In short, there are many important and user-friendly built-in functions that improve the energy management and provide the users with a detailed overview of the performance of the solar PV equipment. At the same time, the "smarter" the inverters and thereby the energy system as a whole turn to, the more data they process and the more disposed they are for different type of cyber threats. Inverters are therefore sometimes even considered to pose a risk for the national security [4] as they transmit and receive sensitive data on national electricity consumption. Taking into account that globally a great proportion of solar inverters are imported from China, i.e. from a country that is often perceived by NATO nations as a rival, competitor, challenge or even a threat, there is potentially a great risk of exposing sensitive data to unauthorized actors. For instance, according to the estimation of Solar Power Europe [5], the share of imported inverters from China to the European market is around 80%.

One comprehensive study conducted in Netherlands about the cybersecurity risks for the solar power sector [6] offers an extensive overview of the different types of threat factors, consequences and possible countermeasures. One of the main conclusions of the study is that although the probability of successful attacks is unclear, the potential impact might be disastrous, including economic and physical damage, but also societal and reputational issues. Moreover, depending on the type and scale of an attack, the negative cascade effect may be felt in other sectors, but also in other countries. The same study also provides a thorough overview of several components that can be vulnerable to cyber threats. Next to the inverters and hardware components inside the inverters, there might be risks, for example, also in: manufacturer cloud portals, mobile applications that interact with PV installation, Home Energy Management Systems, monitoring and metering devices. Also the attackers and their aims are very diverse ranging from individuals to state actors.

Additionally, the National Association of State Energy Officials (NASEO) of the USA has also provided a useful tool for evaluating possible risks regarding the solar energy cybersecurity [7]. It stipulates that the most severe impact would derive from the attacks on the programmable reclosers, transformers, data acquisition systems, smart meters and smart inverters. Other components are listed as having rather marginal or negligible impact on the system.

Researchers at the cybersecurity company Bitdefender [8] exposed a series of vulnerabilities in two Chinese PV plant management platforms of Solarman and Deye. These included the possibility to gain control over the accounts, modify inverter parameters or change the interaction between inverter and grid and data leakage (e.g. private details of customers, Wi-Fi credentials, and software versions). This could pose serious vulnerability risks to individuals or businesses and might lead to targeted phishing attacks. Moreover, the access to devices interacting with the grid might have a severe impact on the grid itself. The researchers have listed the following threats: unauthorized control leading to power generation disruption and voltage fluctuations, modified settings of solar inverters, impacting grid stability and also potentially leading to the blackouts.

Another crucial risk factor is related to the deliberately built-in vulnerabilities in solar PV hardware, i.e. the "hardware backdoors", referring to the attacks, malicious code or modified

hardware components that are introduced into the target system during the manufacturing process or supply chain and can enable remote access, data theft or surveillance [9]. There seems to be no clear-cut consensus about the probability of having deliberately built-in vulnerabilities in the solar PV systems manufactured by China or some other non-NATO country, but the quite recent case of Huawei technology ban in 5G networks is one practical example of the complexity of the problem and the coordinated response process.

The consequences of cyber-attacks on solar PV installations is variable depending on the sector, scale and situation of the systems. In critical and sensitive sectors, such as military, health care, communications, financial services or government institutions, the negative effect of cyber-attacks is likely more severe than in individual households or companies. However, one might not neglect the impact of societal disruption, chaos, or fear that could cause devastating results at every level, especially in the case of multiple simultaneous attacks or when combined with disinformation or other hybrid attack elements.

One possible scenario with a cascade effect is well described in the study conducted by T. Krause et al. [10]. They explain how an attacker may gain control remotely over a large number of consumer solar power cells and thereby influence the frequency within the grid. This risk factor would require countermeasures applicable to all operators and users in interconnected power grids. Moreover, improvements are necessary in different fields, such as strengthening collaboration between the electrical engineering and cybersecurity community, improving software security, but also raising awareness. In short, they call for necessary changes in four levels: a) device and application security, b) network security, c) physical security, d) policies, procedures and awareness.

Until now, a coordinated simultaneous attack of multiple systems is rather a hypothetical and theoretical situation and there are different views about the real probability of witnessing these types of attacks. However, having a detailed real-time information about several individual solar PV systems in one specific area, for example, due to pre-installed hardware backdoors, would be an enabling factor for coordinated attacks organised by malicious actors. Moreover, as several studies have shown, the solar PV is vulnerable to a wide variety of cyber threats and as the Allies are currently importing most of the solar PV system components from a non-NATO country, including the crucial smart inverters, the risk of foreign interference and data leakages could not be underrated. Also due to the complicated and volatile geopolitical situation, the preparedness and awareness are definitely relevant countermeasures for building resilient societies.

Wind power

Wind power is another key renewable energy source that is increasingly used globally. For example, in 2023, it was the third largest source of renewable capacity (after solar and hydropower) at 26.3% (1017 GW) [3]. It is expected that by 2030 the share of wind power in meeting global demand will double - surpassing hydropower - even despite several supply chain and macroeconomic challenges [1]. China's role is also noticeable here. In 2023, China's share in the global offshore wind supply chain reached around 60-75% and about 90% of global onshore wind manufacturing capacity expansion [1]. Therefore, it is not surprising that words like “climate technology leadership” or “climate technology giant” [11] are often used for describing China.

