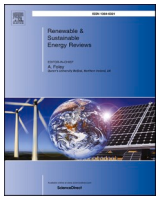
Renewable and Sustainable Energy Reviews 150 (2021) 111476

Contents lists available at ScienceDirect

Renewable and Sustainable Energy Reviews

journal homepage: www.elsevier.com/locate/rser



Energy system resilience – A review

Justinas Jasiūnas **, Peter D. Lund *, Jani Mikkola

Aalto University, School of Science, New Energy Technologies Group, P.O.Box 15100, FI-00076, Aalto, Espoo, Finland

ARTICLE INFO

Keywords:
Resilience
Energy systems
Power systems
Energy security
Extreme weather
Climate
Cybersecurity
Threat landscape

ABSTRACT

The term resilience describes the ability to survive and quickly recover from extreme and unexpected disruptions. A high energy system resilience is of utmost importance to modern societies that are highly dependent on continued access to energy services. This review covers the terminology of energy system resilience and the assessment of a broad landscape of threats mapped with the proposed framework. A more detailed discussion on two specific threats are given: extreme weather, which is the cause for most of the energy supply disruptions, and cyberattacks, which still are a minor, but rapidly increasing concern. The framework integrates various perspectives on energy system threats by showcasing interactions between the parts of the energy system and its environment. Weather-related threats are discussed distinguishing relevant meteorological parameters and different durations of disruptions, increasingly related to the impacts of the climate change. Extremes in space weather caused by solar activity are very rare, but are nonetheless considered due to their potentially catastrophic impacts on a global scale. Digitalization of energy systems, e.g. through smart grids important to renewable electricity utilization, may as such improve resilience from traditional weather and technical failure threats, but it also introduces new vulnerabilities to cyberattacks. Major differences between the internet and smart grids limit the applicability of existing cybersecurity solutions to the energy sector. Other structural energy system changes will likely bring new threats, which call for updating the threat landscape for expected system development scenarios.

1. Introduction

Modern societies rely on access to large amounts of energy meaning that reliable functioning of energy systems is of vital importance for their existence. At the same time, as the reliance on energy and energy-based services continues to grow, both energy systems and their environment are changing rapidly. Technology progress and environmental degradation along with other developments are introducing new risks that may be difficult or even impossible to identify and quantify before disruptions unfold in practice [1]. Some developments, such as climate change, may be undesirable irrespective of their effects on energy systems [2] while others such as electrification [3] and digitalization [4], may provide greater benefits to the society than the costs of the associated risks. Regardless of their origin, many emerging risks noticeably increase uncertainties and potential damages [5–9]. As a result, traditional risk management approaches may no longer be sufficient to cope with these [10]. The concept of resilience, which refers to the ability of the system to survive strong and unexpected disruptions and to recover quickly afterward, appears to be a crucial addition for developing approaches to deal with the kind of risks to which energy systems are increasingly exposed [11–13].

A large part of the literature on energy system resilience and overlapping energy security focus on threats of a specific type (e.g. weather [14–22], technical failures [19,23,24], cyberattacks [25–29], and geopolitics [29–31]), or, for a specific energy sector (e.g. electricity [16–20,25–29], oil, and gas [31–34]). Several studies have attempted to provide a more integrated view on energy security and energy resilience by discussing and defining related terminology [35,36], concepts [1,37,38], and different perspectives on the issues [39,40]. However, energy system resilience is strongly linked to the types of threats and energy systems in question, which limits a generalization of the concept and may thus require better specification or categorization of cases considered. On the other hand, attempts to provide a comprehensive overview of energy security by listing multiple dimensions and indicators [41,42] have been criticized on practical and methodological grounds [38,39,43]. No such attempts of classification were found for energy system resilience.

* Corresponding author.
** Corresponding author.
E-mail addresses: justinas.jasiunas@aalto.fi (J. Jasiūnas), peter.lund@aalto.fi (P.D. Lund).

https://doi.org/10.1016/j.rser.2021.111476
Received 7 October 2019; Received in revised form 10 June 2021; Accepted 6 July 2021
Available online 15 July 2021

Nomenclature

IEA	International Energy Agency
VRE	Variable Renewable Energy
CI	Critical Infrastructure
NG	Natural Gas
EWE	Extreme Weather Events
SG	Smart Grid
IAM	Integrate Assessment Model
EU	European Union
US	United States

This work aims to improve the basis of complex considerations needed for resilience improvement measures. The specific objectives are to: (1) clarify the meaning of energy system resilience, (2) map out a broad landscape of threats to energy systems from a resilience perspective, (3) map out a more detailed landscape of threats and countermeasures for a specific type of threats with high relevance. In response to each objective, this paper presents a state-of-the-art review of energy system resilience aspects shown in Fig. 1. Clarification of the resilience concept in the energy system context covers terminology and means for assessment. Introducing the terminology is a necessary starting point given the absence of consensus on definitions for the key terms. The section on means of assessment further elaborates in more concreate, yet still system and threat independent, terms that are usually meant by energy system resilience. The broad landscape of threats is mapped out using a simple and grounded framework that integrates the most relevant perspectives and observed trends in the literature. The landscape covers all layers, sectors, and supply chains of the energy system as well as different threat characteristics. This is followed by a more detailed discussion of threats from weather (the cause for most of the energy supply disruptions) and cyberattacks (minor, but rapidly increasing concern). Weather threats are mapped out and discussed in the more specific landscape that distinguishes different meteorological parameters and durations of disruption. Defense measures against short-term extreme weather events are discussed distinguishing phases of disruption as an example of a resilience specific approach. Cyberattack threats, which so far have a few large historical examples and subsequently structured literature investigations, are discussed in terms of increasing digitalization of energy systems, growing interest and capabilities of adversaries, and countermeasures available for energy system operators.

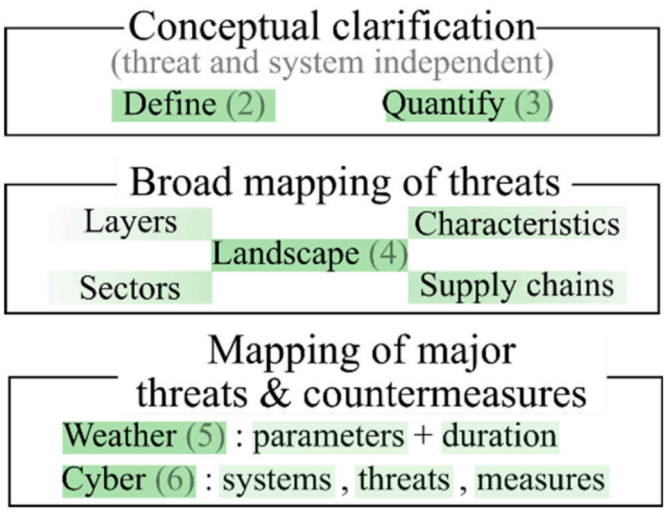


Fig. 1. Structure of the paper. The numbers refer to the corresponding sections of the paper.

Scope-wise the work aims for all types of threats reviewed to cover national and regional energy systems with all sectors and parts of the supply chain, even though there is more attention on the electricity sector systems due to more abundant literature. However, even when reviewed papers explicitly focus on electricity systems many observations seem to apply to other (not necessarily all) energy sectors. Additionally, the expected electrification as an important decarbonization strategy can significantly increase the electricity share in the overall energy demand. Thus, in this paper the more general term of energy systems including all sectors is used for all statements that are not unique to power systems. Policy and research methodology aspects of energy security are outside the scope of this work.

2. Terminology

Discussion of energy system resilience starts with clarifying the terminology used since there is no broad consensus regarding the definition of the term [1,11,17,40,44–46]. This is complicated by the fact that energy security as well as other interlinked terms are also defined differently by different sources [35–38,47–50].

2.1. Energy system resilience

Resilience is a broad concept of "bouncing back" (literal translation of the Latin word "resiliere" [51]) that allows application in many fields, but is difficult to precisely define [52]. The vague definition is found to be the most common critique of the resilience concept [52]. This could be addressed by specifying the definition and the associated theory for the research field or even the research question. All energy system resilience definitions in the reviewed literature include some specification of the system and disruption aspects, but the sets of these aspects vary significantly. The most widely accepted and used definition of energy system resilience is given by the International Energy Agency (IEA) and includes an exceptionally long set of specifications: "*The capacity of the energy system and its components to cope with a hazardous event or trend, to respond in ways that maintain its essential functions, identity and structure as well as its capacity for adaptation, learning and transformation. It encompasses the following concepts: robustness, resourcefulness, recovery*" [46]. In comparison, Roege et al. refer to energy system resilience simply as "*The ability of a system to recover from adversity*" [13]. Arghandeh et al. [11] illustrate the distinction between strength and flexibility associated with resilience by describing a major storm in which a strong oak breaks, whereas a flexible reed bends and survives.

Table 1 provides a summary of the aspects mentioned in various energy system resilience definitions loosely grouped into system aspects to be secured, system abilities to do so, system abilities to counter disruption, and disruption aspects. System aspects to be secured in definitions range from "system" itself to specific performance characteristics. Given a sufficiently strong disruption some damage is unavoidable which calls for prioritized system degradation followed by quick recovery or alternative transformation. Typically, in energy systems and engineering systems more broadly only a single stable state is

Table 1
Summary of aspects and system abilities mentioned in various energy system resilience definitions [11,17,35,40,44,46,51].

System aspects	components, system, structure, (critical) functions, abilities, performance, state
System focused abilities	maintain, degrade gracefully, survive; recover quickly, transform
Disruption focused abilities	anticipate, absorb, withstand, adapt to, learn from
Disruption aspects	internal or external, momentary or continuous, unpredictable, unexpected, high impact, low probability

considered to which system needs to return after a disruption, but multiple stable states are possible [52]. For example, instead of rebuilding damaged equipment, it can be replaced with superior technology and architecture in more suitable locations. In extreme disruptions (some energy system resilience definitions explicitly specify disruptions as extreme and high impact [1,17]) key system ability can come down to survival of critical functions and recovery capacity. Some system abilities to counter disruption (i.e. absorb and withstand) can be viewed as synonyms for system abilities to secure itself. However, some definitions go beyond that and include pre-disruption anticipation [17] and post-disruption learning [46] or even adaptation [13]. Some definitions also provide a classification of disruptions themselves, though this can be expended considerably as it will be shown in the latter section on the threat landscape. Given a large number of possible aspects not covered in reviewed definitions it may be more practical to have simple general definition of energy system resilience and specify it for each use case.

2.2. Energy security

The concept of energy security overlaps with energy system resilience. Often information on energy system resilience is actually present under the energy security label. The IEA defines energy security as *"uninterrupted availability of energy sources at an affordable price"* [53], but there are many other definitions as well [35,37] with commonalities [36] and major differences. Moreover, the energy security definition has changed over the years [35,54] with broadening and diverging interpretations later accompanied by generalization and integration efforts.

Initially, before the oil crises in the 1970s, the meaning of energy security was self-evident as it was predominantly used to describe the supply security of oil in the developed countries [35,54]. Gradually, the definition was broadened up to include other types of fuels, countries, market actors, and perspectives. At the start of the 21st century, environmental and social issues began to be regarded as part of energy security issues [35]. The key questions of "security for whom?", "for what values?", and "from what threats?" became much more difficult to answer [38] which lead to many groups creating their own definitions.

Complexity, narrow focus, and intentional inflation seem often to be the reason for diverging definitions [50]. Given the complexity of the energy security concept in terms of its contextual and multidimensional nature [36,37,41,50], it is not surprising that narrower definitions are often used, which could explain to some extent the differences in the definitions [37]. The complexity of the energy security concept in terms of its blurred and slippery nature makes it difficult to distinguish clearly what is or isn't part of energy security [36,37,55,56].

Cherp and Jewell [39] have tried to simplify the discussion by integrating robustness, sovereignty, and resilience perspectives into energy security. Gracceva and Zeniewski [57] describe energy security in terms of five systemic properties addressing threats at different time horizons. Kruyt et al. [49] described energy security in four dimensions: availability, affordability, accessibility, and acceptability. While this description became quite popular, it was criticized for failing to provide solutions or even raise the key questions [38]. Other studies have identified a large number of dimensions and related parameters [41,42], though such approaches may pose methodological risks [43].

2.3. Overlap between energy security and resilience

The overlap between energy system resilience and energy security concepts is evident though identifying the commonalities and differences exactly is difficult given the blurriness of both concepts. Within the context of broader energy security definitions, resilience is often considered as one of the energy security aspects [35,38,39,47,57].

In reference [1] both concepts were directly compared stating that the differences are subtitle, mainly in the severity of impact and means of evaluation – security against "credible" contingencies measurable at a single state, resilience against high impact and rare unexpected events measurable only considering all phases of disruption. This is consistent with the observation that resilience literature tends to focus on extreme, unexpected, or unknown threats regardless of the occurrence likelihood [1,10,51]. Also, by comparing multiple definitions it is easy to observe that resilience explicitly refers to a possible response to threats (endurance and recovery), while the security concept does not.

In this paper, the distinctions between the security and resilience terms are considered not critical and these could be used interchangeably unless there is an explicit reference to resilience specific concepts, primarily surviving and rebounding from a disruption event.

2.4. Related concepts

Other commonly used concepts in literature on energy system resilience include reliability, robustness, risk, stability, survivability, flexibility, agility, fault tolerance, and vulnerability. Many of these also suffer from differing definitions and are often used interchangeably. Reliability and robustness were found to be the most commonly mentioned concepts directly compared to resilience in multiple sources.

Reliability is compared with resilience in [1,10,11,17,50,51] with main distinguishing themes being time dependence, severity, and likelihood of threats addressed. All sources distinguish reliability as a static concept with time-averaged metrics from resilience, which addresses dynamics during a disruption event. Many of these papers describe the focus of reliability as operation within desired system state boundaries under high probability threats, while the resilience focus is described in terms of less likely threats that knock the system outside the desired system state [10,17,50,51].

Robustness is compared with resilience in [11,39,57]. Arghandeh et al. [11] relate robustness with the strength of the system to perform under designed conditions. However, strength without flexibility, which is concerned by resilience, can lead to fragility and severe system failures once outside the designed conditions. Cherp and Jewell [39] described robustness and resilience as two perspectives of energy security. The robustness perspective was linked to technical failures of energy systems under engineering and natural science disciplines, whereas the resilience was linked to energy market liberalization under economics and complex system analysis disciplines. Gracceva and Zeniewski [57] further specified robustness as a system property to deal with threats on time scales longer than the investment cycle and flexibility as a system property dealing with threats on short to medium (hours to months) time scales.

Definitions on stability, vulnerability, and risk have been discussed in [11]. Definitions for fault-tolerance, survivability, and agility are briefly introduced in [51].

