Internet of Things 11 (2020) 100204

Contents lists available at ScienceDirect

Internet of Things

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

Review article

Cyber resilience in firms, organizations and societies

Kjell Hausken

Faculty of Science and Technology, University of Stavanger, 4036 Stavanger, Norway

ARTICLE INFO

Article history:
Received 22 April 2020
Accepted 28 April 2020
Available online 17 May 2020

Keywords:
Cyber resilience
Recovery
Non-threat actors
Threat actors
Levels of organization
Insurance
Internet of things

ABSTRACT

Cyber resilience involves most societal actors, i.e. organizations, individuals, threat actors, governments, insurers, etc., at most levels of organization. Actors are embedded within each other and choose strategies based on beliefs and preferences which impact and is impacted by cyber resilience. The article reviews the literature, attempting to capture the core ingredients of cyber resilience. Non-threat actors seeking to obtain cyber resilience are distinguished from threat actors. Actors have resources, competence, technology, and tools. They make choices that impact the cyber resilience for all actors, including themselves. Cyber resilience relates to cyber insurance through entry requirements or preconditions for cyber contracts, need for various services such as incident response, data gathering, and cover limitations. Cyber resilience is linked to the internet of things which in the future can be expected to simplify life through artificial intelligence and machine learning, while being vulnerable through a large attack surface, insufficient technology, challenging handling of data, possible high trust in computers and software, and ethics.

1. Introduction

1.1. Background

Resilience has been analyzed extensively within risk analysis, especially related to physical infrastructures [4,9,13]. Knowledge within mature research fields gets more settled into practices, laws and regulations, the education of practitioners, etc. Cyber resilience currently experiences many developments.[1] Our knowledge about the factors associated with cyber resilience grows but needs to adapt to rapid changes. Enhancing our understanding of cyber resilience becomes imperative. A mapping of relevant factors is essential.

1.2. Contribution

The article reviews the state of the art of some of the enormous literature within cyber resilience, and intends to identify the core ingredients of cyber resilience to facilitate progress beyond the state of the art. Common definitions of cyber resilience are presented and further refined and clarified. Non-threat actors are distinguished from threat actors and hybrid

E-mail address: kjell.hausken@uis.no

[1] For example, CISA [7], within the US Department of Homeland Security, offers an assessment to evaluate an organization's operational resilience and cybersecurity practices.

https://doi.org/10.1016/j.iot.2020.100204

actors. Actors which may be threatening or not, levels, beliefs, and preferences relevant for cyber resilience are presented. Resources, competence, technology, tools, and strategies in cyber resilience are outlined. The relationship between cyber resilience and cyber insurance is sketched. The role of cyber resilience in the future is assessed. Future research possibilities are suggested.

1.3. Article organization

Section 2 reviews the literature. Section 3 defines cyber resilience, an actor, and cyberspace. Section 4 assesses resources, competence, technology, tools, and strategies in cyber resilience. Section 5 sketches the relationship between cyber resilience and cyber insurance. Section 6 outlines possible future developments. Section 7 sketches future research possibilities. Section 8 concludes.

2. Literature review

This review categorizes the literature into history and review, infrastructure, management, policy, economics, insurance, and the internet of things (IoT).

2.1. History and review of cyber resilience

Hult and Sivanesan [23] provide a historical context on how cyber security has evolved, and outline what good cyber resilience looks like. They suggest that relying on traditional protection and preventive controls are not enough, and recommend a more agile approach. Zemba et al. [56] review 74 literature measures or definitions of resilience, across the four phases prepare, absorb, recover, adapt. They evaluate the effectiveness of training or intervention into teams to increase resilience and performance. They argue that resilience in small groups can be increased by focusing on absorption and adaptation related to mission execution, in addition to the common focus on recovery. Kott and Linkov [30] review and assess the cyber resilience of systems and networks, distinguishing between security, risk and resilience. They describe current and possible future cyber resilience practices and techniques, accounting for technical issues.

2.2. Infrastructure

Herrington and Aldrich [22] identify complex state–private citizen partnerships involving intelligence, security and resilience due to national infrastructure being partly in private hands, while legislation and imposing legal duties for service providers to improve resilience are public. To avoid such risk shifting when systems fail, they identify analogue and manual systems as a solution, in addition to technical solutions, to obtain robust cyber defense. Wood, Wells, Rice, and Linkov [53] illustrate for large organizations how organizational strengths, weaknesses, synergies, and redundancies related to resilience can be identified through comparing quantitative indices across subcomponents, and mapping across event cycle phases and context-specific resilience domains. DiMase, Collier, Heffner, and Linkov [8] argue for a systems engineering integrated framework across the physical, information, cognitive, and social domains. The seek to integrate security into interdependent computing systems and adjacent systems architectures, to ensure cyber physical security and resilience, and continued functionality of critical services. Kaufmann [28] considers cyber resilience in the European Union.