One main component of the wind power system that is usually linked to cyber security risks is the turbine. The vulnerability of wind turbines derives mainly from its interconnections and dependency on digital technologies, similarly to the solar inverters. For instance, the sensors of the turbines could be used to transmit data, the angle of the blades could be changed [12], the turbines could be controlled and shut down remotely, malicious code could alter the turbine's steering [13] and attacks on the sensors could result in physical damage or shut down, loss of communication [14] and remote monitoring [15]. The digitally networked nature of wind farm installations also increases the risk of domino effect, for example, the cyber-attack at a land-based sub-station could quickly propagate through the network as a whole [16]. The severe vulnerability is also highlighted by the fact that the topic of hybrid threats to renewable energy, including the risk factors of wind turbines, was addressed during the NATO Exercise Nordic Pine 2024 [17]. The abovementioned failures in the systems could also contribute to similar wider negative impacts as mentioned by solar power, such as disruptions, economic or reputational damage. Another indirect effect of the successful cyberattacks could also be the lowering of public trust in wind or other renewable energy sources [14].

The study conducted by the Swedish National China Centre [13] provides an exhaustive overview of different types of threats regarding the use of Chinese components in wind power systems. One of the conclusions is that the turbines made in China or containing components of Chinese manufacturing might be more vulnerable to IT sabotage by Chinese actors due to their knowledge of the system design, potential deliberate vulnerabilities or China's close relations with Russia, referring thereby to the backdoor option as described in the previous section about solar PV. Additionally, J. Weiss [15] has proposed an additional threat vector, proposing that Chinese components (in this case, the transformers) would allow to find out the best time for cyberattacks to occur due to the information gathered. Idaho National Laboratory has also highlighted the risk of intentionally introducing a bug in software or a monitoring device in hardware as a supply chain attack [18]. Also the dependency on regular maintenance or technical support for the technology could entail additional point of entry that might be exploited to introduce malicious software at a later point [19].

Similarly to solar power, there is also a risk of a multiplier effect within wind power. A single cyberattack to one wind turbine will most probably not significantly impact power generation nor cause a large-scale negative impact, but simultaneous attacks on multiple turbines, on an entire farm, or on the integration between wind farm and power grid, may result in cascading damage [14]. Some recent incidents also highlight the vulnerable parts of the wind power system. One real-life example is the partial outage of a European satellite provider in 2022 that affected around 5,800 wind turbines of Enercon GmbH with a total capacity of ca. 11 GW [20] by interrupting the remote maintenance and control of the turbines.

Several studies have indicated that offshore wind farms are more vulnerable to cyberattacks compared to the wind farms situated on land. The main reason is the remoteness and complex cyber infrastructure that present multiple access points for possible attacks [21]. Another potential risk factor is the connection between offshore wind farms and other subsea infrastructure. The information received from sensors and cameras integrated to the offshore wind farm monitoring systems could include sensitive data about the functioning and settings of the wind farm, but also about other relevant offshore infrastructure that could enhance thereby other type of attacks. For instance, C. Bueger and T. Edmunds [16] have emphasised that the expansion of offshore wind farms can facilitate other maritime crimes. There have also

been warnings about the usage of Chinese cameras in sensitive areas and also some restrictions applied, for example by Australia, the UK and the US [22]. The main concern is related to the possibility of built-in backdoors in the monitoring systems and to the Chinese legislation (especially the Data Security Law [23]) that stipulates the obligation to cooperate by relevant organizations and individuals, when the national security organ needs to obtain data. Therefore, this risk factor could not be excluded also by wind farms.

Comparison of the main risk factors of solar and wind power

There are many similarities between the risks related to the solar and wind power, but also some crucial differences. Table 1 summarises some of the most common risk factors. The aim is not to be exhaustive, but rather to outline some key vulnerabilities.

Table 1. *Overview of the main risk factors of solar and wind power.*

	Solar power	**Wind power**
Similar risk factors	Increase of cyber-attacks due to wider smart technology usage	
	Potential built-in "backdoors"	
	Many stakeholders involved	
	Dependency on non-NATO country	
	Multi-level dependencies	
	Time pressure from climate crisis	
	Cascade effect	
	Potential for hybrid attack	
Different risk factors	Different level of cybersecurity measures implemented due to wide individual, small-scale usage	Vulnerabilities of offshore wind farms
	Negative impact mainly on individual households or companies	Possible relation to other maritime security risks

First of all, the use of smart technology features is more common and popular by both power types. In general, this is clearly a positive factor, enabling to optimise energy usage patterns, enhance energy efficiency and reliability, and providing the users a comprehensive overview of the system and its failures. However, with respect to the cyber security risks, it is also one of the areas that needs attention, especially as the systems transmit sensitive data and there are monitoring features involved. Also the possibility of having pre-installed hardware backdoors could not be excluded. Due to the great number of stakeholders involved (e.g. individual users and households, industries, governments etc.), the risk mitigation is a complicated task that requires a comprehensive approach and countermeasures taken in all levels.