3. Means for assessment

Given the large number and abstract nature of energy system resilience definitions, it is not obvious what indicators, let alone models, should be used for a qualitative or quantitative assessment. Resilience assessment is further complicated by being a system characteristic. Resilience as a characteristic of the system is often influenced more by the system structure, relationships and interactions between different components rather than by the performance of the individual components of the system [50]. Resilience also depends a lot on the type of disruption so much so that increasing the resilience of the system against one type of threat can reduce the resilience to other types of threat [11,44,58]. Thus, it may be better to consider a set of threat specific resiliencies instead of just general resilience. On the other hand, many generic characteristics which make the system resilient against a wide range of threats are known from various fields, where the resilience concept is used [40]. These characteristics include: redundancy, functional diversity (often more important than redundancy), adequate

adaptability (as appose to optimality), firebreaks (the capacity to island subsystems within networks to stop the spread of attacks or failures), and disorder [40]. The latter part of this section presents generic (i.e. threat and system independent) indicators, models, and methods for energy system resilience assessment found in the literature. Many resilience indicators are based on resilience curve, which is presented first.

3.1. Resilience curve

System resilience is often described by its performance changing in time from a disruption event over several phases in so-called resilience curve [1,10,12,17,18,20,51,59–62]. A schematic representation of such performance dynamics is summarized in Fig. 2. Basically, the system performance is reduced after the disruption event hits the system and is restored afterward. The real system performance dynamics in such a case can be very complicated and is therefore approximated by several distinct phases. In the disturbed state not only the system performance is decreased, but also its resilience, i.e. the system becomes more vulnerable to other attacks. Mathaios et al. address this by distinguishing power systems operational resilience (indicated by share of power load served) from infrastructure resilience (indicated by share of powerlines online) [20]. However, alternative indicators may be more suitable or additionally needed depending on system and threat, especially if non-physical infrastructure aspects are relevant. As another example, Erker et al. proposes a set of quantifiable indicators in combination with abstract values like community believes and attitudes [44]. Thus, the selection of indicators for system performance or system resilience may be a complex issue, similar to issues of selecting resilience [63] and security [36,57,64] indicators. During extreme disruption events when damage is unavoidable the main objective becomes minimizing that damage. Controlled and prioritized performance degradation can aid in this regard [1,59,61] and could be viewed as a strategic "retreat" in system functionality. Such "retreating" relies on system modularity, ability to operate without whole segments of the system where impacts of system damage are isolated [12,40]. Here modularity should not be viewed narrowly only within specific physical infrastructure (i.e. decentralization of power production supply side) as an ability to operate when surrounding systems (e.g. digital control platforms [65]) fail may be as important. Right after the end of disruption, the immediate objective is to restore the system as quickly as possible. This involves replacing, fixing, and rebuilding damaged system components. Replacement requires spare components to be available, but allows quick restoration, especially if these components are not just stocked up in warehouses but are already deployed presenting a reserve capacity.

3.2. Indicators

Many resilience indicators appear to be a proxy of the resilience curve, namely height, width, area, or some combination of these three for a certain phase or system performance level [20,51,61,66,67]. Some of these proxies for a specific type of system and threat are linked to the specific characteristics of system components. For example, in absence of cascading failures, the magnitude of a power system's performance drop during a windstorm is largely determined by the fragility of the powerline poles as a function of the wind strength [20,68,69]. Such links enable assessments that do not require complex system models. Linking of the dynamic system characteristic proxy with the system component technical characteristics appears to be similarly used for flexibility, another increasingly important energy system characteristic. Instead of resilience curve, system flexibility information is largely contained in the residual demand curve. For example, high and tilt in the daily residual demand increases and decreases for the systems with a large share of solar power and provide information on the ramp up and down capacity and its rate requirements [70]. This suggests that experiences in attempts to quantify flexibility seem particularly relevant for resilience quantification. Despite the convenience of proxy-based indicators, there is an inevitable loss of information that resilience or residual demand curves contain. Given the possibility to measure dynamics for residual demand or resilience curves retaining this information would enable a more comprehensive and possibly more insightful representation of the system resilience. Thus, more mathematically sophisticated approaches with consideration of trade-offs between ease of use and retaining information seem a promising avenue for energy system resilience quantification improvement that was not found in the literature.

Resilience indicators that do not refer to parameters of a resilience

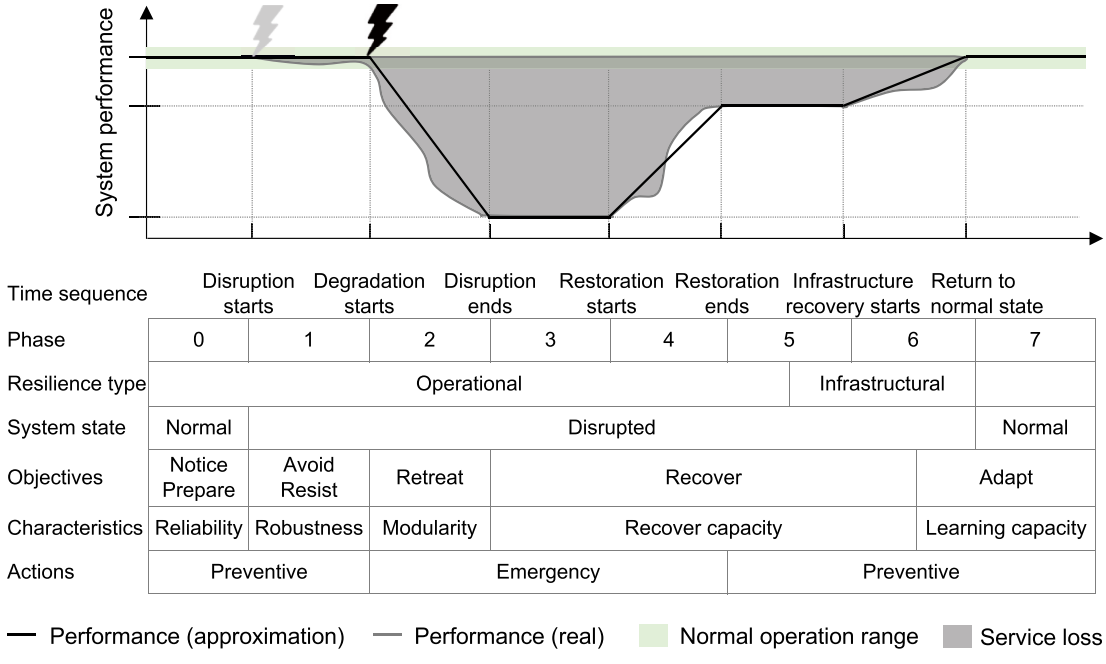


Fig. 2. Resilience curve showing the system performance in time during the disruption event.

curve nonetheless correspond to a certain phase of disruptions. A large number of such metrics corresponding to the four disruption phases has been generated by Roege et al. for physical, information, cognitive, and social aspects of energy systems [13]. Connection with the disruption phases is also maintained in most of the indicators that include additional dimensions, most notably space and uncertainty. The spatial location of the disruption indicators is used for defining system performance with the help of network concepts like closeness centrality or simple heuristics like a sum of demand among accessible nodes [51]. Uncertainty dimensions can be accounted for by stochastically modeling at least one of the variables with an otherwise deterministic formula. However, some formulations define system resilience as a probability of something, e.g. probability that disruption will not reduce system performance more than a specified amount and will not reduce it for a longer period than specified [51]. Apart from the link to a disruption phase, these indicators are very similar to energy security indicators for which the literature is more abundant. Common practices for security indicators such as aggregation into complex indexes and knowledge of associated methodological issues [71] may apply to resilience indicators.

3.3. Models and methods

Presented indicators for existing systems can be obtained using historical data and for future systems using a multitude of methods from various fields. Several papers present extensive lists of assessment methods grouped in different ways. Hosseini et al. present an extensive list of previously mentioned indicators, quantitative frameworks and qualitative models for assessing engineering system resilience [51]. Qualitative conceptual frameworks provide lists of categories, steps, and aspects for resilience evaluation. They resemble similar points covered in energy system resilience definitions, though in higher detail. Quantitative models include system structure-based models using optimization, simulation, and fuzzy logic approaches. Wang et al. review 30 models for power and natural gas networks from a resilience perspective [72]. These models are grouped into optimal operation, topological network, agent-based, probabilistic, and other modeling approaches. Among these categories, the optimal operation models are most widely used, but rarely simulate disruptions. Topological network models represent real network topology with simplified power flow representation that sometimes leads to overly optimistic results (e.g. there is no possibility of cascading failures). Agent based models provide a possibility to model interconnected systems, which is becoming increasingly relevant. Probabilistic models are used to capture uncertain characteristics of system failure. Among probabilistic models the Monte Carlo method is common. Månsson et al. present strengths and weaknesses with examples of methodologies for energy security evaluation from fields of economics, engineering, system studies, and natural sciences [50]. Månsson et al. stated that despite the abundance of methods important gaps remain, especially for assessing future threats. To address these gaps, more work is needed to better represent the evolution of threats and their effect on system development, and comparison of different energy carrier's supply chains.

Among models for physical energy systems subject to disruptions statistical and simulation methods can be distinguished [16,73]. Statistical methods rely on damage assessments of historical disruption data quality. They can be very accurate in aggregate for types of disruptions that are frequent and already have a long historic record [74]. However they are difficult to extend for disruptions without historic precedent and they do not explain the mechanisms of damage. Knowledge of the damage mechanisms can be improved through simulation models, which replicate the disruption and system response. Representation of the failure and restoration processes is a necessary requirement in bottom up type models to capture the resilience as an emerging system quality [75]. Such simulations can be done by modeling the failure (and later restoration) for individual system components using fragility curves (see Fig. 3) that show the failure probability based on the intensity of an environmental parameter (e.g. wind gust speed). Fragility curves were originally developed for modeling building failures during earthquakes, but are increasingly used for power grid component failures during windstorms [68,69,76,77]. A fragility curve for each type of component can be constructed using historical failure data, simulation, physical characterization, or expert knowledge. Multiple fragility curves are needed to accurately represent the impact of different environmental parameters. While power lines have distinctly only two states (working, not working) other components may have partially damaged states.

Considering the large number of assessment approaches presented above, one should note that the ultimate measure of resilience models and indicators is their usefulness in guiding planning for resilience [51]. Likewise, the ultimate measure of energy systems is their impact on everyday life [51].

4. Threat landscape

Energy systems are exposed to numerous threat types, mitigation of which requires different and sometimes contradictory measures. System changes that improve resilience against one threat may be completely ineffective or even decrease resilience to another threat. This indicates that the development and operation of energy systems which ensures their resilience depend on knowledge about a broad landscape of threats. However, even a rough overview is hard to make comprehensively, especially for different energy sectors, non-physical aspects, and threats with characteristics without historic precedent. Fig. 4 presents an attempt to provide a simple and grounded framework for mapping the landscape of major threats to energy systems integrating various perspectives, categorizations and characterizations of energy system threats discussed in the literature. This framework is based on the basic concepts of the system, its environment, and interaction between parts of the two. Threats to energy systems (an extensive list of possible threats by threat source can be found in [5]) originate either from inside the system or from the surrounding environment, while the environment itself can also be disrupted by the energy system. The energy system is presented as a set of overlapping, but distinct layers including all sectors and parts of the supply chain.

Comprehensive mapping of the current threat landscape requires detailed consideration of all framework aspects for the existing system. For future threats, comprehensive mapping requires additional consideration of framework aspects for the system and its environment in their assumed evolution scenarios. Current expectations about the energy transition should be treated with caution, acknowledging uncertainties, especially in case of major failures. Even if energy systems evolved as expected, extrapolating the evolution of current threats may be insufficient as changes in scale can lead to changes in the nature of threats. Generally, new energy sources, technologies, and sector practices replace rather than eliminate energy system vulnerabilities [56,79].

The following discussion in this section presents major examples of

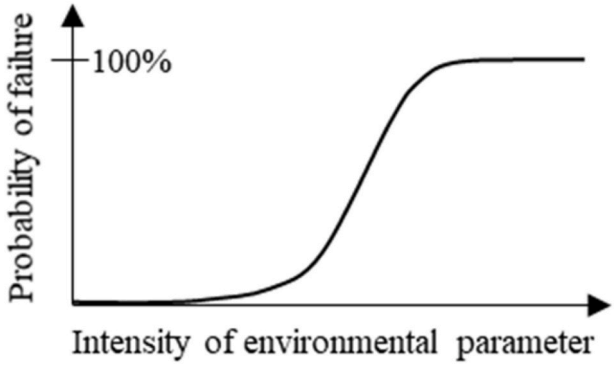


Fig. 3. Fragility curve of an energy system component.

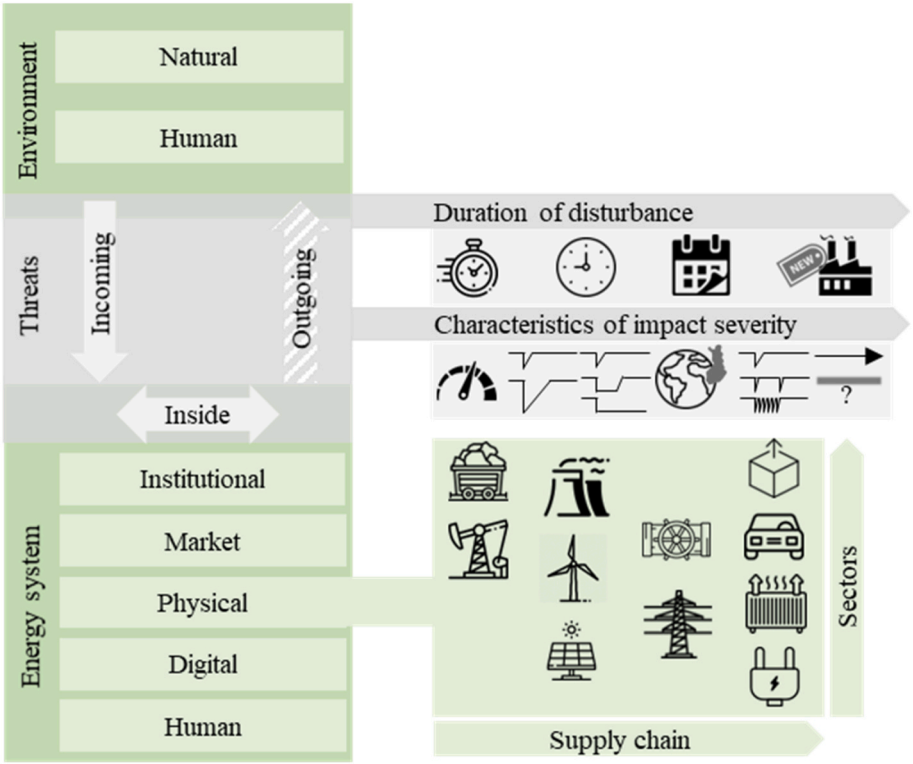


Fig. 4. Framework for mapping landscape of threats to energy systems. (Icons are from flaticon.com).

threats found in the literature focused on broader coverage of energy systems. This undoubtedly leaves out threats discussed in literature focused on specific energy system parts and aspects. However, comprehensive coverage of the landscape (all relevant technologies, sectors, layers, threat aspects) and its evolution (e.g. due to major technological and structural sector changes) is outside the scope of this review.