2.3. Management

Linkov, Roslicky, and Trump [35] present multiple perspectives on the management of hybrid threats involving digital systems with implications for diverse fields such as medicine, social media, and homeland security. Various strategies are proposed for protection and recovery under different disruption scenarios, focusing on risk and resilience in the information domain. Linkov and Palma-Oliveira [34] advocate for a systems-driven view of resilience and risk related to the environment and cyber and other domains. To address emerging threats they propose resilience -based management in methodology and tools in infrastructure, cyber, and social domains. Flammini [14] considers paradigms and techniques for the transition from risk modeling to threat counteraction for the resilience of cyber-physical systems. Both exposure to new threats and cyber-physical systems' potential to counteract the threats through management and mitigation are considered.

2.4. Policy

Gisladottir, Ganin, Keisler, Kepner, and Linkov [16] consider resilience of cyber systems with over-regulation and under-regulation. They acknowledge the common approach of implementing new regulations against new threats to harden the system, which causes stress due to spending more time on training and policy implementation. Bostick, Connelly, Lambert, and Linkov [5] consider how risk-based policymaking and investment decisions impact resilience in damaged communities, and how economic motivations for resilience management play a role in large scale complex systems. Linkov et al. [33] observe that cyber attacks may cause damage disproportionate to the sophistication and cost of launching the attack. They identify and apply a variety of quantitative and qualitative measures from the literature to develop resilience metrics for

cyber systems across the physical, information, cognitive, and social domains. Their generic approach intends to integrate actual data, technical judgment, and literature-based measures. They link national policy goals to specific system measures, so that resource allocation translates into actionable interventions and investments. Harrop and Matteson [19] review critical national infrastructure and cyber security protection measures in the UK and USA. They assess the vicarious nature of well planned and executed cyber attacks, illustrated with well-known historical examples, and identify key steps in detection, deterrence, and disruption.

2.5. Economics

Incorporating economic factors and policy, Anderson, Bohme, Clayton, and Moore [2] assess 15 policy proposals and how information security should be coordinated among the members of the European Union. Moore [37] considers the economics of cyber security, accounting for misaligned incentives, information asymmetries, and externalities, which extend beyond technical approaches. For example, actors providing, regulating, and consuming cyber security have different costs and benefits. Regulatory options are suggested to overcome these challenges.

2.6. Insurance

Cyber security has been extensively analyzed related to insurance. Talesh [48] shows how insurance companies are compliance managers for businesses, proceeding beyond pooling and transferring risk. Schneier [45] claims that the computer security industry in the future will be run by the insurance industry. Woods and Simpson [55] present a framework for policy measures and cyber insurance which involves a public–private partnership between governments which may intervene and the insurance industry. Romanosky, Ablon, Kuehn, and Jones [44] conduct content analysis of cyber insurance policies and assess how carriers price cyber risk. Woods, Agrafiotis, Nurse, and Creese [54] analyze 24 insurance proposal forms to assess compliance with ISO/IEC 27,002:2013 [26] and the CIS Critical Security Controls Version 6.0. Adverse selection and whether incentives can cause disparity between insurance practice and information security best practice are assessed. Franke [15] interviews 15 insurance companies and intermediaries selling cyber insurance in Sweden, finding annual premiums at 0.5–1% of the indemnity limit, assessing avoidance and mitigation for immature customers, discrepancies between insurers, market segmentation, pricing, business continuity, and information asymmetry.

2.7. Internet of things (IoT), artificial intelligence, machine learning, and cloud computing

Jiang et al. [27] apply deep learning, such as convolutional neural networks and recurrent neural networks, to multichannel attack detection for information security. They generate classifiers based on training neural network, and introduce a voting algorithm to decide whether the input data is an attack or not. Almomani, Gupta, Wan, Altaher, and Manickam [1] present a neural fuzzy framework which applies hybrid learning and adapts the evolving connectionist system to detect dynamically online zero-day phishing e-mails. Stergiou, Psannis, Kim, and Gupta [46] review whether the integration of cloud computing and internet of things (IoT) is secure. They find that the cloud computing technology improves the function of the IoT. Gupta, Agrawal, and Wang [17] consider the principles, algorithms, applications, and perspectives in the management and engineering of computer security. Gupta, Agrawal, and Yamaguchi [18] identify research, perspectives, techniques, and best practices within cryptology and cyber threat prevention. Plageras, Psannis, Stergiou, Wang, and Gupta [40] assess the role of cloud computing, IoT and monitoring for collecting and managing sensors' data in a smart building, which may enable energy efficiency. Memos, Psannis, Ishibashi, Kim, and Gupta [36] present an algorithm for media-based surveillance which combines information and communication technology and IoT which may benefit users and companies of a so-called "smart city," in terms of users' privacy, media security, and sensor node memory requirements.