Another important risk factor is the potential overreliance of NATO nations and partners on one country and, especially, on a non-NATO country. As it is often said, and more frequently also in the energy security context, one should not put all the eggs into one basket, referring to the need to diversify the energy sources and providers. The dependency in the renewable sector is quite complicated and expressed in several layers. Importantly, there is a dependency on specific components (e.g. solar inverters or wind turbines). This is well reflected by the data in

Figures 1 and 2 that show the dominance of China in solar PV and offshore and onshore wind equipment manufacturing capacity globally.

Figure 1 shows the share of manufacturing capacity of some key components and materials of solar PV systems (modules, cells, wafers, polysilicon) by regions in 2021. However, as mentioned previously, according to the current trends and predictions, China's share in all manufacturing stages of solar panels will grow furthermore. Figure 2 shows, on the other hand, the manufacturing situation of the main wind power components (both onshore and offshore), such as nacelles, towers and blades in 2022. Also here China's manufacturing capacity exceeds other regions' capacity.

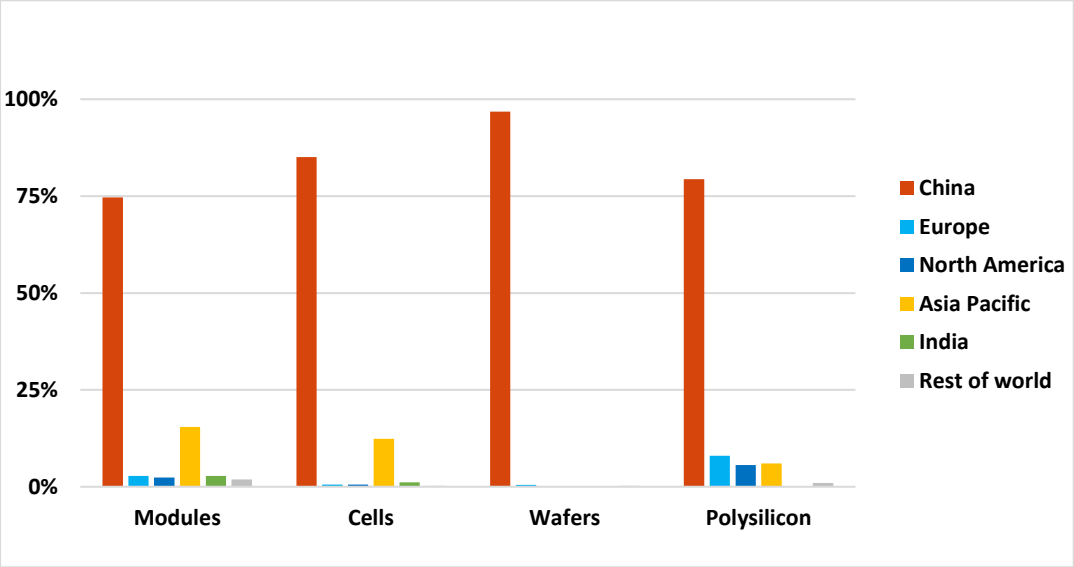

Figure 1. *Solar PV manufacturing capacity by country and region, 2021 in %.* Source: IEA [24].

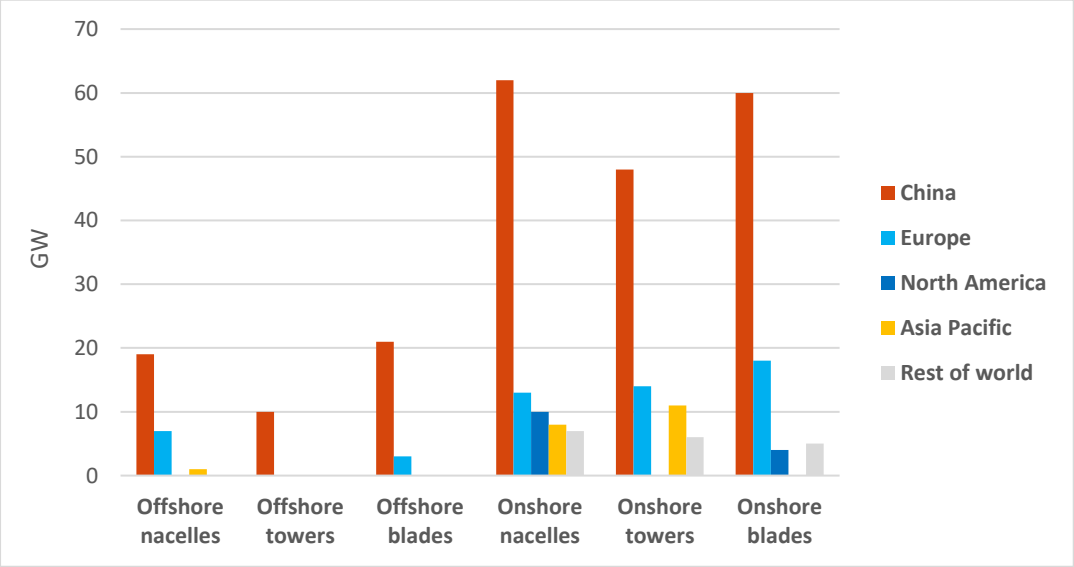

Figure 2. *Onshore and offshore wind equipment manufacturing capacity by region and component in 2022, in GW.* Source: IEA [25].