4.1. Environment and its interaction with energy system

Performance of energy system shapes and is shaped by its environment. Energy system impacts on its environment is a direct concern to resilience of systems composing that environment. The same impacts affect energy systems only indirectly and thus it is not clear if these impacts should be considered as energy system resilience concerns. While certain indirect impacts can be among the major threats to an energy system (e.g. climate change) or major justifications for funding measures to enhance energy security (e.g. high cost of lost load [80], air quality impacts to health [81]) some distinction should be made to avoid confusion and excessive securitization. After all, the issue does not have to be part of the energy system resilience concerns to be important and worth proper resources for mitigation.

The natural layer of environment presents major threats to energy systems in form of extreme weather, space weather, and geological seismicity events [5,16,82]. Extreme weather events are responsible for most of the disruptions in the energy supply, while rare extreme space weather events represent potentially the most catastrophic damage.

The human layer of environment refers to human systems of any type as long as they are outside the energy systems. Probably the clearest distinction within this layer can be made between national and subnational actors. National actor threats to the energy sector are of geopolitical nature. They represented the core theme of traditional energy security until social and environmental concerns started to gain prominence in the 2000s [35,38]. On a subnational level, a large number of actors can represent a threat to energy system resilience. Separatist movements, organized crime and terrorist organizations can physically sabotage energy infrastructures, kidnap personnel and use other means to disrupt normal operation of energy systems [5,83]. On the lower end, individuals can engage in energy and equipment theft [5] or oppose various energy system development projects either by driving up their costs or prohibiting them completely ("not in my back yard" phenomena) [35,41,84–87]. More recently, digitalization has enabled cyber-attacks which could be made by almost any actor though sophisticated attacks would require considerable resources [4]. Growing possibilities for causing a lot of damage by disrupting energy systems and the potential growth of adversaries to do so is indicated by a growing, but still a small number of malicious disruptions [5].

4.2. Energy system

The framework distinguishes five energy system layers that affect each other with failure in one exposing others to additional damage. Three layers are discussed in this subsection with the remaining physical and digital layers covered in higher detail later in the paper. The physical layer that refers to the physical infrastructure of all energy sectors and parts of a supply chain is discussed in Subsection 4.3. Cyber threats for the digital layer that refers to hardware and software infrastructure for monitoring, communication, automation, and remote control are discussed in Section 6.

4.2.1. Institutional layer

The institutional layer refers to public institutions governing the energy system by setting and enforcing policies and regulations. These institutions essentially set the rules for the development and operation of other layers and thus play a key role in determining the resilience of the whole system [83,88,89]. However, this is far from a trivial task in complex energy systems.

Properly functioning institutions aim to govern complex systems timely, efficiently, and consistently in face of high uncertainty. Time constraints set by climate change mitigation efforts are relevant not only

for the decarbonizing the energy sector, but also for diversifying economies of petrostates and ensuring the competitiveness of any country in the future economy, where new energy sources are expected to play a significant part [90]. Additional requirements are set by technological developments that enable new modes of operation (e.g. storage and demand response) and vulnerabilities (e.g. to cyberattacks). Even currently well performing institutions may fail in changing conditions due to so-called institutional inertia, i.e. inability to change established expertise, processes, and incentive structures. In extreme mismanagement cases, countries may become poorer after the discovery of valuable resources experiencing the so-called resource curse. Policy inconsistencies and discontinuities are particularly detrimental for capital intensive markets like nuclear and renewable [91] energy, lengthy technology research and development [92]. However, the success of long-term policies depends on the knowledge about future developments, uncertainties of which can only be partially addressed.

While various energy system analysis techniques can significantly improve the understanding of future developments, there are limits to analytical learning. For example, scenario analysis is feasible only for few scenarios while the presence of only a few unknown variables can lead to thousands of plausible scenarios [93]. Proper consideration of such limitations is arguably as important as studying the observations themselves. Many energy system models use simplifications that severely limit the applicability of their results to real systems [94]. However, such studies, especially in presence of incentives for result hype and politicization, can be taken as a basis for major policy considerations [95]. In other words, there is a risk of energy system studies (used outside their scope of applicability) providing a false sense of confidence that could endanger not only advocated changes to energy systems but also current system functionality. In fact, the existing security of energy systems is not given and may need additional maintenance measures just to maintain current performance. This includes not only physical infrastructure, but also fewer tangible aspects like qualified workforce, governing institutions, and public support.

4.2.2. Market layer

The market layer refers to diverse public and private actors that control the operation and development of energy systems. Examples of major risks in this layer include under-investment or over-investment, time or sector-wise inconsistent development, overoptimization, and outright market manipulation. Under-investment into new capacity is particularly problematic in face of fast demand growth or decommissioning of old capacity. While the capacity adequacy traditionally has concerned developing countries lacking capital, now it may also concern developed countries aiming to close fossil fuel and nuclear power plants quickly without providing sufficient incentives for investment in alternative technologies [96]. The capital intensiveness of renewable and nuclear energy technologies requires patient investors which are complicated by the so-called tragedy of the horizon, i.e. short-term focus in the financial analysis [97]. The opposite problem of over-investment can strand capital intensive assets [90] and raises costs to final consumers. Cost increases can be further exacerbated by inconsistent development in time, i.e. business boom and bust cycles. Furthermore, inconsistent development among system sectors (e.g. renewable energy capacity outgrowing the capacity of the grid [3]) may even create security concerns. Aims to optimize the system can also be pushed too far. Efficiency improvement as the major argument for pushing power sector privatization and deregulation could be questioned in major disruptions such as exceptionally cold weather creating system-wide power shortages for few days in Texas 2021 [98]. During these few days spot market prices rose so much that producers still able to generate electricity collected $44.6 billion, worth their 3-year annual income [99]. Overall economic damage for the state from this extreme weather event range up to $130 billion [100]. Another example of disruption costs exceeding the yearly system costs include manipulation of the newly liberalized power market in California in 2000–2001 that resulted in the state spending an additional $42 billion (in comparison the total energy costs in the Californian wholesale power market were $7.4 billion) [101]. Looking forward some of the market risks posed by the energy transition to renewable technologies concern intellectual property and manufacturing capacity, potentially with even higher market concentration than in the current energy industry [90].

4.2.3. Human layer

The human layer refers to the energy sector employees and customers. Employee-related risks include unintentional and intentional damage to systems accessible by an employee, and workforce shortages. Unintentional damage can be direct (operation mistakes) or indirect (e.g. mismanagement of security credentials). Intentional damage refers to insider risk that is extremely dangerous in the case of nuclear power [102]. Workforce shortages not only increase costs and decrease the innovativeness of energy companies, but also have the potential to shut down services altogether. In case of e.g. epidemic, famine or military conflict significant share of the specialized workforce could be lost without the possibility to replace it quickly. Consumer-related risks include energy theft, consumer manipulation, and social acceptance. Consumer manipulation has not yet been a significant concern, but could become such with growing smart grid capabilities [103]. Social acceptance must be maintained for long periods if major developments such as energy transition are to be achieved. However, the acceptance of such developments depends on many factors, including scale and duration (e.g. size and duration of subsidies needed), and major failures. Major failures of new technologies can quickly turn the public opinion even if the failure occurs in a different country as was the case with nuclear power. Social acceptance research in the energy field mostly focuses on “not in my back yard” phenomena (even though it is a contested concept) in technology and research field-specific ways [104]. Recently this research started to shift from political to psychological aspects and from one technology (mostly wind) to broader systems [104].

4.2.4. Energy system as critical infrastructure

A supplementary approach for mapping threats to the energy system by analyzing its parts could be studying it as critical infrastructure (CI) and common threats posed to it. As with the previously discussed terms, there is no universally accepted definition of critical infrastructure. In general, more developed countries tend to have a longer list of infrastructure systems labeled as critical [105]. However, energy and especially electrical energy systems are almost always considered critical. Furthermore, most if not all CIs are reliant on an uninterrupted power supply.

High interdependency that produces complex behavior is characteristic of CIs. Processes that seem linear are likely to be complex when a broader context with coupling to other infrastructures and environment is considered. Infrastructures can be interconnected physically, digitally, geographically (one facility is close enough to another to cause damage in case of failure), logically (e.g. power market link to the physical power supply). Modeling such complexities is not trivial as simple hooking of different models technically constrained (linking is not always possible due to model specific assumptions or data inconsistencies) and emergence behavior is rarely captured. As a result, infrastructure failures in modern societies rarely result in isolated incidents. Even a single failure in the power system may affect large areas, including areas over multiple countries. The continued growth of interconnectedness between systems forming systems of systems without a single owner or operator, that improves efficiency and convenience at expense of increasing vulnerabilities and cascading failure risks [106,107].

4.3. Physical layer

The physical layer refers to the physical infrastructure of all energy sectors and parts of the supply chain. The commonly used division along

supply chains is between supply and demand sides [108].

4.3.1. Supply side: primary energy

Supply security of oil was the initial focus in energy security viewed through the geopolitical sovereignty perspective [39]. The main oil security concerns involved import dependency (share of imports and options to choose a supplier), reliability of oil supplying countries, and security of transit routes [39,50,80]. The security of transit routes primarily involves the security of key chokepoints in main marine routes [50,90]. The main measures to increase oil security concentrate on increasing the upstream oil resource and extraction system control, diversification (more suppliers or more fuels other than oil), and emergency stock capacity [39]. Security issues of natural gas (NG), which emerged later, are similar but with a more regionalized market (which is now converging due to the spread of transportation in the liquefied form [109]) and higher importance of transportation by pipelines. Coal and uranium are more readily available and their supply is usually not considered a security concern.

Expected growth of variable renewable energy (VRE) would shift system vulnerabilities from stocks to flows [56,90], however, continued use of NG or uptake of sustainably produced chemical fuels such as hydrogen would retain many existing energy security considerations. From a resilience point of view, it is far from obvious if the electrification of energy supply is even desirable if chemical fuels could be produced sustainably and economically on a large scale. Other energy services are already dependent on uninterrupted power supply (e.g. pumping of NG, liquid fuels, hot water in district heating systems), but further electrification could remove important delays between a power outage and effects in other sectors and may reduce options for emergency operations. The geographical distribution of renewables is wider, but still unevenly spread. This suggests reduced rather than eliminated dependency on imports as many renewable studies tend to assume [56]. Also, the increasing competitiveness of renewables is not set in stone - there are limits to economies of scale and there is the possibility of technological breakthroughs not only in renewable but also in fossil fuel technologies. While the fossil fuel industry is old and matured, recent growth in shale gas is a concrete example of additional possibilities. Development of an economic way to extract shale gas outside of North America or more abundant carbon hydrates [110] may decrease the fossil fuel cost and reduce the support for renewables in countries where import dependency is a major driver for transition.

4.3.2. Supply side: energy conversion technologies

Traditionally, the major concern related to energy conversion technologies has been their security against extreme weather events and technical failures. Such threats have often been treated through a technical robustness perspective [39] and addressed with infrastructure hardening and capacity reserves. Specific security concerns with nuclear power have been an important factor for decreasing public acceptance and increasing the costs of this technology [111]. While technical assessments may indicate a low probability for nuclear accidents, nuclear power is subject to unexpected natural, institutional and other risks, most famously illustrated by the accident in Fukushima, Japan [112,113].

Currently, power systems show increasing vulnerability to weather variability [3,96], market variability (origin of resilience perspective in energy security studies [39]), and disruptions in other systems [6]. Energy systems with increasing shares of VRE such as wind and solar power are subject to larger and longer-term weather variations [114], which will require major changes in physical infrastructures and market mechanisms introducing new risks. Further cross-sectorial integration increases risks of cascading failures over multiple sectors [6] that can be partially mitigated by the addition of firebreaks. The development of energy storage addresses these issues and was shown to improve energy security, though the level of improvement depends a lot on storage technology [85].

Further growth of renewables would undoubtedly increase the demand for certain materials while implications to the energy system seem more nuanced. Rare or critical materials needed for renewable technologies may be concentrated in fewer countries than fossil fuels are today, though material supply risks could be mitigated with increased availability and quality of substitutes as well as increased recycling [56]. Furthermore, R. Hoggett compared solar and nuclear supply chains concluding that smaller-scale technologies have shorter and more secure supply chains [115]. However, a frequent portrayal of renewable technologies as small scale with low vulnerability to single-point failure risks could be scrutinized. Renewables are also subject to economies of scale which suggest that a significant share of renewable power production capacity will be in sites with an as large or even larger capacity than many existing fossil fuel plants [56,116]. Similarly, another frequently mentioned benefit from increasing the share of renewable energy, increasing diversification occurs only when renewables are not dominant sources in the system.

4.3.3. Supply side: transmission and distribution

Electricity transmission and distribution networks are growing in size connecting countries and regions driven by economic and geopolitical reasons. This raises risks of cascading failures in larger systems [6] and geopolitical concerns of dependency on neighbors. Emerging dependencies in the power sector seem to have similar characteristics to NG pipeline networks. However, given the mutual balancing needs and local (though more expensive) production options for an electricity importing country, the exporter-importer relationship is expected to be more symmetrical [117]. Examples of developments that may have major geopolitical impacts include the Chinese global energy networks the “Belt and Road Initiative”-project and the “Global Energy Interconnection”-project. The potential implications of the future Chinese infrastructure developments have even been compared to the US protection of sea lanes in the past [90]. The capacity of electricity systems would also need to grow several times if electrification is applied as the main means for economy-wide decarbonatization.

Electrifying other energy sectors allows utilizing large amounts of wind and solar technologies which have advanced significantly in recent years at the cost of losing unique and in some aspects superior qualities other energy vectors provide to the system [118]. For example, the NG network can transport a higher amount of energy (a typical NG pipeline can have up to 40-times higher transfer capacity than a typical electricity transmission line) over long distances without losses and store energy amounts to cover months of regional demand [119]. In both the EU and US more energy is transferred via the NG network than the electricity grid [119]. Additional arguments for maintaining the NG infrastructure include the role of NG for balancing VRE supply [120]; possibility to convert it for transporting sustainable gases such as hydrogen; use of least carbon-intensive fossil fuel in hard to electrify sectors. On the other hand, NG is still a fossil fuel that must eventually be phased out or combined with carbon capture and storage technologies if climate objectives are to be achieved. Thus, prior arguments could also be viewed as fossil fuel industry excuses to continue using it. Furthermore, embracing NG as a transitional technology contains a risk of creating mid-transition lock-ins. While the net value of phasing out of coal and oil may be less ambiguous, some important system qualities may be also lost.