3. Defining cyber resilience, actor, and cyberspace

3.1. Cyber resilience

Kott and Linkov [30] provide multiple definitions and review of cyber resilience in their introductory chapter. One widely used definition of resilience by the National Academies of Science (NAS) is "the ability to prepare and plan for, absorb, recover from, and more successfully adapt to adverse events" ([30], p. 3). Summaries of further definitions are provided by Linkov et al. [35]. Zemba et al. [56] review how resilience is defined, measured and used in small teams. They identify a focus on recovery with limited attention given to absorption and adaptation. Linkov et al. [33] develop and organize resilience metrics for cyber systems that link national policy goals to specific system measures, to assess resilience across physical, information, cognitive, and social domains. Wood et al. [53] show how large organizations can map resilience across threat event cycle phases and context-specific domains to contextualized resilience metrics, with comparison of subcomponents. Bostick et al. [5] describe economic motivations for implementing resilience assessment and management in damaged communities, and call for examining risk-based policymaking and investment decisions. Kishor et al. [29] define resilience as the ability of a system, person, or organization to recover from, defy, or resist from any shock, insult, or disturbance. Our

Table 1
A non-threat actor's, a threat actor's, and a hybrid actor's attitude towards its own cyber resilience and other actors' cyber resilience.

Actor	Seeks to preserve its own cyber resilience	Seeks to preserve other actors' cyber resilience	May be indifferent about other actors' cyber resilience	Seeks to compromise one or several other actors' cyber resilience
Non-threat actor	Yes	Sometimes yes	Sometimes yes	No
Threat actor	Usually yes, except for suicide bombers, masochistic actors, etc	No	Yes or no	Yes
Hybrid actor	Yes	Sometimes yes	Sometimes yes	Sometimes yes

definition of cyber resilience builds on the definitions and work above by introducing an actor defined in Definition 2 in the next Section 3.2, and by restricting the scope to cyber incidents.

Definition 1. Cyber resilience is the ability of an actor to resist, respond and recover from cyber incidents to ensure the actor's operational continuity.

Moreover, as commonly defined in the literature, a cyber threat targets entities in cyberspace defined in Section 3.3, causing cyber incidents which are events that occur with certain probabilities, which express cyber risk for these events. Cyber resilience impacts the information the actor requires or the systems the actor uses to do business.

3.2. Actor

Definition 2. An actor is any individual or collective unit usually assumed to preserve its own cyber resilience. A non-threat actor is an actor seeking to obtain, or to be indifferent regarding, the cyber resilience of some other actor. A threat actor is an actor compromising the cyber resilience of some other actor. A hybrid actor is an actor seeking to obtain cyber resilience in some regards, and compromising cyber resilience in other regards.

Definition 2 uses the term "usually" since exceptions exist for threat actors, such as suicide bombers or masochistic actors which may compromise their own cyber resilience. An actor may be an individual, group, super group, organization, industry, sector, community, county, region, country, continent, world. Cyber resilience may be obtained or compromised at all these levels. Actors may be e.g. benevolent, self-interested, or altruistic. Examples of an actor are an individual, employee, citizen, entrepreneur, developer, consumer, producer, manufacturer, system integrator, cyber security provider, environmentalist, philanthropist, representative, elected official, stakeholder, organization, interest group, idealistic organization, non-profit organization, non-governmental organization, governmental organization, intergovernmental organization, international organization, governmental unit, government, country, union of countries, for-profit organization, firm, business, enterprise. These actors are non-threat actors to the extent that they seek to obtain cyber resilience.

Actors differ in their preferences for the resilience of other actors. For mutually exclusive actors, which thus are not embedded within each other, we may distinguish between how actors prefer cyber resilience for other actors. Idealistic actors are non-threat actors who prefer all actors to be cyber resilient to maximize social welfare. Some actors (e.g. countries) may prefer some other actors (e.g. allies) to be cyber resilient while being indifferent regarding the cyber resilience of some other actors (e.g. those that are not allies), and may prefer some actors not to be cyber resilient (e.g. enemies). Some actors (e.g. criminal organizations) may prefer those actors they prefer to attack or hack not to be cyber resilient.