Additionally, the dependence could continue with the maintenance and technical support needed for these specific components and systems offered by the same producers, enabling additional point of entry for cybersecurity risks. Moreover, the reliance on critical materials and minerals needed for manufacturing adds another relevant layer of dependence. There are already several ongoing or planned initiatives and activities in many countries with the aim of boosting national manufacturing capacity as a counter-measure. However, as this is rather a long-term and complex endeavour including many stakeholders, it might take some time for minimizing the dependency.

The dependency issue is also related to the next important factor, i.e., the time pressure derived from the climate crisis and the climate targets taken by the countries. This means that the appetite and necessity for renewable energy expansion are enormous, motivating governments to increase renewable capacity in the quickest possible way. However, this will challenge the possibility of minimizing dependency on external providers.

Other relevant common aspects that need to be considered are the possibilities of a negative cascade effect deriving from a row of attacks on several solar PV power plants or wind farms simultaneously or during a short time span, and also the potential to use the attacks on solar or wind power system as part of a wider hybrid attack scheme. As mentioned before, currently this is rather a hypothetical scenario, but it should also be taken into account by the potential threat matrix.

There are also some pertinent differences between the risks related to solar and wind power. For example, solar power has an additional risk factor due to the large number of small-scale operators and individual users who often lack the necessary resources to safeguard their systems with strong cyber security measures. This also implies that a disruption is probably foremost felt by individual households or companies, but one could not exclude also the possibility of a cascade effect described before.

In the case of wind power, residential use is until now rather a niche sector and, therefore, does not entail that frequent individual risks as by solar power. On the other hand, wind power, especially offshore wind farms, has other vulnerabilities. As described previously, many studies indicate that especially offshore wind farms are more vulnerable to cyberattacks because of their remoteness and complex cyber infrastructure. Due to the fact that many countries are keen to expand the offshore wind power generation capacity in the coming years with a more rapid pace, the risk factor is even more crucial. Another difference related to offshore wind farms is the possibility to facilitate other types of maritime crimes through sensitive data leakages about subsea infrastructure.

Warnings and countermeasures

Several governments, think tanks, industries and other stakeholders have issued warnings or called for greater cautiousness due to the vulnerability of renewable energy to cyber threats, especially solar PV or wind power systems, and because of the vulnerabilities deriving from the dependence on any one non-NATO country, especially China. The following is not an exhaustive list of these statements, but aims to demonstrate the variety of perspectives of growing concerns among the societies. The warnings differ in their level of detail and target audience, but could generally be divided into three main types:

1) warnings about China's threat in a more general level, including cyber espionage among others, issued by the FBI [26], Director of National Intelligence of the USA [27], Canadian Centre for Cyber Security [28], Centre for Cyber Security of Denmark [29], Ministry of Foreign Affairs of the Czech Republic [30], Latvian State Security Service [31]; Ministry of National Defence and State Security Department of Lithuania [32]; National Cyber Security Centre of the United Kingdom [33]; Norwegian Police Security Service [34]; NATO Centre of Excellence – Defence Against Terrorism [35];

2) warnings about the dependence on Chinese technology in different sectors and the possible consequences derived from this, including cyber security issues, issued by the Royal United Services Institute [36], conveyed during the speech by the former NATO Secretary General Jens Stoltenberg at the NATO Cyber Defence Conference [37] or also expressed in the European Parliament resolution [38];

3) warnings about the vulnerability of solar or wind power systems due to cyber security issues and/or Chinese dominance in the sector issued by the Estonian Foreign Intelligence Service [39], Swedish National China Centre [13], Government of Australia [40], Solar Power Europe [41] and described also in a report conducted by Secura for the Netherlands Enterprise Agency and Energy Innovation Netherlands [6].

The risks deriving from the high level of dependency on one country regarding solar and wind power have also triggered governments to create several policy measures with the aim to increase domestic production. Some examples from the EU and the US include the US Inflation Reduction Act, the EU Net Zero Industry Act, Critical Raw Minerals Act, tariffs and anti-subsidy measures complemented also by stronger cyber security rules, such as the EU NIS2 Directive or EU Network Code on Cybersecurity for the electricity sector.