4.3.4. Demand side

Demand side measures have a high potential of making the overall energy system more efficient, flexible, and resilient at relatively low costs. However, tapping into this potential requires dealing with increased complexity and less well-established structure even in the physical layer [108]. Furthermore, the rise of prosumers (consumers which also produce some energy) and energy storage [4] is blurring the line between supply and demand.

One major demand-side threat to energy system resilience within the

physical layer is the decreased diversity of final energy forms. For example, electrification of the heating and transportation sectors makes electricity disruptions much more costly. However, this issue has not been addressed in the literature.

4.3.5. Energy storage

Energy storage allows to balance both inherent and disruption-induced supply-demand disbalances. Thus storage both inherent to the system and specifically in-built storage capacity typically have a positive effect on the resilience. Of course, new facilities come with a cost without necessarily providing additional functions to the system and may also introduce new points of failure. Energy can be stored at various points of the energy system on the supply and demand sides and thus should be considered as another aspect throughout the whole supply chain with a focus on dominant energy vectors in the system.

Currently, the dominant coal and oil can be stored in their original form while NG requires facilities where it can be compressed or liquified. The need for oil reserves was most notably exposed by the oil-embargo from the major oil-exporting countries in 1973–1974. This caused a significant shock to developed countries, which later led to building national reserves and forming the International Energy Agency to coordinate this [121], which remains one of the core responsibilities of the organization [53]. Given the more regional nature of NG, its supply has not experienced disruptions on the scale the oil supply has. However, there were major regional NG disruptions such as 19-day-long shut down of NG gas supply from Russia to Ukraine in the winter of 2009 that also transports a significant portion of NG to other countries in Europe [122]. The more recent example of NG supply disruption includes NG shortage for 31 GW power production capacity due to freezing in Texas 2021 [98]. While large-scale NG storage requires capital-intensive infrastructure and suitable geology, the European Union countries have 86 billion m^3 storage capacity [123], which corresponds to around one fifth of the annual demand [124]. The operation of pipelines and storage facilities for both oil and gas depends on uninterrupted power supply. This also applies to automobile fuel stations. On the other hand, on-demand electricity production depends on fossil fuel stocks as electricity storage is negligible compared to the fuel stock. 97% of the electrical capacity that does exist is in the form of pumped hydro [85]. The remaining 3% are composed of compressed air, thermal and electrochemical storage types. However, electrochemical storage, i.e. batteries, may have higher relevance for security by providing emergency supply to communication infrastructure [125].

The expected higher role of VRE in the future would significantly reduce the inherent storage provided by fossil fuels, part of which would need to be replaced somehow. Part of the new storage capacity needed could be gained from the inherent heat storage capacity of buildings and electrified transport through sector coupling. Regarding additional storage requirements, both power and energy capacities [85] should be considered. However, the current focus is only on the former, e.g. IEA projects batteries to be the fastest growing source of flexibility in power terms for the next 20 years [126]. Batteries could be used in many ways to improve system resilience, e.g. distributed near or at households would lower the vulnerability to grid failures. However, batteries due to high costs of the storage medium are unlikely to become economical for long-term storage, which would be needed in VRE dominated systems [120]. Retaining fossil fuel use just enough to cover seasonal shortages would greatly simplify the challenge, but it would not be consistent with the climate mitigation goals in a long term. Pumped hydro and compressed air storages are also unlikely to be used as seasonal storage – while the storage medium (water or air) is cheap, it has low energy density and requires large-scale infrastructure. This leaves chemical fuels such as hydrogen as an option, which is typically considered for long-term electrical storage [123,127,128]. Both the possibilities of using some fossil or sustainable chemical fuels would suggest that some of the existing storage issues would remain far into the future.

4.4. Threat characteristics

Given the number of possible threats to the energy systems, there is a need to determine which of these are of the highest relevance and how to prepare for them. One way to proceed could include filtering potential threats using various characteristics. Winzer et al. [37] proposed a framework to prioritize threats to energy systems according to the severity of the criteria shown in Table 2. Most of these characteristics are self-explanatory – faster, bigger, longer, or more widely spread disruption will affect the system more severely. The duration of disruption is rarely specified though it could be assumed to range from a few seconds to several days, considering the type of disruptions typically concerned. There are, however, disruptions with much longer duration (e.g. droughts, trade embargos, technological breakthroughs [5,57]). The frequency of disruption becomes relevant when the system does not have enough time to recover its level of resilience [44]. Multiple contingencies in a short period are unlikely, but they are possible [129]. Frequent disruption events are much more likely when there are linkages between these events. For example, a malicious attack could be specifically timed after a natural disruption event that has damaged the system. The last characteristic in Table 2, the sureness, distinguishes disruption events according to information available about them. The less is known about the event the more relevant resilience concepts become.

5. Weather-driven threat

While literature tends to focus on the impacts of energy systems on the environment [14,21,130], energy systems themselves are among the most vulnerable systems to environmental changes [131,132] and weather extremes. Fig. 5 maps out the landscape of weather-related direct threats to energy systems accounting for weather parameters, the typical duration of the disruption, and the type of the impact. This landscape representation is limited in the following ways:

- The typical duration of the threat is indicative only;
- Climate change includes only threats from changes in typical weather excluding extremes, even though the changes in frequency and intensity of certain extreme weather events could be the major impact of climate change [73,133];
- Indirect impacts on energy systems through other systems such as oceans and cryosphere (e.g. sea-level rise impact), biosphere (e.g. biomass use for food versus energy) are excluded;
- Only broad weather-related threats are discussed.

5.1. Extreme weather events

Most of the energy system disruptions are caused by extreme weather events (EWEs) [5,16]. EWEs refer to an occurrence of weather with specific meteorological parameters close to the upper or lower bounds of historical data for a certain period [58], i.e. they are rare. EWEs foremost affect the physical layer of the energy system (Fig. 2) in a specific geographical area. Most of the weather-related disruptions in power systems are due to storms [5,16,18]. Heat waves, droughts, and floods

Table 2
Threat characteristics and their possible types [37].

Characteristics	Types
Speed	Constant/Slow changes/Fast changes
Size	Impeding change/Small change/Phase change
Sustention	Transitory/Sustained/Permanent
Spread	Local/National/Global
Singularity	Unique/Seldom/Frequent
Sureness	Deterministic/Stochastic/Heuristic/Unknown

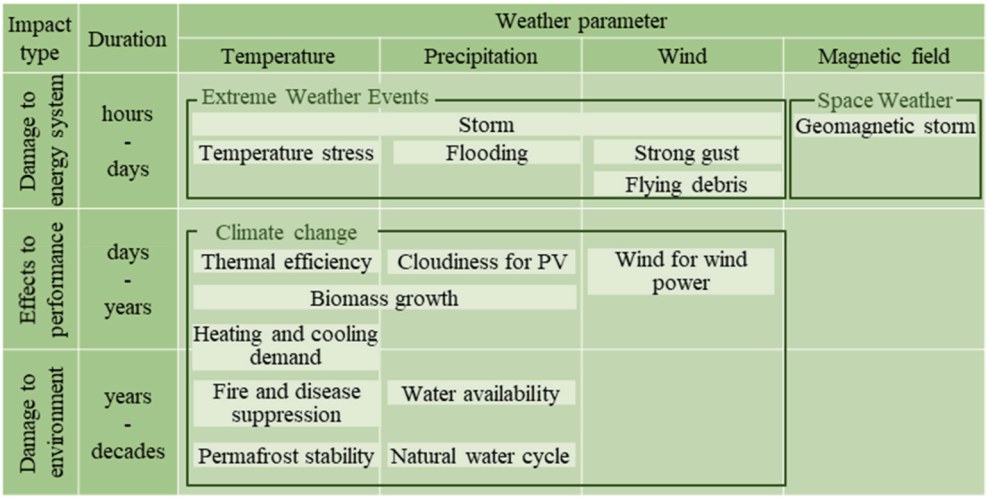


Fig. 5. The landscape of direct weather-related threats to energy systems. Damage to the environment refers to damage to natural systems whose replacement by human-made systems will require large amounts of energy.

may also cause damages to energy systems. From the resilience analysis point of view, these can be viewed in the same way as storms. The risk of mechanical damage of equipment under thermal stress exceeding the design temperature range of equipment may need different analysis, but it is not considered here. For longer-term weather extremes, resilience improving measures are slightly different and are discussed separately together with climate change issues in Section 5.2.

From a resilience perspective, the defense measures for any type of threat should be viewed by distinguishing the different phases of disruption, i.e. following the resilience curve (Fig. 2). Given the large number of historic cases, EWEs are arguably the most suitable disruption type for showcasing established defense measures throughout the disruption phases.

Phase 0 – calm before the storm. Weather cannot be reliably forecasted for more than a few days. Therefore all major preparations against disruptions need to be made based on historical data and estimates of specific EWE occurrence likelihood. Probabilistic methods for such estimates need to account for more extreme events than previously observed [78].

The most straightforward type of methods to improve resilience against EWE is the hardening of the physical infrastructure. Hardening refers to retrofitting and reinforcing physical equipment to make it less susceptible to hazards, primarily for wind, flying debris, and flooding. It includes equipment revitalization and reinforcement, undergrounding or elevation, relocation, the addition of duplicative components and water insolation, vegetation management (especially relevant to electricity transmission and distribution grids) [16,17,62,134–136]. Many of the hardening techniques are very expensive limiting their economic viability to special cases for the most important, exposed, and yet-to-be-built system components [134,135]. Measures which are not cost-effective from the utility point of view may still be very economic when societal costs are considered [135]. However, even when a hardening measure is economic its impact on resilience against different threat types needs to be evaluated. For example, undergrounding of power lines make them impregnable to wind and surface debris, but is more expensive and lengthy if the line is broken by other causes such as earthquakes [136].

Other methods to increase resilience include changing system topology (e.g. decentralized and interconnected systems are significantly less vulnerable to single-point failures), stocking of functioning repair equipment and spare parts, obtaining mobile units for temporary operation, employing a sufficient number of repair crews, developing emergency strategies, and training personnel [1,16].

Phase 1 – early forecast. Once the forecast becomes available about an approaching EWE, newly obtained information can be used to change energy system operation to a safer mode. For example, the UK power grid operates in normal conditions with the N-2 requirement level (system has to be able to withstand the failure of the two largest components), and in bad weather conditions, the N-3 requirement level is applied [62].

Phase 2 – absorbing the hit. System performance and capabilities maintained at this stage are largely dependent on the preparation level of physical infrastructure and operating personnel. Another major factor at this stage is situational awareness, which can be significantly enhanced with digital grid capabilities [16]. Since most EWEs are over in a matter of hours, days at most, the shutdown of a large part of the system during this time to secure the equipment is an option.

Phases 3–4 – power restoration. The extent energy services can be restored and the speed of this restoration depends critically on the type of damage and prior preparation including the presence of redundant elements in the system, remote control and automation capabilities, training of operating personnel.

Phases 5–6 – infrastructure restoration. The pace of infrastructure recovery depends a lot on the availability of spare parts, repair crews, and remote monitoring capabilities, damage, and clog in the surrounding environment (e.g. damaged bridges and trees on the road). Survived segments in more decentralized and interconnected systems can not only contribute to the overall system restoration but also may have an option to operate in island mode [16].

Phases 6–7 – adaptation. It is a common practice to rebuild damaged system components or to replace them with the same type and size components in the same place. This may not be optimal, especially in the case of large-scale damage in energy systems or systems consuming that energy [137]. If the restored level of system operation is satisfactory, actions are no longer so urgent and some alternatives can be considered.

5.2. Climate change

Climate change represents changes in typical and extreme weather conditions (precipitation, solar radiation, wind speed), which affect the performance of both renewable [21] and fossil-based energy systems.

5.2.1. The basis for climate impact knowledge

Climate change impacts on the energy sector and their implications to society have mainly been studied using integrated assessment models (IAMs). IAMs include several stages to model the future climate and direct effects to energy systems in which the climate and possibly

societal effects based on previously computed energy system change [132]. IAMs are limited by many simplifications and abstractions [138], climate data availability and quality [139], limited empirical validation [132], cascading errors and uncertainties adding up with each model stage [131], lack of representation for changing demand and available equipment, and geographical coverage (especially for large developing countries) [132]. Also, IAMs use high geographical, time, and technology aggregation in part due to data limitations, but also due to the need to obtain climate change trends with confidence [139]. The data limitations have noticeably been reduced in recent years [138]. Other areas of IAMs, where additional research is needed, include the integration of different disciplines on climate impact modeling, effects on the supply side, and impacts of stochastic EWEs [132].

5.2.2. Temperature

On the supply side, the temperature affects the efficiency of thermal and solar power plants [73,138–140], cooling requirements [6], biomass output (length of the growing season, water availability, crop diseases) [140,141]. Low temperatures can lead to icing of equipment (e.g. 9–45% of the wind power downtimes in Finland may be due to icing [15]), or icing of sea cover with major implications to offshore operations. On the other hand, higher temperatures in permafrost areas can cause foundation stability issues for all large objects.

In electricity transmission and distribution lines, a higher temperature reduces the power transfer capacity and the efficiency as well as the earthing efficiency [73,140].

Some demand, most notably space heating and cooling, is highly dependent on temperature changes [132,139]. There is a consensus on an increasing cooling demand with increasing temperatures, but such a consensus for the change in heating demand has not been obtained [138, 140–142]. The resulting demand changes impact not only the total energy consumption but also the consumption seasonality and the preferred fuels (e.g. cooling is predominately powered by electricity while heating mostly utilizes other energy sources).

5.2.3. Precipitation

Precipitated water is used in upstream fuel treatment, power production in hydropower plants, cooling in thermal power plants, cleaning of solar panels, etc. In 2016 hydropower was the largest renewable energy resource in the electricity sector accounting for 16.6% of global power production [143]. This production is subject to high annual variability. Dry years are a significant energy security concern to countries with high shares of hydropower [129]. Thermal power production relies heavily on water for cooling (e.g. 43% of the water demand in the European Union is used for cooling in power production) [6]. This creates a risk of losing a large portion of production in case access to water is limited. For example, during the heat waves in the year 2009, one third of French nuclear power plants were shut down [6]. Due to the cooling water demand, power plants are often built near water sources, which puts them at risk of flooding [141].

The use of carbon capture and storage is also expected to increase the water demand [132]. Water is also needed for the cleaning of solar panels (an important constraint in dessert areas) [144]. Cloudiness affects the solar radiation and thus also the solar power output [139]. Water availability affects biomass growth and its quality. In contrast, wind power does not require water [145]. Most of the electrical energy storage capacity (>99%) is based on pumped hydro storage [123,128, 146], which depends on water availability in open reservoirs.

Significant amounts of energy are used for water transportation, treatment, and increasingly for desalination in the end-use side of energy systems. The need for water may increase if natural water is replaced by transported water (e.g. south-north water transfer project in China [147]).