Examples of a threat actor are a hacker, criminal, terrorist which seek to maximize some objective through compromising (e.g. through an attack) the cyber resilience of other actors. Examples of a hybrid actor may comprise most of the examples above given that the actor has a double objective. First, the hybrid actor seeks to obtain cyber resilience in some regards, i.e. preserving the cyber resilience of itself and its chosen allied actors. Second, the hybrid actor seeks to compromise, and may sometimes inadvertently compromise, the cyber resilience of some selected other actors. Examples are a firm seeking to gain competitive advantage by compromising the cyber resilience of other firms, an airline checking its own passengers and baggage, but not passengers and baggage transferring to other airlines [31], or a polluting firm maximizing profit by not installing purification systems, thus causing surrounding or interacting actors to become less cyber resilient. Table 1 summarizes the attitudes of a non-threat actor, a threat actor, and a hybrid actor towards its own cyber resilience and other actors' cyber resilience.

For actors embedded within each other, such as employees embedded within departments embedded within organizations, preferences regarding cyber resilience are usually at least minimally aligned. Otherwise the organization does not function optimally. Such actors may have different preferences regarding the importance, and the amount of resources, to be allocated to cyber resilience. Some organizations may have moles or spies undermining the cyber resilience of the organization from within.

An actor may have a variety of characteristics. Actors generally have different beliefs about the cyber world. Such beliefs may vary greatly. Some actors quickly absorb the relevant knowledge, competence, technology, and tools, while other actors lag behind in forming cyber-related beliefs. Actors such as non-profit organizations, for-profit organizations, and criminal organizations, vary greatly regarding their preferences. They may maximize profit, cyber resilience, some idealistic cause, or

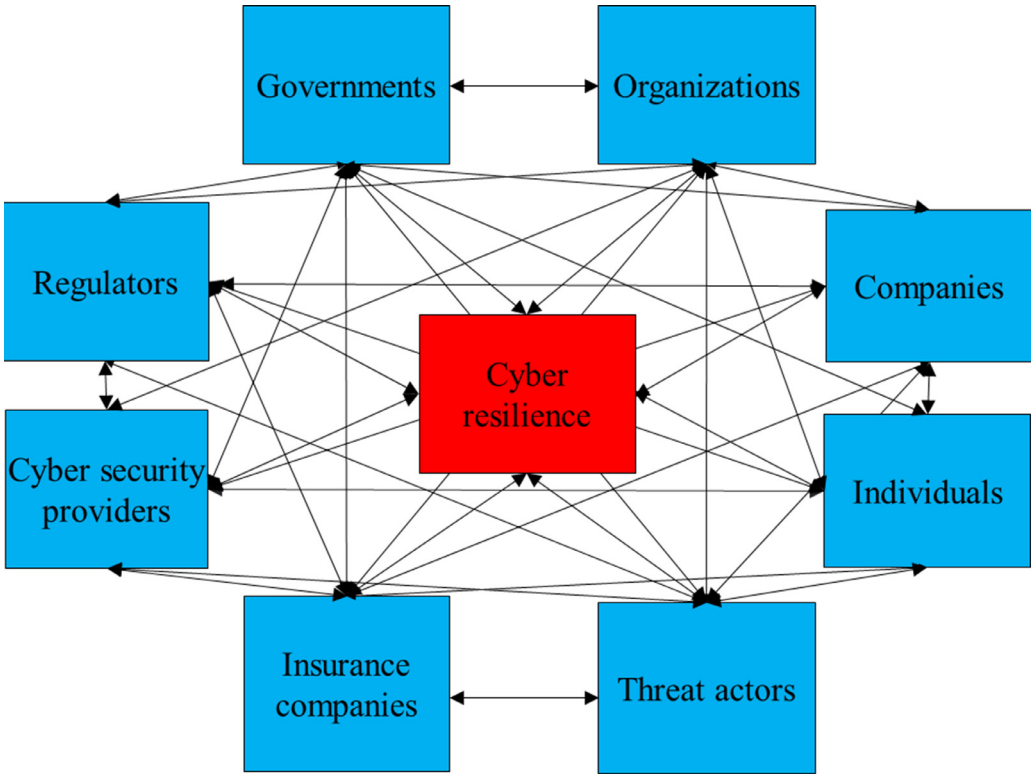

Fig. 1. Examples of actors involved in cyber resilience.

they may follow norms, laws, rules, and procedures. Some of the actors and their involvement in cyber resilience are shown in Fig. 1, with the purpose of identifying key actors relevant for preserving and compromising cyber resilience.