Some countries have, however, even gone a step further by introducing additional restrictive national policies. One recent example is Lithuania whose parliament adopted in November 2024 amendments to its Electricity Law by introducing additional security measures for solar and wind power plants and energy storage devices over 100 kW with the aim to reduce the risks and threats posed to the operation of the electricity system by the remote use of equipment produced by hostile countries [42]. The amendments stipulate that entities from countries that pose, according to the National Security Strategy, a threat to the national security of Lithuania, should not have access to these systems. The National Security Strategy includes explicitly references to Russia, Belarus and China [43]. European Solar Manufacturing Council welcomed these amendments immediately and called for other Member States to replicate them [44]. Romania, on the other hand, has developed plans to introduce a mandatory cyber audit of newly built solar power plants to protect national infrastructure against vulnerabilities and avoid the risk of transmitting data to state and non-state parties hostile to Romania [45]. Germany has also recently introduced an action plan for addressing the challenges to German and European wind energy, by aiming to minimise the cyber and data security risks [46].

These examples demonstrate the variable level of perceived risk and readiness, but as Europe has an interconnected power grid and great interdependency between the countries, a coordinated regional or international approach would definitely be more effective. Also the abovementioned study conducted in Netherlands [6] highlighted that an attack on a solar PV system in one European country would have an impact on other European countries as well, referring to the need to have a more harmonised approach, at least regionally. Taking into

account the possibilities of spill over to the wider energy and national security issues, a well-coordinated approach with NATO, the EU and other partners would be a more effective solution.

Dilemmas and challenges

Previous sections demonstrated the situation's complexity and the significant number of stakeholders, interests, and challenges involved in the current solar and wind power landscape. It also illustrated many concerned voices amongst national policymakers. At the same time, the threat is not perceived equally among all NATO nations and partners and often there are difficult dilemmas between finding the balance between trade and economic benefits, the speed of reaching climate targets and the security aspects. The situation is comparable to the so called Huawei dilemma that demonstrated different views and concerns regarding the ban of Huawei technology in 5G networks.

The Figure 3 below illustrates the matrix of main dilemmas and challenges that both sides – NATO nations and partners on the one side, and China, on the other side, currently are facing in the realm of renewable energy technology. Once again, this is not an exhaustive list of factors, but rather a schematic overview of some key aspects that were described in the previous sections.

First of all, one of the main questions for many NATO nations and partners is finding the balance between energy transition needs and ensuring the necessary level of security, encompassing cyber and energy security as well as national security as a whole. This inherent dilemma is constantly impacted by several external factors. For instance, the climate targets that many nations have taken are usually binding and stipulated in written regulations. Moreover, the demand from society to decarbonise is increasingly strong due to the devastating effects derived from the climate crisis. This means that many governments are encountered with the need to meet climate targets in a limited timeframe and using thereby also renewable energy sources as one of the key drivers. The initiatives to enhance and boost national green technology industries are definitely welcomed, but are also relatively time consuming in a wider scale.

At the same time, the increasing trend of cyber-attacks has induced the governments to think about additional measures to avoid possible future attacks, especially on critical energy infrastructure. Possible stricter regulations, bans or other similar measures to curb technology from third countries or minimise the dependence on some specific country, would, however, probably slow down the pace of energy transition.

On the other side, the figure outlines some key challenges of China. For instance, China needs to manoeuvre between the economic benefits deriving from the exports of renewable energy systems, components, and critical materials and the political interests. Some factors that are impacting the challenges are the market situation and the role of third countries. The first refers to the many economic gains that China would not like to lose, especially if taking into account the statistics indicating China's dominant role in renewable energy manufacturing capacity. Chinese actions reflect its need to maintain or increase its so-called climate technology leadership role. However, there might also be possible political gains or wider impact deriving from the actions of third countries that would encourage China to use its cyber capabilities as a possible measure to meet its political interests, thereby putting its economic gains at risk.

Additionally, both sides are influenced by the two dominant factors, i.e. the geopolitical situation and global competition. These factors are crucial in decision making and could change the balance quite suddenly, especially due to the current international volatile and complex situation. For instance, the dynamics of China's cooperation with Russia might be one compelling element, or, conversely, the impact of possible restrictive measures, such as tariffs and bans. However, both sides also need to maintain cooperation and engagement with each other, especially in certain global issues where international cooperation is imperative, but also due to the interdependency and interconnectedness, especially in trade. Therefore, the matrix of dilemmas and challenges is quite complex and unpredictable and depends on various internal and external factors.