Another important resilience aspect in water-energy system interaction is the transboundary nature of large river basins (e.g. 40 out of 110 river basins in the European Union are located in at least two countries [6]). Geopolitical implications of associated relationships are likely to intensify in case of water scarcity.

5.2.4. Wind

While extreme winds are among the largest hazards to power grids [5], typical wind speed characteristics almost exclusively concern wind power production. Possible wind speed changes due to climate change are already a major concern as they can affect the overall economics, suitability of specific sites, plant design, and operation strategy [15]. These changes could become a concern for power system stability given the expected growth of wind power, but this has not yet received much attention [21]. The number of studies on the effects of climate change on wind resources is ample, but they are subject to high uncertainties and a lack of agreement between results from different models [145]. The difficulties in these studies include the unclear extent to which local conditions need to be accounted for shaping the wind resource [21], lower accuracy of models in predicting wind climate compared to other meteorological variables [22]. Most existing studies report a change in annual wind power output variation to be less than 15% depending on the location [21,22,145,148].

5.2.5. Solar geoengineering

While greenhouse gasses (mainly CO_2) increase the global temperature by reflecting the earth's outgoing infrared radiation, other gases and particles could do the opposite, i.e. reflect incoming solar radiation thus reducing the temperature. Such human-controlled global climate referred to as solar geoengineering could be done at relatively low costs. Due to the global mixing of the atmosphere, solar geoengineering cannot be limited to a particular location. Also, the pre-industrial temperature level is unlikely to be reached, nor would ocean acidification be stopped. Specifics on the physical implications of solar geoengineering are poorly understood. In addition to this, solar geoengineering presents major geopolitical risks including weaponization and misuse of geoengineering, and disagreements between countries in the desired climate [149,150].

5.3. Space weather

Space weather refers to conditions in our solar system created by energetic particles and subsequent magnetic fields released from the sun [151]. Space weather is generally calm, but occasionally extreme events occur [152] when high amounts of particles are released during solar flares. Fluxes of these particles can overpower the earth's magnetic field and cause a geomagnetic storm in the earth's atmosphere. Such a magnetic field can induce currents in power lines and physically damage electrical equipment.

The most powerful geomagnetic storm recorded known as the Carrington event happened in 1859 causing a 2-day failure of telegraph systems over Europe, North America, and some parts of Asia and Australia [9,153–155]. A much weaker solar storm was experienced in Quebec, Canada in 1889 causing a 9-h blackout [151,155–157].

A Carrington-type of event would be catastrophic for present power systems. Long transmission lines allow the induction of large static currents, which can damage connected infrastructure, especially transformers [151,153,158]. Generators may also be damaged if not disconnected in time [159]. Similarly, geomagnetic storms can induce currents in other networks such as digital communication, railways, oil and gas pipelines [159]. Unlike the other natural disasters, the effects of the major geomagnetic storm would be global and affect developed countries more than developing ones. As a result, spare parts, access to human and other resources from neighboring regions could be limited. Also, power restoration may become difficult and lengthy if major system components are damaged requiring their replacement [9,153,160]. Power shortage for even a few days could paralyze critical services like water supply, food refrigeration and distribution, health care (after the fuel in backup generators run out) [9,153,155,161], and longer-term

shortages could even affect food production [162].

Terrestrial weather storms occur much more frequently than geomagnetic storms. It is estimated that major Carrington-type of geomagnetic storms could occur around once in 150 years, whereas a Quebec-type of the storm could occur once in less than 40 years [155].

Efforts to minimize the impact of a geomagnetic storm include a better understanding of the physical phenomenon itself, observations on the solar activity, preparedness to shut down and disconnect equipment before the storm, and improving power grids' physical resilience. The physical phenomenon of a solar flare causing geomagnetic storms is complicated and the current understanding is not yet adequate to make reliable forecasts [154,160]. Building capabilities for solar activity tracking and subsequent storm forecasting is often considered one of the key areas to increase resilience against geomagnetic storms [153,155,163,164]. The typical travel time for charged solar particles from the sun to the earth is around 3–4 days, but travel times shorter than even an hour are theoretically possible [152,153]. A Carrington-type geomagnetic storm reaches earth in under 18 h [155,160,165]. Physical infrastructure could be made less vulnerable by power line undergrounding, enabling transformer tripping, adding grounding points, capacitors to block additional direct currents, redundant and backup transformers [164]. Described measures to improve resilience are, however, still subject to many unknowns concerning the effects form geomagnetic storms on the power grids [163].

6. Cyber threats

Increasing digital capabilities to energy systems make them more efficient and secure against traditional threats such as extreme weather events and technical failures. At the same time, digitalization exposes the energy sector to cyberattacks through an increasing attack surface [8,166–168]. While cyberattacks remain responsible only for a small fraction of energy supply disruptions, the potential damage is significant and increasing quickly.

Potential consequences of cyberattacks include data theft, power theft, denial of power supply, disruption of normal energy system operation, and even destruction of equipment [27,29,166]. The most commonly used grouping of cyberattacks and corresponding defense objectives concern with energy system component availability, integrity, and confidentiality [29,169–172]. Attacks on availability aim to delay, block, or corrupt communication; attacks on integrity to modify or disrupt data exchange [173]; attacks on confidentiality to acquire unauthorized information. Availability and integrity are critical for the reliable operation of energy systems. Compromised confidentiality would not be critical in this respect, but its importance increases with an increasing number of smart customers and amount of sensitive data [29].

The landscape of cybersecurity could be described as a kind of arms race taking place in the digital layer of energy systems between system operators and their adversaries. This continuous race has an inherent asymmetry as the defenders have to protect the system against every attack, while the attackers can attempt disruptions continuously mostly without consequences [7].

Comprehensive assessment of the attack surface and subsequent security landscape involves identifying the target (equipment or software) and its functionality, possible attacks and their implications [166]. Examples of such analysis performed for advanced metering infrastructure [166] and wind power plant farms [174] indicate common cyber security issues for quite distinct system components.

Digitalization of energy systems is especially intensive in so-called smart grids (SGs), which handle large amounts of data on power supply and demand for the optimal and effective operation of power systems. Abundant SG literature often overlooks security concerns focusing more on technical implementation and corresponding benefits [7,174]. Among reviewed sources, the most extensive discussion on SG cybersecurity issues was found to be the guidelines composed by the National Institute of Standards and Technology [175].

6.1. Digital layer of energy systems

6.1.1. Network differences: smart grids versus internet

Digital networks in energy infrastructure differ from established information and communication technology networks such as the internet, which severely limits the applicability of existing cybersecurity solutions. Differences with obvious cybersecurity implications include [7,26,29,176] the following:

- **longevity** of component lifecycles is much longer than in consumer electronics, which requires installing hardware compatible with future software updates and integrating hardware already in the field;
- **remoteness** of many components makes remote control and updates an economic necessity while at the same time limiting feasible digital and physical security options;
- **speed** requirements are much stricter than in traditional data transfer networks; sometimes critical operations in SGs require delays to be shorter than a few milliseconds [29];
- **always on** requirement – while almost all data systems could be temporarily stopped and rebooted in case of infection, such procedures in power systems would be complicated and expensive;
- **privacy** and security goals may be conflicting.

Differences with less obvious, but nonetheless important cybersecurity implications include [7,26,29,176] the following:

- **size** of the system as SGs can have 2 to 3 orders of magnitude larger number of connected intelligent devices than the internet, making network monitoring and managing extremely difficult [26];
- **monocultures** of hardware and software are subject to identical vulnerabilities [7];
- **heterogeneity** in protocols due to lack of standardization is an opposite problem, complicating energy system management and potentially opening security gaps;
- **machine to machine** as a dominant communication type is vulnerable to data spoofing.

The differences mentioned above have implications for the rollout of security solutions. The software industry has a history of releasing insecure products and patching them later [177,178]. In the energy sector, this could result in "billion-dollar bugs" [179,180], which could not be easily fixed as testing would be required before patches could be applied to critical infrastructure [177]. Thus, software development in more security-sensitive sectors such as banking may provide more applicable lessons. However, some widely used SG components were initially designed without much security considerations. For example, the SCADA systems used to monitor and remotely control components of critical energy infrastructure were initially designed to be closed systems, but are now interlinked with other systems [181].

6.1.2. Digitalization of consumers

Traditionally, energy consumers have been very passive actors in energy systems. However, the situation is changing with the rising number of consumers connected to SGs, increasing amount of data flows, and control capabilities. Along with these developments, the number of risks is increasing as well. First, privacy concerns over larger amounts and more sensitive data increase. Personally identifiable information from SGs (e.g. consumption patterns indicating the use of appliances and presence of people at home) on its own or combined with consumer data from the internet [7] can enable people with excessively invasive or malicious intentions [172,182]. Second, smart devices could be hacked to manipulate consumer behavior causing problems both to consumers and the overall network (e.g. increasing peak consumption,

lower voltage profiles) [182]. Hacked devices could also be used as an entry point for hacking into other devices at home [183]. Third, the proliferation of power system control capabilities takes place at least in part at expense of traditional system operators. Smart consumers, which still are likely to have more limited understanding and technical means, can be manipulated or have their systems hacked [65,103], but traditional operators would have a much harder time correcting the situation. Finally, major incidents in SGs could shift public opinion against this technology in a similar way as with nuclear power in the past [178]. This would not only limit the SG technology and market development but also reduce the number of acceptable technological options for advancing energy system transition objectives.

Digital platforms are developed to monitor and manage energy flows between consumption loads, production and storage units as well as to crowdfund renewable energy investments. These platforms can unlock otherwise economically inaccessible capital and flexibility resources aiding VRE growth while increasing energy system resilience. The same platforms can also "disrupt" existing market safeguards by modifying skills and resources that previously were part of the public sphere [65].

Digital platforms in the energy sector have a non-negligible influence on the ethical discourse of the energy transition, especially in the context of the politicization of energy consumption. This influence may not be optimal given the current dissonance between rhetoric and reality of digital platforms as shown in Table 3. Rising barriers for new entrants could also lead to market monopolization. Only a small number of platforms could become dominant over large areas in case they develop similarly to social platforms [65]. Even if such a platform aggregates highly decentralized physical assets, its hacking could have more damaging impacts than hacking of major components in a highly centralized system. Likewise, simple misinformation spread over social networks could have significant damages in SGs [103].

6.2. Cyberattack security environment

6.2.1. Adversaries

Adversaries to energy system cybersecurity can be distinguished by their capabilities, objectives, and relationship to the targeted energy system. By capabilities, adversaries range from amateur hackers, against which most companies can protect themselves, to state actors against which government support may be necessary [4] (see Fig. 6). All these actors seek an economic, market, or political benefits. Adversaries can be divided into inside misbehaving and outside malicious actors [29]. The former group includes consumers interested in stealing energy [168] and companies interested in gaining competitive advantage through unlawful means [7,26]. The latter group is more dangerous and includes individual criminals, criminal and terrorist organizations, and state actors. State actors interested in influencing the decisions of other countries are particularly dangerous due to the vast resources at their disposal and their particular interest in energy systems as critical infrastructure. Cyberattack capabilities of such state actors are increasing quickly [182].

Table 3
The dissonance between the rhetoric of how digital platforms are representing themselves and reality [65].

Aspect	Rhetoric	Reality
Digital platform's role	facilitation	mediation
Traditional system's role	no longer needed	used without paying for leads to higher cost for other consumers, higher grid strain, utility death spiral
Energy cooperatives	frontrunners of energy democracy	potential users of public good for communal benefits
Digital platform's impact	accessibility, openness, and equality	infrastructural layer of political divisions
	transparency and choice	transparency and choice, plus new opacities, dependencies, and uncertainties

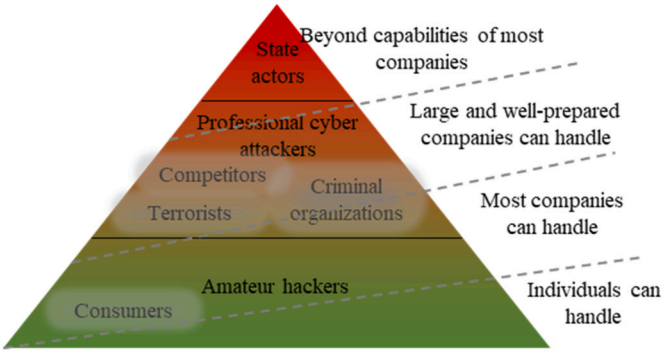


Fig. 6. Energy system actors and adversaries by their capabilities. Adapted from IEA [4].

6.2.2. Attacks and means of attack

New types of cyberattacks have recently been witnessed. These include advanced persistent threats, botnets, zero-days, and distributed denial of service [25,167,184]. Even though new stealthy and multi-stage attacks are extremely hard to defend [7], many companies may need to address more basic security concerns first [180]. For example, initial access to energy infrastructure in some of the major cyberattacks was obtained through emails [7].

While a large number of companies have experienced cyberattacks, the number of successful large-scale cyberattacks remains, however, limited [177,185]. Examples of large-scale damage include the destruction of electrical power restoration equipment and cutting off the power supply for over two hundred thousand consumers in Ukraine [166,186] and destruction of uranium enrichment centrifuges in Iran by changing their spinning speeds [4,7].

Pure cyberattacks can be combined and enhanced by attacks on human and physical layers of the energy system [170,171]. The cyber-attack surface can be widened up by compromising employees with access to secured systems through bribery or threats. Cyberattacks could also be made in combination with physical attacks on energy infrastructure. While combined attacks could have a high impact [28], the damage caused even in pure cyberattacks is difficult to predict [182].

Malicious software (malware) for SGs differs greatly by intended functions, capabilities present, methods used for its spread (active worms and passive viruses), and operation after infection. Examples of methods employed to avoid detection include encryption, generation of distinct instances, and self-disinfection. The key trends in the recent development of malware for SGs include increasing complexity and modularity, operation becoming slower, but stealthier, a shift from disruption towards espionage and data theft, increasing capabilities of physical destruction, broadening of capabilities and access vectors, and attacks becoming more targeted. Possible future malware types (pandemic, endemic, contagion) have been identified and their characteristics and key countermeasures have been investigated based on analogies with biological diseases [7].

6.3. Defense measures

Cybersecurity defense measures involve people, software, physical infrastructure, and underlining energy system architecture. The key measures are shown in Table 4 and explained in more detail later in this subsection.

Network protocol design methods allow to detect and block denial of service attacks based on signal characteristics (strength and transmission failures for detection, transfer frequency, and source address for

Table 4
Key cybersecurity defense measures [7,29,174,182].

People	Software	Hardware	System
cyber-hygiene	Use:	Software determined:	security by design
access restrictions	- timely updates	- sizing for updates	implicit deny
password policy	- strict firewall	- air gaps	segmentation
user education	- antimalware	Physical security:	decentralization
security personnel expertise	- backups	- strong doors and locks	fall-back strategies
cross-department communication	Design:	- cameras	
	- network protocols	- security personnel	
	- cryptography		

blocking). Network measures can help ensure availability, but are ineffective for securing integrity and confidentiality of energy system operations [29].