The two-way arrows in Fig. 1 specify any kind of relationship or interaction. We assume generally two-way arrows, though one-way arrows may apply in special cases. Some actors impact cyber resilience to a larger extent than they are impacted by it, and vice versa for other actors. The eight kinds of actors play different roles related to cyber resilience in a plethora of senses. For example, governments prefer improved cyber resilience within their jurisdiction, from which many organizations, companies, and individuals benefit. In contrast, threat actors, which may be individuals or collective units, prefer to decrease cyber resilience or exploit lacking cyber resilience to their advantage. Cyber security providers may prefer lacking cyber resilience, but available technology, so that they have something to provide. Regulators and insurance companies may prefer a state of affairs which enables a role for regulation and insurance which impacts cyber resilience.

3.3. *Cyberspace*

Cyberspace is in the literature defined in various ways, and is used in many contexts. The European Union uses it more or less in the same meaning as the Internet [12]. International Organization for Standardization [24] and Tanenbaum [49] consider cyberspace for all practical purposes as synonymous with the Internet, which is a global cyberspace in the public domain. International Telecommunication Union [25] uses the term cyber environment, which roughly equals "a system that makes use of cyberspace." Other initiatives focus more on cyberspace in relation to critical infrastructures [38,52]. Examples of cyberspaces that are not connected to the Internet are military computer networks, as well as emergency communication networks and systems. Examples of cyberspaces that preceded the Internet were the non-commercial National Science Foundation Network [39], as well as the Advanced Research Projects Agency Network [3] that was operative from 1969.

Eling, Schnell, and Sommerrock [10] and Refsdal, Solhaug, and Stølen [43] define cyberspace as a collection of interconnected computerized networks, including services, computer systems, embedded processors, and controllers, as well as information in storage or transit. A common form of interconnected computerized networks is a collection of local area networks (LANs) that are connected by a wide area network (WAN). The networks may be agile, and may involve personal areas, mobile networking, etc.

Prior to the emergence of today's internet X. 25 was launched as an ITU-T standard protocol suite for packet-switched data communication in WAN, originally defined by the International Telegraph and Telephone Consultative Committee in 1976 [6]. Minitel was a videotex online service accessible through telephone lines. It launched experimentally in July 1980 in Saint-Malo, France, and subsequently spread to other areas [41]. It was the world's most successful online service prior

to the World Wide Web. The internet and other networks are the technical foundation of today's cyberspace. Cyberspace is the virtual sphere in which network users interact. Cyberspace is at a higher abstraction level than the networks. We thus define cyberspace as follows:

Definition 3. Cyberspace is the virtual sphere of any collection of interconnected networks within which network users interact.

4. Resources, competence, technology, tools, and strategies in cyber resilience

Now that we have considered the actors, levels, beliefs, and preferences relevant for cyber resilience, and what we mean by cyber resilience, let us proceed to consider the resources, competence, technology, tools, and strategies in cyber resilience. An actor such as a firm may have certain resources and may decide how to allocate resources to cyber resilience. Another actor such as a branch of government may be allocated resources from a budget earmarked for resilience generally, or for cyber resilience in particular. Applying resources requires competence in what technology and tools to acquire, and which strategies to choose. Choice of technology and tools may enlarge or constrain one's available strategies. Some tools may be costly and have some advantages enhancing cyber resilience, but also disadvantages or limitations potentially compromising cyber resilience. Choice of technology and tools, and how to update these over time, express adaptation to changes, which in turn impact cyber resilience over time. Understanding oneself as an actor, one's supporting actors, and the typology of threat actors (i.e., a systematic classification of their types according to their common characteristics), is essential for developing appropriate strategies for cyber resilience. For example, understanding how to share information with one's cooperating actors may be essential to deter attackers [21]. Moreover, concentrating on a single aspect of cyber resilience and taking measures, e.g. by devoting resources into preventing denial of service attacks, lacks a balanced approach and leaves the door open, e.g. for Trojan horse attacks." Attacking actors can be expected to analyze the characteristics and especially vulnerabilities for the actors they attack, and substitute between various preferred strategies to apply [11,20,32]. Actors apply resources, competence, technology, and tools, to choose optimal strategies when interacting with each other to maximize one's cyber resilience, and sometimes to minimize the cyber resilience of other actors.

5. Cyber resilience and cyber insurance

The relationship between cyber resilience and cyber insurance is a form of risk transferal. The relationship depends on the preferences, beliefs, responsibilities, and actions of the different actors, i.e. the companies, organizations, and individuals requesting cyber insurance; the threat actor typology and threat actors; the incident responders; the governments including regulators and international bodies; the insurers; and the brokers.

The relationship between cyber resilience and cyber insurance further depends on entry requirements or preconditions for signing cyber contracts which impact premiums, the services provided by insurance companies such as incident response, data gathering from claims, and limitations on coverage based on security measures in place.

Cyber insurance can improve cyber resilience through the influence of insurance companies on insured organizations, applying various cyber security arrangements. Influential are also third-parties including supply chains, trusted relationships especially relevant for large organizations, and best practices especially relevant for small and medium enterprises.