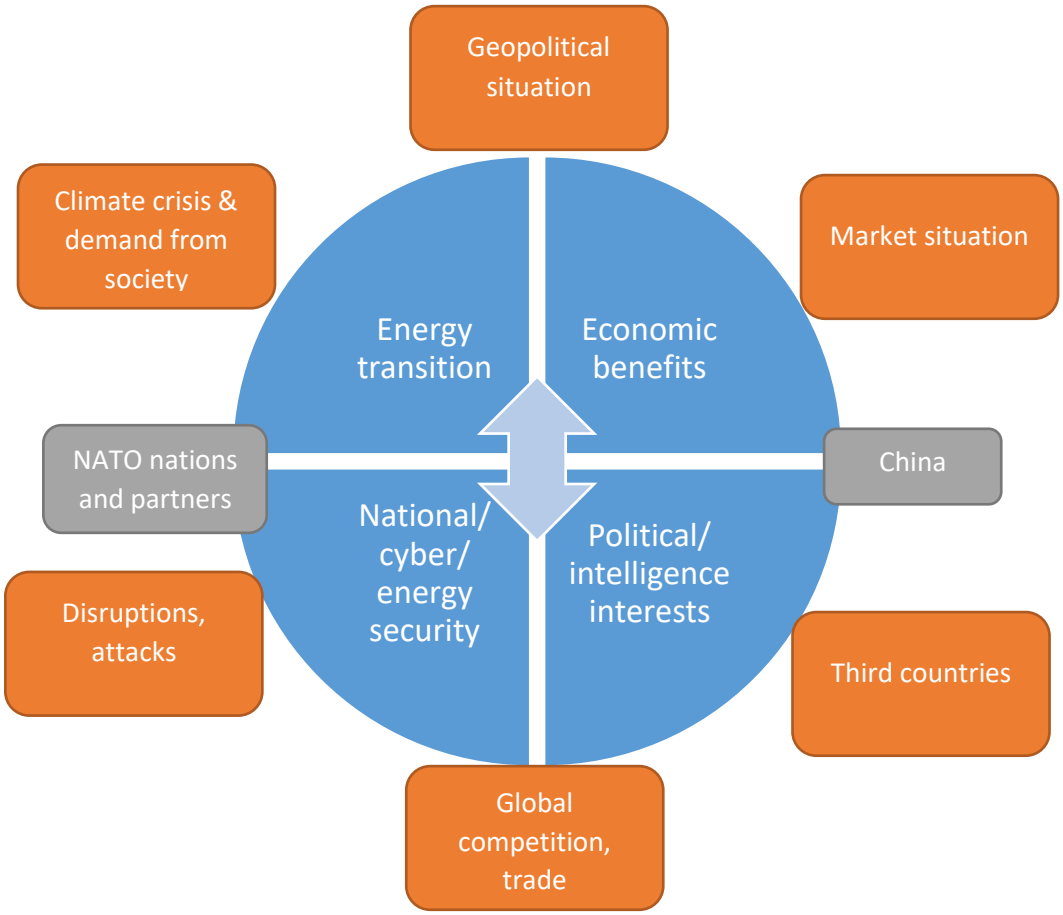

Figure 3. *Matrix of main dilemmas and challenges related to renewable energy technology.*

Summary

The role and importance of renewable energy cannot be underestimated. The world needs clean energy sources in order to tackle the pressing climate crisis. This has led to an increased usage of solar and wind power in different sectors, including in the military. It is expected that these two types of renewable energy sources will become even more relevant in the coming decades. Also the increasing number of user-friendly and efficient smart technology features of solar and wind power make them an increasingly popular choice.

At the same time, there are some worrying tendencies regarding the use of solar and wind power, especially with respect to the cyber security risks and the overreliance on one non-NATO country, China. Solar and wind power have many important differences that have been described in the paper, but at the same time, also several similarities that facilitate joint analysis of these two types of energy sources and the drawing of similar conclusions. For instance, although the vulnerable parts are different, they are still related to the modern smart systems and features that could be used by malicious actors and be prone to severe cyber-attacks.

The issue is complicated, including different layers of dependence and risk factors. One of the concerns is related to the growing cyber security risks due to the wider usage of smart technology. This could entail small-scale risks related to the sensitive data leakage and power outages at the household level. However, theoretically, there are also possibilities for more severe cascade effects encompassing several solar PV systems or wind farms simultaneously, and also the possibility for using this as part of a wider hybrid attack. These abovementioned failures in the systems could thereby also lead to large-scale economic or reputational damage. Another indirect effect of successful cyberattacks could also be the lowering of public trust in renewable energy sources.

Chinese dominance in the solar and wind power market is increasingly visible and many governments, industries or think tanks have already pointed to this phenomena as a growing problem. There have been several warnings issued about China's threat in general, including cyber espionage, about dependence on Chinese technology and its consequences and also more concretely about the vulnerability of solar and wind power systems due to cyber security.

The risks deriving from the high level of dependency on China regarding solar and wind power, have also triggered some policy measures with the aim to increase domestic production. There are also a few examples regarding the restrictions of the origin of renewable energy technology components. Although tackling the dependency issue effectively is a complicated task due multi-level dependencies and many interrelated challenges, a coordinated response would be more effective. NATO nations and partners could therefore consider discussing the possibility of having a more common approach and measures to raise awareness on this matter and bolster the energy security.

In recent years, there has been a significant increase in cyber-attacks against energy systems. Until now, their impact has been rather low and many risks mentioned in this paper reflect hypothetical possibilities. However, preparedness and well-coordinated risk minimizing activities should be the key considerations, especially when taking into account the current complicated geopolitical situation and volatile environment.

Referenes

[1] International Energy Agency (IEA). "Renewables 2024." IEA, October 2024. https://www.iea.org/reports/renewables-2024/global-overview (accessed: November 13, 2024).

[2] NATO. "NATO 2022 Strategic Concept." NATO. https://www.nato.int/strategic-concept/ (accessed November 11, 2024).

[3] International Renewable Energy Agency (IRENA). "Renewable energy highlights." IRENA, July 11, 2024.