Physical hardware security measures are not available for each of the system components leaving higher requirements for other types of measures.

Cryptographic measures aid all aspects of the energy system (availability, integrity, and confidentiality). Different types of cryptography are available differing in their symmetry of decryption key and transfer time. A major dilemma for choosing a certain cryptography type for a specific SGs application is the balance between the security level provided and computational resources required [29]. In case of future advancements in quantum computing, existing cryptography methods may become ineffective and new ones may need to be developed [182].

Security by design refers to the practice of considering security aspects already in the network design stage and not as additions for an already developed network [182].

Implicit deny measures allow to minimize the attack surface leaving necessary functionality only. It should be applied to all aspects of the system, including user management, firewall rules, installing hardware without (or at least with disabled) unnecessary functionality [26,174,177].

Decentralization of critical digital energy system capabilities requires counteracting malware propagation methods without using attacked network [7].

Fall-back strategies in the SG context consistent with the resilience concept could mean a system's ability to remain operational while "going dumb". For example, cyberattacks like the one in Ukraine could be more damaging if successfully executed in more modern grids [187].

Both establishing and utilizing these measures require cyber situational awareness which includes knowledge of the current network situation, situation evolution during an attack, quality of collected information, the impact of attacks on critical equipment, attacker behavior, and possible future steps [7]. Implementation of sufficient cybersecurity measures in the energy sector relying only on internal quality assurance and certification may be insufficient. Regulation, similar to one in the health sector, may be needed [179]. An important question is which portion of the digital value chain should be under government control. Other potentially needed roles of the government in the energy system cybersecurity space include certain intelligence information sharing [182] and the establishment of a cyber incidence response ecosystem [177].

7. Conclusions

Energy systems are exposed to numerous threats, the potential impacts of which range from inconsequential (energy systems can absorb them without change in performance) to society threatening (restoration taking years) ones. The concept of resilience provides a valuable perspective for developing countermeasures to address many of these threats. It allows to deal with moderate disruptions in a more economic manner and is essential in overcoming extreme and less known threats. The current growth in uncertainties and potential societal costs of energy system disruptions is placing resilience among the major considerations for the design and operation of energy systems.

Designing a resilient energy system can build upon abundant experiences from the resilience concept used in multiple fields as well as from the knowledge about threats from different energy security and reliability studies. A resilient system is generally characterized by high redundancy, functional diversity, adaptability, and modularity. Arguably, the most distinct aspect of a resilient system is its ability to bend rather than break, i.e. controlling unavoidable damage in a way that allows reducing the extent and/or duration of the damage. The ability to recover from disruptions is in fact present in almost all energy system resilience definitions that despite the common themes vary noticeably. The extent and duration of a damage are measured by most of the resilience indicators that take a proxy of the resilience curve, i.e. the system performance change during the disruption. Resilience as system an ability obviously depends on the system, but the threat type and the characteristic dependence are equally important. Given that the mitigation of one threat can increase the vulnerability against other threats, calls for at least rough understanding of the broad threat landscape.

This work presented a broad overview of the threat landscape and a more detailed review of the weather and cyber threats. The landscape was mapped using a framework that distinguishes: (1) interactions between parts of the energy system and its environment; (2) energy system layers, sectors, and supply chains; (3) threat characteristics. The physical layer in the literature has the most established structure and could be the basis for grounding the other layers. The other layers are important not only in terms of their relationship to the physical system, but can disrupt the energy system by themselves (e.g. market manipulation or a cyber-attack stopping the energy supply without physical damage). Weather threats traditionally were a major concern to energy systems in terms of short-term extremes (namely storms), which in some locations can increase in intensity and frequency due to the climate change. However, climate change is also relevant in terms of typical weather changes as it can strand capital-intensive infrastructure in no longer optimal conditions. This presents significant risks as energy systems, both fossil fuel and renewable energy dominated, are among the most vulnerable infrastructure systems to the natural environment. Extreme space weather events, though rare, have the potential to cause major blackouts and physical damage to power system components on a global scale. The relevance of cyber threats is increasing rapidly due to increasing: (1) attack surface, (2) malware capabilities, (3) number and resourcefulness of adversaries. Despite these developments, surprisingly little attention to cybersecurity has been given. Existing cybersecurity solutions, primarily from the internet industry, can be employed only to a limited extent due to the major differences between the networks. The attach surface is increasing primarily due to digitalization that not only helps to improve the system efficiency but also the resilience against traditional weather and technical failure threats. This is one of the best examples of resilience trade-offs that require serious consideration of different threat types, including traditionally insignificant threat types.

Structural changes expected in the energy transition can reduce many of the currently relevant vulnerabilities to energy systems, but can also exacerbate other vulnerabilities. Some of the most relevant threats to future systems may be entirely irrelevant for current systems. This indicates a need for broad remapping of threats to expected future system in the development scenarios. Future resilience evaluations should be treated with caution as a false sense of security is itself a major vulnerability. Also, it should not be forgotten that changes in scale could lead to changes in the nature of threats. The increasing interconnectedness of systems in particular increases the complexity hiding security gaps and the increasing magnitude of worst-case costs that could instantly wipe out any savings from system coupling. In the long run,

systems that are safe to fail may outperform systems designed with consideration of a larger number of threats and for higher reliability standards.

Considering future work several themes appear highly promising:

- resilience quantification that represents the resilience curve more comprehensively than arbitrary proxy while retaining ease of use would be very useful for studying the resilience of energy systems undergoing structural changes;
- mapping landscape of defense measures over different threat types distinguishing disruption phases (as it was done for the extreme weather events in this paper) and time until the disruption (preparatory versus reactive actions) may complement the resilience perspective;
- applicability of defense theories against diverse and unexpected threats from other fields like military to energy systems;
- resilience tradeoffs for electrification and sector coupling;
- robustness of energy system development scenario preferences in case of major disruption.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This work was supported by the Nordic Energy Research (project Flex4RES, grant number 76084) and the Research Council at the Academy of Finland (project WISE, grant number 312626).

References

[1] Gholami A, Shekari T, Amirioun MH, Aminifar F, Amini MH, Sargolzaei A. Toward a consensus on the definition and taxonomy of power system resilience. IEEE Access 2018;6:32035–53. https://doi.org/10.1109/ACCESS.2018.2845378.
[2] Core Writing Team, Pachauri RK, Meyer LA. Climate Change 2014: Synthesis Report. Contribution of Working Groups I, II and III to the Fifth Assessment Report of the Intergovernmental Panel on Climate Change. 2014. Geneva, https://ar5-syr.ipcc.ch/.
[3] IEA. System. Integration of Renewables. 2018.
[4] IEA. Digitalization & Energy. 2017.
[5] Bompard E, Huang T, Wu Y, Cremenescu M. Classification and trend analysis of threats origins to the security of power systems. Int J Electr Power Energy Syst 2013;50:50–64. https://doi.org/10.1016/j.ijepes.2013.02.008.
[6] Rübbelke D, Vögele S. Impacts of climate change on European critical infrastructures: the case of the power sector. Environ Sci Pol 2011;14:53–63. https://doi.org/10.1016/j.envsci.2010.10.007.
[7] Eder-Neuhauser P, Zseby T, Fabini J, Vormayr G. Cyber attack models for smart grid environments. Sustain Energy Grids Netw 2017;12:10–29. https://doi.org/10.1016/j.segan.2017.08.002.
[8] Langer L, Skopik F, Smith P, Kammerstetter M. From old to new: assessing cybersecurity risks for an evolving smart grid. Comput Secur 2016;62:165–76. https://doi.org/10.1016/j.cose.2016.07.008.
[9] Brooks M. Space weather: worse than hurricane Katrina. New Sci 2009;31–5. https://doi.org/10.1016/S0262-4079(09)60799-5.
[10] Chi Y, Xu Y. A state-of-the-art literature survey of power distribution system resilience assessment. IEEE Power Energy Soc Gen Meet PESGM 2018:1–5. 2018.
[11] Arghandeh R, Von Meier A, Mehrmanesh L, Mili L. On the definition of cyber-physical resilience in power systems. Renew Sustain Energy Rev 2016;58:1060–9. https://doi.org/10.1016/j.rser.2015.12.193.
[12] Sharifi A, Yamagata Y. Principles and criteria for assessing urban energy resilience: a literature review. Renew Sustain Energy Rev 2016;60:1654–77. https://doi.org/10.1016/j.rser.2016.03.028.
[13] Roege PE, Collier ZA, Mancillas J, McDonagh JA, Linkov I. Metrics for energy resilience. Energy Pol 2014;72:249–56. https://doi.org/10.1016/j.enpol.2014.04.012.
[14] Chandramowli SN, Felder FA. Impact of climate change on electricity systems and markets - a review of models and forecasts. Sustain Energy Technol Assess 2014;5:62–74. https://doi.org/10.1016/j.seta.2013.11.003.
[15] Pryor SC, Barthelmie RJ. Climate change impacts on wind energy: a review. Renew Sustain Energy Rev 2010;14:430–7. https://doi.org/10.1016/j.rser.2009.07.028.
[16] Wang Y, Chen C, Wang J, Rb-ITransP Syst. U. Research on resilience of power systems under natural disasters—a review. IEEE Trans Power Syst 2016;31:1604–13. 2016.
[17] Panteli M, Mancarella P. The grid: stronger, bigger, smarter? IEEE Power Energy Mag 2015;58–66. https://doi.org/10.1109/MPE.2015.2397334.
[18] Jufri FH, Kim JS, Jung J. Analysis of determinants of the impact and the grid capability to evaluate and improve grid resilience from extreme weather event. Energies 2017;10. https://doi.org/10.3390/en10111779.
[19] Cadini F, Agliardi GL, Zio E. A modeling and simulation framework for the reliability/availability assessment of a power transmission grid subject to cascading failures under extreme weather conditions. Appl Energy 2017;185:267–79. https://doi.org/10.1016/j.apenergy.2016.10.086.
[20] Panteli M, Mancarella P, Trakas DN, Kyriakides E, Hatziargyriou ND. Metrics and quantification of operational and infrastructure resilience in power systems. IEEE Trans Power Syst 2017;32:4732–42. https://doi.org/10.1109/TPWRS.2017.2664141.
[21] Hdidouan D, Staffell I. The impact of climate change on the levelised cost of wind energy. Renew Energy 2017;101:575–92. https://doi.org/10.1016/j.renene.2016.09.003.
[22] Koletsis I, Kotroni V, Lagouvardos K, Soukissian T. Assessment of offshore wind speed and power potential over the Mediterranean and the Black Seas under future climate changes. Renew Sustain Energy Rev 2016;60:234–45. https://doi.org/10.1016/j.rser.2016.01.080.
[23] Hernandez-Fajardo I, Dueñas-Osorio L. Probabilistic study of cascading failures in complex interdependent lifeline systems. Reliab Eng Syst Saf 2013;111:260–72. https://doi.org/10.1016/j.ress.2012.10.012.
[24] Zeng X, Liu Z, Hui Q. Energy equipartition stabilization and cascading resilience optimization for geospatially distributed cyber-physical network systems. IEEE Trans Syst Man Cybern Syst 2014;45:25–43. https://doi.org/10.1109/TSMC.2014.2320877.
[25] Leszczyna R. A review of standards with cybersecurity requirements for smart grid. Comput Secur 2018;77:262–76. https://doi.org/10.1016/j.cose.2018.03.011.
[26] Aloul F, Al-Ali AR, Al-Dalky R, Al-Mardini M, El-Hajj W. Smart grid security: threats, vulnerabilities and solutions. Int J Smart Grid Clean Energy 2012;1–6. https://doi.org/10.12720/sgce.1.1.1-6.
[27] Liu X, Li Z. False data attack models, impact analyses and defense strategies in the electricity grid. Electr J 2017;30:35–42. https://doi.org/10.1016/j.tej.2017.04.001.
[28] Sun CC, Hahn A, Liu CC. Cyber security of a power grid: state-of-the-art. Int J Electr Power Energy Syst 2018;99:45–56. https://doi.org/10.1016/j.ijepes.2017.12.020.
[29] Wang W, Lu Z. Cyber-security in smart grid: survey and challenges. Comput Electr Eng 2018;67:469–82. https://doi.org/10.1016/j.compeleceng.2018.01.015.
[30] Wilson JD. A securitisation approach to international energy politics. Energy Res Soc Sci 2019;49:114–25. https://doi.org/10.1016/j.erss.2018.10.024.
[31] Smith Stegen K. Deconstructing the “energy weapon”: Russia’s threat to Europe as case study. Energy Pol 2011;39:6505–13. https://doi.org/10.1016/j.enpol.2011.07.051.
[32] Rose A, Wei D, Paul D. Economic consequences of and resilience to a disruption of petroleum trade: the role of seaports in U.S. energy security. Energy Pol 2018;115:584–615. https://doi.org/10.1016/j.enpol.2017.12.052.
[33] Tchórzewska-Cieslak B, Pietrucha-Urbanik K. Approaches to methods of risk analysis and assessment regarding the gas supply to a city. Energies 2018. https://doi.org/10.3390/en11123304.
[34] Global IEA. Gas Security Review 2017. How is LNG Market Flexibility Evolving?. 2017.
[35] Azzuni A, Breyer C. Definitions and dimensions of energy security: a literature review7. Wiley Interdiscip Rev Energy Environ; 2018. p. 1–34. https://doi.org/10.1002/wene.268.
[36] Ang BW, Choong WL, Ng TS. Energy security: definitions, dimensions and indexes. Renew Sustain Energy Rev 2015;42:1077–93. https://doi.org/10.1016/j.rser.2014.10.064.
[37] Winzer C. Conceptualizing energy security. Energy Pol 2012;46:36–48. https://doi.org/10.1016/j.enpol.2012.02.067.
[38] Cherp A, Jewell J. The concept of energy security: beyond the four as. Energy Pol 2014;75:415–21. https://doi.org/10.1016/j.enpol.2014.09.005.
[39] Cherp A, Jewell J. The three perspectives on energy security: intellectual history, disciplinary roots and the potential for integration. Curr Opin Environ Sustain 2011;3:202–12. https://doi.org/10.1016/j.cosust.2011.07.001.
[40] Molyneaux L, Brown C, Wagner L, Foster J. Measuring resilience in energy systems: insights from a range of disciplines. Renew Sustain Energy Rev 2016;59:1068–79. https://doi.org/10.1016/j.rser.2016.01.063.
[41] Vivoda V. Evaluating energy security in the Asia-Pacific region: a novel methodological approach. Energy Pol 2010;38:5258–63. https://doi.org/10.1016/j.enpol.2010.05.028.
[42] Sovacool BK. Evaluating energy security in the Asia pacific: towards a more comprehensive approach. Energy Pol 2011;39:7472–9. https://doi.org/10.1016/j.enpol.2010.10.008.
[43] Cherp A. Defining energy security takes more than asking around. Energy Pol 2012;48:841–2. https://doi.org/10.1016/j.enpol.2012.02.016.
[44] Erker S, Stangl R, Stoeglehner G. Resilience in the light of energy crises – Part I: a framework to conceptualise regional energy resilience. J Clean Prod 2017;164:420–33. https://doi.org/10.1016/j.jclepro.2017.06.163.