Improved cyber insurance is possible by designing and monitoring appropriately the insurance contracts between the insured actor (seeking insurance) and the insurance company. Both the insured actor and the insurance company should adopt good practices, support each other in case of cyber events, and respond fast to each other to limit the losses. The responsibilities of the various actors should be defined. The exposures and the claims should be reported efficiently. Data should be gathered reliably. Appropriate incentives should be provided to the IT systems managers in the insured companies. Regulations should be appropriate.

6. Cyber resilience in the future

The internet of things (IoT) exists today in a premature state. The IoT is like the regular internet, except that it is tailor-made for communication between us and the things around us, and automatic interaction between things themselves. Today, only a few of the things we use are online, and the interaction is mainly manual. For example, when we turn on the heat in the cabin via the internet, we communicate with an oven. It seems possible that in the future, many man-made things will be available online with more automatic and intelligent communication. For example, our car may turn on the cabin heat when the GPS tracker realizes where the car is headed. Intelligent appliances such as turning on cabin heat can be considered IoT. Especially in large quantities, such appliances can impact the physical infrastructure substantially, e.g. the power grid transmission and distribution elements, or metro operations, which by themselves are not IoT.

The IoT is challenging from a security perspective which causes a linkage between IoT and cyber resilience, which impact each other mutually. On the one hand, the quality of cyber resilience depends on the state of the art within the IoT. On the other hand, the development of the IoT depends on the quality of cyber resilience, as IoT benefits from an improved cyber resilience stance of cyberspace as a whole. The following exemplify future challenges:

- Colossal attack surface: Since everything is linked to everything and potentially reachable from anywhere in the world, a tremendous attack surface exists. For example, a high-voltage transmission tower that could previously only be cut down or blasted physically, may potentially be disabled electronically from the other side of the globe.

- Insufficient technology: Information technology providers strive to offer new networks and platforms for the Internet of Things. Worldwide, more than 400 mobile networks exist today [50], in addition to cloud back-ends, IoT hardware, and firmware. On top of these, a "grand experiment" [51] occurs where little-tested and sometimes immature products are integrated. Such products may sometimes have been designed for a different use, a different security need, and potentially with limited battery capacity, computational power or memory.
- Challenging handling of data: Representing, compiling, transferring, and storing data may involve mis-representation, incorrect compilation, misuse, and manipulation. Data needs to be available but also secure, and algorithms and machines need to be trustworthy and reliable. For example, it may be easy to hide information on page 2 of google. Data aggregation, anonymizing data, stalkerware, and targeted surveillance, may cause further challenges.
- Possible excessive trust in computers and software: The algorithms in computers exceed or may exceed human capabilities in many areas, such as computation, handling complexity, consistency according to specified criteria, and reliability of detection. In other areas, the algorithm may be inferior, e.g. by misrepresenting reality and interpreting data in a faulty manner. Consider e.g. an autonomous car which may keep perfect distance to the car ahead which may move erratically. However, the car's algorithm may have overlooked aspects where humans may be superior, such as assessing unusual circumstances, contextual factors, weather conditions, and pedestrians with different characteristics.
- Ethics: The emerging technologies involved in cyber resilience and IoT raises new ethical challenges. For example, the financial sector (banks, investment companies, insurance companies, real estate firms, etc.) has traditionally had controls such as job rotations, forced/required holidays, and separation of duties. These controls may be insufficient when a leaving employee may use the new technologies criminally e.g. to copy confidential records of clients. As another example, the increased used of facial recognition and surveillance may enable trusted employees in companies to stalk targets, e.g. by using emails and related information obtained in their job to contact the targets privately

Interviews of 105 security experts from Asia and Europe conducted by Radar Services [42] reveal seven kinds of findings regarding future developments. First, 72%, 21%, 7% believe that companies are not (well) prepared, prepared, and (very) well prepared, respectively for the future regarding information technology security management. Second, regarding frequently neglected loopholes, "55% name users as the most neglected security risk," "16% criticize the security of current IoT devices," and "12% miss clear responsibilities and processes." Third, on average 300% growth of cyber attacks a year is expected, divided so that 7% expect above 1000% growth, 24% expect 500–1000% growth, 30% expect 100–500% growth, and none expect a sideways trend or decline towards 2025. Fourth, among the experts regarding future cyber attacks, 34% expect attacks against IoT, 28% expect attacks against critical infrastructure, 6% expect smartphone attacks, 6% expect social engineering, 6% expect attacks against cloud services, and 20% expect other kinds of attacks. Fifth, within 2025, 89% of the experts "are convinced of well and very well-advanced machine learning" and artificial intelligence capabilities within information technology security, while 11% are not yet convinced of such capabilities. Sixth, regarding future resource allocation, 40% suggest artificial intelligence and machine learning, 26% suggest continuous security monitoring, 7% suggest blockchain, 5% suggest awareness training, 5% suggest encryption, and 17% suggest other allocation. Seventh, for information technology security that will lose importance until 2025, 33% suggest antivirus, 14% suggest signature-based systems, 12% suggest firewalls, 9% suggest blockchain, 7% suggest that all technologies will stay relevant, 5% suggest password protection, and 20% suggest other technologies.