[4] Lipke, A., Oertel, J., O´Sullivan, D. "Trust and Trade-Offs: How to Manage Europe´s Green Technology Dependence on China." European Council on Foreign Relations, May 29, 2024.

[5] Solar Power Europe. "Inverters Explained: The brain of a solar system." June 5, 2023. https://www.solarpowereurope.org/advocacy/position-papers/inverters-explained (accessed: November 22, 2024).

[6] Secura B.V. "Report: Cybersecurity threats and measures for the solar power sector." Secura B.V, 2024.

[7] National Association of State Energy Officials (NASEO). "Decision Support Tool for Solar Energy Cybersecurity Policy and Regulation: A Cybersecurity Advisory Team for State Solar (CATSS) Tool." https://www.naseo.org/issues/cybersecurity/catss (accessed: November 25, 2024).

[8] Melniciuc, I.A., Lazăr, A., Cabău, G., Basaraba, R.A. "60 Hurts per Second – How We Got Access to Enough Solar Power to Run the United States." Bitdefender, August 7, 2024. https://www.bitdefender.com/en-us/blog/labs/60-hurts-per-second-how-we-got-access-to-enough-solar-power-to-run-the-united-states (accessed: December 3, 2024).

[9] TATA Communications. "Backdoor Attack – Guidelines for Identification and Aversion." https://www.tatacommunications.com/knowledge-base/backdoor-attack/ (accessed: December 3, 2024).

[10] Krause, T., Ernst, R., Klaer, B., Hacker, I., Henze, M. (2021). "Cybersecurity in Power Grids: Challenges and Opportunities." Sensors, 2021, 21(18).

[11] Mazzocco, I. "Balancing Act: Managing European Dependencies on China for Climate Technologies." Center for Strategic and International Studies (CSIS), December 13, 2023. https://www.csis.org/analysis/balancing-act-managing-european-dependencies-china-climate-technologies (accessed: December 12, 2024).

[12] Ainger, J. "EU Wind Industry Warns Germany over Large Chinese Turbine Deal." BNN Bloomberg, July 23, 2024. https://www.bnnbloomberg.ca/investing/commodities/2024/07/23/eu-wind-industry-warns-germany-over-large-chinese-turbine-deal/ (accessed: November 28, 2024).

[13] Wachtmeister, H. "Chinese presence in the Swedish wind energy sector: Vulnerabilities and risks." Swedish National China Centre, 2024.

[14] Knack, A., Kam Hwei Syn, Y., Tam, Kimberly. "Enhancing the Cyber Resilience of Offshore Wind." The Alan Turing Institute, Centre for Emerging Technology and Security Research Report, June 2024.

[15] Weiss, J. "The U.S. electric industry is not responding to cyber-vulnerable Chinese equipment." Security Infowatch, March 4, 2024. https://www.securityinfowatch.com/cybersecurity/article/53098118/the-us-electric-industry-is-not-responding-to-cybervulnerable-chinese-equipment (accessed: November 28, 2024).

[16] Bueger, C., Edmunds, T. "Maritime Security and the Wind: Threats and Risks to Offshore Renewable Energy Infrastructure." Ocean Yearbook 38, July 2024, 433-458.

[17] The Total Defense Foundation. “Nordic Pine.” https://totalforsvar.org/nordicpine24/ (accessed: November 28. 2024).

[18] Freeman, S.G., Kress-Weitehnagen, M.A., Gentle, J.P., Culler, M.J., Egan, M.M., Stolworthy, R.V. “Attack Surface of Wind Energy Technologies in the United States.” Idaho National Laboratory (INL), January 2024.

[19] Sambell, K., Lamboo, S., van der Burg, L., Warnaar, P. “The current and future role of China in the wind energy and electrolyser supply chains.” TNO, May 1, 2024.

[20] Vassileva, A. “Satellite outage affects remote control of 5,800 Enercon turbines – report.” Renewables Now, March 1, 2022. https://renewablesnow.com/news/satellite-outage-affects-remote-control-of-5-800-enercon-turbines-report-775234/ (accessed: December 4, 2024).

[21] Concordia University. "Offshore wind farms are vulnerable to cyberattacks." Science Daily, January 24, 2024.

[22] Gaál, F. “China's surveillance tech: Western bans, global growth.” Deutsche Welle, March 29, 2023. https://www.dw.com/en/western-countries-are-banning-chinese-tech-why-is-it-still-spreading/a-65106709 (accessed: December 12, 2024).

[23] The National People's Congress of the People's Republic of China. “Data Security Law of the People's Republic of China.” 29th Meeting of the Standing Committee of the 13th National People's Congress, June 10, 2021. http://www.npc.gov.cn/englishnpc/c2759/c23934/202112/t20211209_385109.html (accessed: December 12, 2024).

[24] International Energy Agency (IEA). “Solar PV manufacturing capacity by country and region.” IEA, 2021. https://www.iea.org/data-and-statistics/charts/solar-pv-manufacturing-capacity-by-country-and-region-2021 (accessed: January 23, 2025).