[45] Hamilton MC, Lambert JH, Connelly EB, Barker K. Resilience analytics with disruption of preferences and lifecycle cost analysis for energy microgrids. Reliab Eng Syst Saf 2016;150:11–21. https://doi.org/10.1016/j.ress.2016.01.005.
[46] OECD/IEA. Making the energy sector more resilient to climate change. 2015.
[47] Martišauskas L, Augutis J, Krikštolaitis R. Methodology for energy security assessment considering energy system resilience to disruptions. Energy Strategy Rev 2018;22:106–18. https://doi.org/10.1016/j.esr.2018.08.007.
[48] Jewell J, Cherp A, Riahi K. Energy security under de-carbonization scenarios: an assessment framework and evaluation under different technology and policy choices. Energy Pol 2014;65:743–60. https://doi.org/10.1016/j.enpol.2013.10.051.
[49] Kruyt B, van Vuuren DP, de Vries HJM, Groenenberg H. Indicators for energy security. Energy Pol 2009;37:2166–81. https://doi.org/10.1016/j.enpol.2009.02.006.
[50] Månsson A, Johansson B, Nilsson LJ. Assessing energy security: an overview of commonly used methodologies. Energy 2014;73:1–14. https://doi.org/10.1016/j.energy.2014.06.073.
[51] Hosseini S, Barker K, Ramirez-Marquez JE. A review of definitions and measures of system resilience. Reliab Eng Syst Saf 2016;145:47–61. https://doi.org/10.1016/j.ress.2015.08.006.
[52] Jesse B-J, Heinrichs HU, Kuckshinrichs W. Adapting the theory of resilience to energy systems: a review and outlook. Energy Sustain Soc 2019;9:27. https://doi.org/10.1186/s13705-019-0210-7.
[53] IEA. Energy security. 2019. https://www.iea.org/topics/energysecurity/. [Accessed 24 April 2019].
[54] Chester L. Conceptualising energy security and making explicit its polysemic nature. Energy Pol 2010;38:887–95. https://doi.org/10.1016/j.enpol.2009.10.039.
[55] Löschel A, Moslener U, Rübbelke DTG. Indicators of energy security in industrialised countries. Energy Pol 2010;38:1665–71. https://doi.org/10.1016/j.enpol.2009.03.061.
[56] Johansson B. Security aspects of future renewable energy systems-A short overview. Energy 2013;61:598–605. https://doi.org/10.1016/j.energy.2013.09.023.
[57] Gracceva F, Zeniewski P. A systemic approach to assessing energy security in a low-carbon EU energy system. Appl Energy 2014;123:335–48. https://doi.org/10.1016/j.apenergy.2013.12.018.
[58] PMM. Managing the risks of extreme events and disasters to advance climate change adaptation. In: Field CB, Barros V, Stocker TF, Qin D, Dokken DJ, Ebi KL, Mastrandrea MD, Mach KJ, Plattner G-K, Allen SK, Tignor M, editors. A Special Report of Working Groups I and II of the Intergovernmental Panel on Climate Change; 2012. https://doi.org/10.1596/978-0-8213-8845-7. https://www.ipcc.ch/report/managing-the-risks-of-extreme-events-and-disasters-to-advance-climate-change-adaptation.
[59] Panteli M, Trakas DN, Mancarella P, Hatziargyriou ND. Boosting the power grid resilience to extreme weather events using defensive islanding. IEEE Trans Smart Grid 2016;7:2913–22. https://doi.org/10.1109/TSG.2016.2535228.
[60] Henry D, Emmanuel Ramirez-Marquez J. Generic metrics and quantitative approaches for system resilience as a function of time. Reliab Eng Syst Saf 2012;99:114–22. https://doi.org/10.1016/j.ress.2011.09.002.
[61] Moslehi S, Reddy TA. Sustainability of integrated energy systems: a performance-based resilience assessment methodology. Appl Energy 2018;228:487–98. https://doi.org/10.1016/j.apenergy.2018.06.075.
[62] Panteli M. Modeling and evaluating the resilience of critical electrical power infrastructure to extreme weather events. IEEE Syst J 2015;11:1733–42. https://doi.org/10.1109/JSYST.2015.2389272.
[63] Erker S, Stangl R, Stoeglehner G. Resilience in the light of energy crises – Part II: application of the regional energy resilience assessment. J Clean Prod 2017;164:495–507. https://doi.org/10.1016/j.jclepro.2017.06.162.
[64] Jansen JC, Arkel WG Van, Boots MG. Designing indicators of long-term energy supply security, vol. 35; 2004. https://doi.org/10.1007/s12649-013-9223-1. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.197.4269.
[65] Kloppenburg S, Boekelo M. Digital platforms and the future of energy provisioning: promises and perils for the next phase of the energy transition. Energy Res Soc Sci 2019;49:68–73. https://doi.org/10.1016/j.erss.2018.10.016.
[66] Amirioun MH, Aminifar F, Lesani H, Shahidehpour M. Metrics and quantitative framework for assessing microgrid resilience against windstorms. Int J Electr Power Energy Syst 2019;104:716–23. https://doi.org/10.1016/j.ijepes.2018.07.025.
[67] Bie Z, Lin Y, Li G, Li F. Battling the extreme: a study on the power system resilience. Proc IEEE 2017;105:1253–66. https://doi.org/10.1109/JPROC.2017.2679040.
[68] Salman A. Risk-based Assessment and Strengthening of Electric Power Systems Subject to Natural Hazards. Thesis for Doctor of Philosophy in Civil Engineering. Michigan Technological University; 2016. https://doi.org/10.37099/mtu.dc.etdr/207.
[69] Dunn S, Wilkinson S, Alderson D, Fowler H, Galasso C. Fragility curves for assessing the resilience of electricity networks constructed from an extensive fault database. Nat Hazards Rev 2018;19:04017019. https://doi.org/10.1061/(ASCE)NH.1527-6996.0000267.
[70] Wilkinson S, Maticka MJ, Liu Y, John M. The duck curve in a drying pond: the impact of rooftop PV on the Western Australian electricity market transition. Util Pol 2021;71:101232. https://doi.org/10.1016/j.jup.2021.101232.
[71] Valdés J. Arbitrariness in multidimensional energy security indicators. Ecol Econ 2018;145:263–73. https://doi.org/10.1016/j.ecolecon.2017.09.002.
[72] Wang J, Zuo W, Rhode-Barbarigos L, Lu X, Wang J, Lin Y. Literature review on modeling and simulation of energy infrastructures from a resilience perspective. Reliab Eng Syst Saf 2019;183:360–73. https://doi.org/10.1016/j.ress.2018.11.029.
[73] Panteli M, Mancarella P. Influence of extreme weather and climate change on the resilience of power systems: impacts and possible mitigation strategies. Elec Power Syst Res 2015;127:259–70. https://doi.org/10.1016/j.epsr.2015.06.012.
[74] Zhai C, Chen TY, White AG, Guikema SD. Power outage prediction for natural hazards using synthetic power distribution systems. Reliab Eng Syst Saf 2021;208:107348. https://doi.org/10.1016/j.ress.2020.107348.
[75] Ji C, Wei Y, Poor V. Resilience of Energy Infrastructure and Services: Modeling, Data Analytics, and Metrics. Data Anal n.d.;105:1354–1366. https://doi.org/10.1109/JPROC.2017.2698262.
[76] Fu G, Wilkinson S, Dawson RJ, Fowler HJ, Kilsby C, Panteli M, et al. Integrated approach to assess the resilience of future electricity infrastructure networks to climate hazards. IEEE Syst J 2018;12:3169–80. https://doi.org/10.1109/JSYST.2017.2700791.
[77] Panteli M, Pickering C, Wilkinson S, Dawson R, Mancarella P. Power system resilience to extreme weather: fragility modeling, probabilistic impact assessment, and adaptation measures. IEEE Trans Power Syst 2017;32:3747–57. https://doi.org/10.1109/TPWRS.2016.2641463.
[78] Espinoza S, Panteli M, Mancarella P, Rudnick H. Multi-phase assessment and adaptation of power systems resilience to natural hazards. Elec Power Syst Res 2016;136:352–61. https://doi.org/10.1016/j.epsr.2016.03.019.
[79] Watson J, Ketsopoulou I, Dodds P, Chaudry M, Tindemans S, Woolf M, et al. The Security of UK Energy Futures. UK Energy Research Center; 2018.
[80] Månsson A, Johansson B, Nilsson LJ. Methodologies for characterising and valuing energy security - a short critical review. 9th Int. Conf. Eur. Energy Mark. EEM 2012;12:1–8. https://doi.org/10.1109/EEM.2012.6254752. IEEE.
[81] World Health Organization. How air pollution is destroying our health. 2018. https://www.who.int/air-pollution/news-and-events/how-air-pollution-is-destroying-our-health. [Accessed 30 May 2019].
[82] Hines P, Apt J, Talukdar S. Large blackouts in North America: historical trends and policy implications. Energy Pol 2009;37:5249–59. https://doi.org/10.1016/j.enpol.2009.07.049.
[83] Cherp A, Adenikinju A, Goldthau A, Hernandez F, Hughes L, Jansen J, et al. Energy and security. Glob. Energy Assess. International Institute for Applied Systems Analysis; 2014.
[84] Strunz S. The German energy transition as a regime shift. Ecol Econ 2014;100:150–8. https://doi.org/10.1016/j.ecolecon.2014.01.019.
[85] Azzuni A, Breyer C. Energy security and energy storage technologies. Energy Procedia 2018;155:237–58. https://doi.org/10.1016/J.EGYPRO.2018.11.053.
[86] IEA. Re-powering Markets: Market Design and Regulation during the transition to low carbon power systems. 2016. https://doi.org/10.1787/9789264209596-en.
[87] Sircar I, Sage D, Goodier C, Fussey P, Dainty A. Constructing Resilient Futures: integrating UK multi-stakeholder transport and energy resilience for 2050. Futures 2013;49:49–63. https://doi.org/10.1016/j.futures.2013.04.003.
[88] Proskuryakova L. Updating energy security and environmental policy: energy security theories revisited. J Environ Manag 2018;223:203–14. https://doi.org/10.1016/j.jenvman.2018.06.016.
[89] Roques F, Finon D. Adapting electricity markets to decarbonisation and security of supply objectives: toward a hybrid regime? Energy Pol 2017;105:584–96. https://doi.org/10.1016/j.enpol.2017.02.035.
[90] IRENA. A New World. The Geopolitics of the Energy Transformation. 2019.
[91] López Prol J. Regulation, profitability and diffusion of photovoltaic grid-connected systems: a comparative analysis of Germany and Spain. Renew Sustain Energy Rev 2018;91:1170–81. https://doi.org/10.1016/j.rser.2018.04.030.
[92] IEA. Technology. Innovation to Accelerate Energy Transitions. 2019.
[93] Salo A. Why there are so many scenarios? In Scientific Conference Preparing for the future: analyzing and identifying responses to societal challenges using scenarios and other tools for future scanning. Helsinki. 2020.
[94] Heuberger CF, Mac Dowell N. Real-World challenges with a rapid transition to 100% renewable power systems. Joule 2018;2:367–70. https://doi.org/10.1016/j.joule.2018.02.002.
[95] Clack CTM, Qvist SA, Apt J, Bazilian M, Brandt AR, Caldeira K, et al. Evaluation of a proposal for reliable low-cost grid power with 100% wind, water, and solar. Proc Natl Acad Sci Unit States Am 2017;114:6722–7. https://doi.org/10.1073/pnas.1610381114.
[96] Petitet M, Finon D, Janssen T. Capacity adequacy in power markets facing energy transition: a comparison of scarcity pricing and capacity mechanism. Energy Pol 2017;103:30–46. https://doi.org/10.1016/j.enpol.2016.12.032.
[97] 2 Degree Investing Initiative. All Swans are Black in the Dark. 2017.
[98] Severe power cuts in Texas highlight energy security risks related to extreme weather events – Analysis. IEA; 2021. https://www.iea.org/commentaries/severe-power-cuts-in-texas-highlight-energy-security-risks-related-to-extreme-weather-events. [Accessed 25 May 2021].
[99] The two hours that nearly destroyed Texas's electric grid. Bloomberg 2021. https://www.bloombergquint.com/technology/texas-blackout-how-the-electrical-grid-failed. [Accessed 25 May 2021].
[100] Puleo M. Damages from Feb. winter storms could be as high as $155 billion. AccuWeather 2021. https://www.accuweather.com/en/winter-weather/damages-from-feb-snowstorms-could-be-as-high-as-155b/909620.
[101] Weare C. The California electricity crisis: causes and policy options. Public Policy Institute of California; 2004.