The IoT will undoubtedly facilitate many tasks in our daily work, but it will also simplify the lives of, for example, terrorists. It will no longer be necessary to physically hijack a truck or aircraft, and it may possibly become less necessary to blow oneself up in a suicide attack. The IoT keeps gaining electronic access to, for example, the metro in big cities which may trigger a catastrophic event. More generally, cyber resilience in the future will be further impacted by technical and organizational factors, the agile aspects of organizations, various standards, and the IoT.

7. Future research

Future research should scrutinize cyber resilience more thoroughly with at least seven focus points proceeding beyond the focus in this article. First, a systemic and technical focus on controls, measures, and recovery mechanisms, accounting for a changing cyber landscape. Second, a focus on organizational aspects including trust relationships, autonomy, and recovery mechanisms. Third, a focus on human behavioral patterns including human behavior and habits, security awareness and attitudes. Fourth, a focus on policy and regulation. Fifth, a focus on learning from the past, adapting to the present, and evolving into the future. Sixth, compiling historical data of cyber incidents, and causes and consequences of systemic, human, organizational, and strategic errors. Seventh, it may be hypothesized that cyber-resilient actors may potentially be better suited to deal with gray swans, believed to be common in cyberspace. gray swans are distinguished from white swans which are empirically verifiable, and black swans [47] which are known unknowns. Future research should also assess whether cyber-resilient actors may potentially be better suited to deal with unknown unknowns.

8. Conclusion

The article reviews and assesses the emerging role of cyber resilience. First, cyber resilience involves a variety of different actors classified into non-threat actors, threat actors, and hybrid actors. Non-threat actors can be governments, regulators,

incident responders, insurers, organizations and individuals. Threat actors can be hackers and criminals. Hybrid actors can be companies which may sometimes, deliberately or inadvertently, compromise the cyber resilience of other actors. Actors operate at various levels, ranging from the individual, via group, organization, region, etc., to the global level. Each actor chooses strategies based on beliefs and preferences which impact and is impacted by cyber resilience.

Second, common definitions of cyber resilience are refined and expressed as the ability of an actor to resist, respond and recover from cyber incidents to ensure the actor's operational continuity.

Third, the actors impacting and being impacted by cyber resilience are identified. These actors possess resources, competence, technology, and tools of various kinds, which in turn impact strategies and cyber resilience for all actors.

Fourth, cyber resilience relates to cyber insurance through entry requirements or preconditions for cyber contracts which impact premiums, various services such as incident response, data gathering from claims, and cover limitations based on available security measures.

Fifth, the expected role of cyber resilience in the future is sketched. Cyber resilience is linked to the internet of things which can be expected to simplify many aspects of life e.g. through offering artificial intelligence and machine learning. Challenges pertaining to the internet of things are a colossal attack surface, insufficient technology, challenging handling of data, possible excessive trust in computers and software, and ethics. Cyber resilience is also linked to e.g. future use of robots by firefighters attacking a data center fire. Finally, future research possibilities are outlined.

Declaration of Competing Interests

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.

Acknowledgement

I thank Ketil Stølen and participants at the Lorentz Center Workshop for useful discussions: Leiden University, Lorentz Center Workshop, "Lorentz Center Cyber Insurance and its Contribution to Cyber Risk Mitigation," Leiden, The Netherlands, March 25-29, 2019, http://lorentzcenter.nl/lc/web/2019/1096/info.php3?wsid=1096&venue=Oort.