[25] International Energy Agency (IEA). “Offshore wind equipment manufacturing capacity by region and component, 2022-2025.” IEA, 2023. https://www.iea.org/data-and-statistics/charts/offshore-wind-equipment-manufacturing-capacity-by-region-and-component-2022-2025 (accessed: January 23, 2025).

[26] Federal Bureau of Investigation of the United States of America (FBI). “The China Threat.” https://www.fbi.gov/investigate/counterintelligence/the-china-threat (accessed: November 20, 2024).

[27] Office of the Director of National Intelligence (DNI). “Annual Threat Assessment of the U.S. Intelligence Community 2024.” February 5, 2024.

[28] Canadian Centre for Cyber Security. “National Cyber Threat Assessment 2025-2026.” Ottawa: Communications Security Establishment Canada, 2024.

[29] Centre for Cyber Security of Denmark. “Threat assessment: The cyber threat against the Danish energy sector.” Copenhagen: Centre for Cyber Security of Denmark, 2023.

[30] Ministry of Foreign Affairs of the Czech Republic. “Security Strategy of the Czech Republic 2023.” Prague: 2023.

[31] Latvian State Security Service. “Annual Report on the Activities of Latvian State Security Service (VDD) in 2023.” Riga: April 2024.

[32] Ministry of National Defence, State Security Department of the Republic of Lithuania. “National Threat Assessment of 2024”. Vilnius: 2024.

[33] National Cyber Security Centre of the United Kingdom. “Annual Review of 2024.” December 3, 2024.

[34] Norwegian Police Security Service (PST). "National threat assessment 2024." 2024.

[35] Evans, C. V., Anderson, C., Baker, M., Bearse, R., Biçakci,S., Bieber, S., Cho, S., Dwyer, A., French, G., Harell, D., Lazari, A., Mey, R., Sabonis-Helf, T., Verner, D. "Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency." NATO COE-DAT Handbook 1. Carlisle, PA: US Army War College Press, 2022.

[36] Ashbridge, S., Dawda, S. "UK Defence and Solar Panel Supply Risks." Royal United Services Institute, November 2, 2022. https://www.rusi.org/explore-our-research/publications/commentary/uk-defence-and-solar-panel-supply-risks (accessed: November 20, 2024).

[37] Stoltenberg, J. "Speech by NATO Secretary General Jens Stoltenberg at the first annual NATO Cyber Defence Conference." (November 9, 2023). NATO. https://www.nato.int/cps/en/natohq/opinions_219806.htm (accessed: November 21, 2024).

[38] The European Parliament. "European Parliament resolution of 17 January 2024 on the security and defence implications of China's influence on critical infrastructure in the European Union." https://www.europarl.europa.eu/doceo/document/TA-9-2024-0028_EN.html (accessed: November 21, 2024).

[39] Estonian Foreign Intelligence Service. "International Security and Estonia 2024." https://raport.valisluureamet.ee/2024/en/ (accessed: November 20, 2024).

[40] Croft, D. (2023). "Australia plans defences against Chinese cyber attacks on the solar grid." Cyber Daily, October 25, 2023. https://www.cyberdaily.au/government/9734-australia-plans-defences-against-chinese-cyber-attacks-on-the-solar-grid (accessed: November 21, 2024).

[41] SolarPower Europe. "A Harmonised Cybersecurity Baseline for Solar PV." Brussels: SolarPower Europe, 2024.

[42] Seimas of the Republic of Lithuania. "Elektros energetikos įstatymo Nr. VIII-1881 16, 22 ir 48-2 straipsnių pakeitimo ir Įstatymo papildymo 73-3 straipsniu įstatymo projektas." November 12, 2024. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/c3f458c0a1c311ef9db2c9aaf9c67042?jfwid=xdetouvd5 (accessed: November 14, 2024).

[43] Seimas of the Republic of Lithuania. "Dėl Lietuvos Respublikos Seimo 2002 m. gegužės 28 d. nutarimo Nr. IX-907 „Dėl Nacionalinio saugumo strategijos patvirtinimo" pakeitimo." December 16, 2021. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/10625df0623a11ecb2fe9975f8a9e52e?jfwid=4raytmspy (accessed: December 11, 2024).

[44] Vaičiūnas, Ž. "Lithuanian Parliament bans remote access of companies from China to Lithuanian solar, wind and storage devices." European Solar Manufacturing Council, November 13, 2024. https://esmc.solar/lithuanian-parliament-bans-remote-access-of-companies-from-china-to-lithuanian-solar-wind-and-storage-devices/ (accessed: November 21, 2024).

[45] Spasic, V. "Romania to introduce mandatory cyber audit for solar plants." Balkan Green Energy News, October 31, 2024. https://balkangreenenergynews.com/romania-to-introduce-mandatory-cyber-audit-for-solar-power-plants/ (accessed: November 22, 2024).

[46] Bundesministerium für Wirtschaft und Klimaschutz. "Maßnahmenpaket für die Windindustrie in Deutschland und Europa." https://www.bmwk.de/Redaktion/DE/Downloads/M-O/20241016-massnahmenpapier-windindustrie.html (accessed: November 28, 2024).