[102] Kim KN, Yim MS, Schneider E. A study of insider threat in nuclear security analysis using game theoretic modeling. Ann Nucl Energy 2017;108:301–9. https://doi.org/10.1016/j.anucene.2017.05.006.
[103] Pan T, Mishra S, Nguyen LN, Lee G, Kang J, Seo J, et al. Threat from being social: vulnerability analysis of social network coupled smart grid. IEEE Access 2017;5:16774–83. https://doi.org/10.1109/ACCESS.2017.2738565.
[104] Gaede J, Rowlands IH. Visualizing social acceptance research: a bibliometric review of the social acceptance literature for energy technology and fuels. Energy Res Soc Sci 2018;40:142–58. https://doi.org/10.1016/j.erss.2017.12.006.
[105] Forssén K. Resilience of Finnish electricity distribution networks against extreme weather conditions. MSc thesis. Aalto University; 2016.
[106] Johansson J, Hassel H, Zio E. Reliability and vulnerability analyses of critical infrastructures: comparing two approaches in the context of power systems. Reliab Eng Syst Saf 2013;120:27–38. https://doi.org/10.1016/j.ress.2013.02.027.
[107] Rinaldi SM, Peerenboom JP, Kelly TK. Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Contr Syst Mag 2001;21:11–25. https://doi.org/10.1109/37.969131.
[108] Grubler A, Johansson T B, Mundaca L, Nakicenovic N, Pachauri S, Riahi K, et al. Energy Primer. Glob. Energy Assess. International Institute for Applied Systems Analysis; 2014.
[109] Gas IEA. Analysis and forecasts to 2024 2019. 2019. https://www.iea.org/gas2019/. [Accessed 10 July 2019].
[110] Resources to reserves 2013: oil, gas and coal technologies for the energy markets of the future. Paris: IEA; 2013.
[111] Lovering JR, Yip A, Nordhaus T. Historical construction costs of global nuclear power reactors. Energy Pol 2016;91:371–82. https://doi.org/10.1016/j.enpol.2016.01.011.
[112] IAEA. The Fukushima daiichi accident. 2015. Report by the Director General.
[113] Chu S, Richter B, Cavanagh R, Kammen D. Webcast Debate: "The World Needs a Nuclear Renaissance". 2016. https://www.youtube.com/watch?v=uuJodGvyLzM. [Accessed 21 August 2019].
[114] IEA. Status of Power System Transformation: Advanced Power Plant Flexibility. 2018. https://doi.org/10.1787/9789264278820-en.
[115] Hoggett R. Technology scale and supply chains in a secure, affordable and low carbon energy transition. Appl Energy 2014;123:296–306. https://doi.org/10.1016/j.apenergy.2013.12.006.
[116] Offshore Wind Outlook 2019. IEA; 2019.
[117] Overland I. The geopolitics of renewable energy: debunking four emerging myths. Energy Res Soc Sci 2019;49:36–40. https://doi.org/10.1016/j.erss.2018.10.018.
[118] Jaramillo Thomas. Producing renewable fuels and chemicals from CO2 and H2O. Stanf Energy Channel Youtube 2015. https://www.youtube.com/watch?v=O0aCP5OSqG4&t=83s. [Accessed 25 May 2021].
[119] Special Focus on Gas Infrastructure. IEA; 2019.
[120] Getting Wind and Sun onto the Grid. IEA; 2017.
[121] History. From Oil Security to Steering the World Toward Secure and Sustainable Energy Transitions. IEA; 2021. https://www.iea.org/about/history. [Accessed 27 May 2021].
[122] Bouwmeester MC, Oosterhaven J. Economic impacts of natural gas flow disruptions between Russia and the EU. Energy Pol 2017;106:288–97. https://doi.org/10.1016/j.enpol.2017.03.030.
[123] Landinger H, Bunger U, Raksha T, Weindorf W, Simon J, Correas L, et al. Update of Benchmarking of large scale hydrogen underground storage with competing options. 2014.
[124] Natural gas supply statistics n.d. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Natural_gas_supply_statistics. [Accessed 27 May 2021].
[125] Electricity dependence in modern society. In: Finnish: Sahkoriippuvuus modernissa yhteiskunnassa). Security Committee (in Finnish: Turvallisuuskomitea; 2015.
[126] World Energy Outlook 2019. IEA; 2019.
[127] Electrical Energy Storage. White Paper. International Electrotechnical Commission; 2011.
[128] Technology Roadmap Energy storage. IEA; 2014.
[129] Jääskeläinen JJ. An interdisciplinary assessment of energy security risks in the Finnish energy market. PhD thesis. Aalto University; 2019.
[130] Pereira de Lucena AF, Szklo AS, Schaeffer R, Dutra RM. The vulnerability of wind power to climate change in Brazil. Renew Energy 2010;35:904–12. https://doi.org/10.1016/j.renene.2009.10.022.
[131] Bonjean Stanton MC, Dessai S, Paavola J. A systematic review of the impacts of climate variability and change on electricity systems in Europe. Energy 2016;109:1148–59. https://doi.org/10.1016/j.energy.2016.05.015.
[132] Ciscar JC, Dowling P. Integrated assessment of climate impacts and adaptation in the energy sector. Energy Econ 2014;46:531–8. https://doi.org/10.1016/j.eneco.2014.07.003.
[133] Gerlak AK, Weston J, McMahan B, Murray RL, Mills-Novoa M. Climate risk management and the electricity sector. Clim Risk Manag 2018;19:12–22. https://doi.org/10.1016/j.crm.2017.12.003.
[134] Ma S, Chen B, Wang Z. Resilience enhancement strategy for distribution systems under extreme weather events. IEEE Trans Smart Grid 2018;9:1442–51. https://doi.org/10.1109/TSG.2016.2591885.
[135] Salman AM, Li Y, Stewart MG. Evaluating system reliability and targeted hardening strategies of power distribution systems subjected to hurricanes. Reliab Eng Syst Saf 2015;144:319–33. https://doi.org/10.1016/j.ress.2015.07.028.
[136] Panteli M, Trakas DN, Mancarella P, Hatziargyriou ND. Power systems resilience assessment: hardening and smart operational enhancement strategies. Proc IEEE 2017;105:1202–13. https://doi.org/10.1109/JPROC.2017.2691357.
[137] Kwasinski A. Quantitative model and metrics of electrical grids' resilience evaluated at a power distribution level. Energies 2016;9:1–27. https://doi.org/10.3390/en9020093.
[138] Chandramowli S, Felder FF. Climate change and power systems planning-opportunities and challenges. Electr J 2014;27:40–50. https://doi.org/10.1016/j.tej.2014.04.002.
[139] Dowling P. The impact of climate change on the European energy system. Energy Pol 2013;60:406–17. https://doi.org/10.1016/j.enpol.2013.05.093.
[140] DOE US. U.S. Energy Sector Vulnerabilities to Climate Change and Extreme Weather. 2013.
[141] Nierop SCA. Envisioning resilient electrical infrastructure: a policy framework for incorporating future climate change into electricity sector planning. Environ Sci Pol 2014;40:78–84. https://doi.org/10.1016/j.envsci.2014.04.011.
[142] Dirks JA, Gorrissen WJ, Hathaway JH, Skorski DC, Scott MJ, Pulsipher TC, et al. Impacts of climate change on energy consumption and peak demand in buildings: a detailed regional approach. Energy 2015;79:20–32. https://doi.org/10.1016/j.energy.2014.08.081.
[143] IEA. Electricity statistics. 2019. https://www.iea.org/statistics/electricity/;
2019. [Accessed 25 July 2019].
[144] Kurz James. SolarPower Webinar "PV Cleaning: Choosing the Optimal Method and Frequency". 2017. http://www.solarpowereurope.org/wp-content/uploads/2018/07/SolarPower_Europe_Apricum.pdf. [Accessed 10 July 2019].
[145] Johnson DL, Erhardt RJ. Projected impacts of climate change on wind energy density in the United States. Renew Energy 2016;85:66–73. https://doi.org/10.1016/j.renene.2015.06.005.
[146] Ease EERA. European Energy Storage Technology Development Roadmap Towards 2030. 2017.
[147] Economist. China has built the world's largest water-diversion project. 2018. https://www.economist.com/china/2018/04/05/china-has-built-the-worlds-largest-water-diversion-project. [Accessed 10 July 2019].
[148] Davy R, Gnatiuk N, Pettersson L, Bobylev L. Climate change impacts on wind energy potential in the European domain with a focus on the Black Sea. Renew Sustain Energy Rev 2018;81:1652–9. https://doi.org/10.1016/j.rser.2017.05.253.
[149] Keith D. Solar geoengineering to manage climate. Stanf Energy Channel Youtube 2011. https://www.youtube.com/watch?v=zt5yR9dYV64&t=2785s. [Accessed 8 June 2021].
[150] Keith D. Moderate, temporary, and responsive solar geoengineering. Stanf Energy 2019. https://energy.stanford.edu/events/energy-seminar-david-keith. [Accessed 8 June 2021].
[151] Daglis IA. Space Storms and Space Weather Hazards. National Observatory of Athens Metaxa; 2001.
[152] Schrijver CJ, Kauristie K, Aylward AD, Denardini CM, Gibson SE, Glover A, et al. Understanding space weather to shield society: a global road map for 2015–2025 commissioned by COSPAR and ILWS. Adv Space Res 2015;55:2745–807. https://doi.org/10.1016/J.ASR.2015.03.023.
[153] Cooper C, Sovacool BK. Not your father's Y2K: preparing the north American power grid for the perfect solar storm. Electr J 2011;24:47–61. https://doi.org/10.1016/J.TEJ.2011.04.005.
[154] Fry EK. The risks and impacts of space weather: policy recommendations and initiatives. Space Pol 2012;28:180–4. https://doi.org/10.1016/J.SPACEPOL.2012.06.005.
[155] Homeier N, Wei L. Solar Storm Risk to the North American Electric Grid. Lloyd's; 2013.
[156] Pulkkinen A, Kataoka R, Watari S, Ichiki M. Modeling geomagnetically induced currents in Hokkaido, Japan. Adv Space Res 2010;46:1087–93. https://doi.org/10.1016/J.ASR.2010.05.024.
[157] Boteler DH. Dealing With Space Weather: The Canadian Experience. Extreme Events Geosp. Elsevier; 2018. p. 635–56. https://doi.org/10.1016/B978-0-12-812700-1.00026-1.
[158] Ramírez-Niño J, Haro-Hernández C, Rodriguez-Rodriguez JH, Mijarez R. Core saturation effects of geomagnetic induced currents in power transformers. J Appl Res Technol 2016. https://doi.org/10.1016/j.jart.2016.04.003.
[159] Molinski TS. Why utilities respect geomagnetically induced currents. J Atmospheric Sol-Terr Phys 2002;64:1765–78. https://doi.org/10.1016/S1364-6826(02)00126-8.
[160] Talib M, Mogotlhwane TM. Global failure of ict due to solar storm: a worst case scenario ahead. Procedia Environ Sci 2011;8:371–4. https://doi.org/10.1016/J.PROENV.2011.10.058.
[161] Hapgood M. Space Weather: What are Policymakers Seeking? Extreme Events Geosp. Orig. Predict. Consequences. Elsevier; 2018. p. 657–82. https://doi.org/10.1016/B978-0-12-812700-1.00027-3.
[162] Lassen B. Is livestock production prepared for an electrically paralysed world? J Sci Food Agric 2013;93:2–4. https://doi.org/10.1002/jsfa.5939.
[163] Thomson AWP, Gaunt CT, Cilliers P, Wild JA, Opperman B, McKinnell L-A, et al. Present day challenges in understanding the geomagnetic hazard to national power grids. Adv Space Res 2010;45:1182–90. https://doi.org/10.1016/J.ASR.2009.11.023.
[164] Johnson M, Gorospe G, Landry J, Schuster A. Review of mitigation technologies for terrestrial power grids against space weather effects. Int J Electr Power Energy Syst 2016;82:382–91. https://doi.org/10.1016/J.IJEPES.2016.02.049.
[165] Lewandowski K. Protection of the smart city against CME. Transp Res Procedia 2016;16:298–312. https://doi.org/10.1016/J.TRPRO.2016.11.029.
[166] Hansen A, Staggs J, Shenoi S. Security analysis of an advanced metering infrastructure. Int J Crit Infrastruct Prot 2017;18:3–19. https://doi.org/10.1016/j.ijcip.2017.03.004.

[167] Leszczyna R. Cybersecurity and privacy in standards for smart grids – a comprehensive survey. Comput Stand Interfac 2018;56:62–73. https://doi.org/10.1016/j.csi.2017.09.005.
[168] Jiang R, Lu R, Wang Y, Luo J, Shen C, Shen X. Energy-theft detection issues for advanced metering infrastructure in smart grid. Tsinghua Sci Technol 2014;19:105–20. https://doi.org/10.1109/TST.2014.6787363.
[169] Rice EB, AlMajali A. Mitigating the risk of cyber attack on smart grid systems. Procedia Comput Sci 2014;28:575–82. https://doi.org/10.1016/j.procs.2014.03.070.
[170] Xiang Y, Wang L, Liu N. Coordinated attacks on electric power systems in a cyber-physical environment. Elec Power Syst Res 2017;149:156–68. https://doi.org/10.1016/j.epsr.2017.04.023.
[171] Zacchia Lun Y, D'Innocenzo A, Smarra F, Malavolta I, Di Benedetto MD. State of the art of cyber-physical systems security: an automatic control perspective. J Syst Software 2019;149:174–216. https://doi.org/10.1016/j.jss.2018.12.006.
[172] Liu J, Xiao Y, Li S, Liang W, Chen CLP. Cyber security and privacy issues in smart grids. IEEE Commun Surv Tutor 2012;14:981–97. https://doi.org/10.1109/SURV.2011.122111.00145.
[173] Anwar A, Mahmood AN, Tari Z. Identification of vulnerable node clusters against false data injection attack in an AMI based Smart Grid. Inf Syst 2015;53:201–12. https://doi.org/10.1016/j.is.2014.12.001.
[174] Staggs J, Ferlemann D, Shenoi S. Wind farm security: attack surface, targets, scenarios and mitigation. Int J Crit Infrastruct Prot 2017;17:3–14. https://doi.org/10.1016/j.ijcip.2017.03.001.
[175] Guidelines for smart grid cyber security. National Institute of Standards and Technology; 2010.
[176] Ashibani Y, Mahmoud QH. Cyber physical systems security: analysis, challenges and solutions. Comput Secur 2017;68:81–97. https://doi.org/10.1016/j.cose.2017.04.005.
[177] Hagen J. Building resilience against cyber threats in the energy sector. Int J Crit Infrastruct Prot 2018;20:26–7. https://doi.org/10.1016/j.ijcip.2017.11.003.
[178] Pearson ILG. Smart grid cyber security for Europe. Energy Pol 2011;39:5211–8. https://doi.org/10.1016/j.enpol.2011.05.043.
[179] Mcdaniel P, Smith SW. Security and privacy challenges in the smart grid. Secure Syst 2009;72–4.
[180] Ananda Kumar V, Pandey KK, Punia DK. Cyber security threats in the power sector: need for a domain specific regulatory framework in India. Energy Pol 2014;65:126–33. https://doi.org/10.1016/j.enpol.2013.10.025.
[181] Onyeji I, Bazilian M, Bronk C. Cyber security and critical energy infrastructure. Electr J 2014;27:52–60. https://doi.org/10.1016/j.tej.2014.01.011.
[182] Gorndon S, Goeckeler D, Hennessy J. Cybersecurity dialogue 2019. 2019. https://www.youtube.com/watch?v=J1t15Qs1NSA. [Accessed 3 July 2019].
[183] Wu SS, Liu CC, Shosha AF, Gladyshev P. Cyber security and information protection in a smart grid environment. 18th World Congr. Int. Fed. Autom. Control 2011;44:13696–704. https://doi.org/10.3182/20110828-6-IT-1002.02140. IFAC.
[184] Leszczyna R. Standards on cyber security assessment of smart grid. Int J Crit Infrastruct Prot 2018;22:70–89. https://doi.org/10.1016/j.ijcip.2018.05.006.
[185] Booth A, Dhingra A, Heiligtag S, Nayfeh M, Wallance D. Critical infrastructure companies and the global cybersecurity threat. McKinsey & Company; 2019.
[186] Electricity Information Sharing and Analysis Center(E-ISAC). Analysis of the Cyber Attack on the Ukrainian Power grid. 2016. https://doi.org/10.1159/000329982.
[187] Cimpanu C. US wants to isolate power grids with "retro" technology to limit cyber-attacks. 2019. https://www.zdnet.com/article/us-wants-to-isolate-power-grids-with-retro-technology-to-limit-cyber-attacks/. [Accessed 10 July 2019].