References

[1] A. Almomani, B.B. Gupta, T.-.C. Wan, A. Altaher, S. Manickam, Phishing dynamic evolving neural fuzzy framework for online detection "Zero-Day" phishing email, Indian J. Sci. Technol. 6 (1) (2013) 3960–3964.
[2] Anderson, R., Bohme, R., Clayton, R., & Moore, T. (2008). *Security economics and the internal market*. https://www.enisa.europa.eu/publications/archive/economics-sec/.
[3] ARPANET. (2020). Advanced Research Projects Agency Network (ARPANET). Retrieved from https://www.britannica.com/topic/ARPANET, retrieved April 22, 2020.
[4] V. Bier, A. Gutfraind, Risk analysis beyond vulnerability and resilience - characterizing the defensibility of critical systems, Eur. J. Oper. Res. 276 (2) (2019) 626–636, doi:10.1016/j.ejor.2019.01.011.
[5] T.P. Bostick, E.B. Connelly, J.H. Lambert, I. Linkov, Resilience science, policy and investment for civil infrastructure, Reliab. Eng. Syst. Saf. 175 (2018) 19–23, doi:10.1016/j.ress.2018.02.025.
[6] CCITT, Sixth Plenary Assembly: Orange Book, Geneva: International Telecommunications, Union, 1978 http://search.itu.int/history/HistoryDigitalCollectionDocLibrary/4.257.43.en.1001.pdf.
[7] CISA. (2020). Assessments: Cyber Resilience Review. Retrieved from US Department of Homeland Security, https://www.us-cert.gov/resources/assessments, retrieved April 22, 2020.
[8] D. DiMase, Z. Collier, K. Heffner, I. Linkov, Systems engineering framework for cyber physical security and resilience, Environ. Syst. Decis. 35 (2) (2015) 291–300.
[9] I. Ed-daoui, A. ElHami, M. Itmi, N. Hmina, T. Mazri, Resilience assessment as a foundation for systems-of-systems safety evaluation: application to an economic infrastructure, Saf. Sci. 115 (2019) 446–456, doi:10.1016/j.ssci.2019.02.030.
[10] M. Eling, M. Schnell, F. Sommerrock, Ten Key Questions On Cyber Risk and Cyber Risk Insurance, The Geneva Association, Zurich, 2016.
[11] W. Enders, T. Sandler, A. Silke, G. Ilardi (Eds.), Researching Terrorism: Trends, Achievements, Failures, Ilfords, UK, 2003 Frank Cass.
[12] European Commission. (2013). *Join 1 Final: Cybersecurity Strategy of the European Union – An Open, Safe and Secure Cyberspace*. https://ec.europa.eu/digital-single-market/en/news/communication-cybersecurity-strategy-european-union-%E2%80%93-open-safe-and-secure-cyberspace.
[13] Y.P. Fang, E. Zio, An adaptive robust framework for the optimization of the resilience of interdependent infrastructures under natural hazards, Eur. J. Oper. Res. 276 (3) (2019) 1119–1136, doi:10.1016/j.ejor.2019.01.052.
[14] F. Flammini, Resilience of Cyber-Physical Systems: From Risk Modelling to Threat Counteraction, 1st ed, Springer International Publishing: Imprint: Springer, 2019 2019. ed.Cham.
[15] U. Franke, The cyber insurance market in Sweden, Comput. Secur. 68 (2017) 130–144, doi:10.1016/j.cose.2017.04.010.
[16] V. Gisladottir, A.A. Ganin, J.M. Keisler, J. Kepner, I. Linkov, Resilience of cyber systems with over- and underregulation, Risk Anal. 37 (9) (2017) 1644–1651, doi:10.1111/risa.12729.
[17] B.B. Gupta, D.P. Agrawal, H. Wang, Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives, CRC Press, Taylor & Francis, Boca Raton, Florida, 2018.
[18] B.B. Gupta, D.P. Agrawal, S. Yamaguchi, Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security, Hershey, Pennsylvania: IGI Global, 2016.
[19] W. Harrop, A. Matteson, Cyber resilience: a review of critical national infrastructure and cyber security protection measures applied in the UK and USA, J. Bus. Contin. Emer. Plan. 7 (2) (2013) 149–162.
[20] K. Hausken, Income, interdependence, and substitution effects affecting incentives for security investment, J. Account. Public Policy 25 (6) (2006) 629–665, doi:10.1016/j.jaccpubpol.2006.09.001.
[21] K. Hausken, Security investment, hacking, and information sharing between firms and between hackers, Games 8 (2017) 2, 23 pages, doi:10.3390/g8020023.
[22] L. Herrington, R. Aldrich, The future of cyber-resilience in an age of global complexity, Politics 33 (4) (2013) 299–310, doi:10.1111/1467-9256.12035.
[23] F. Hult, G. Sivanesan, What good cyber resilience looks like, J. Bus. Contin. Emer. Plan. 7 (2) (2013) 112–125.

[24] International Organization for Standardization. (2012). *ISO/IEC 27032 – Information Technology – Security Techniques – Guidelines For Cybersecurity*. International Electrotechnical Commission.
[25] International Telecommunication Union. (2008). *Itu-T X.1205 – Data Networks, Open System Communications and Security – Telecommunication Security – Overview of Cybersecurity*.
[26] ISO/IEC. (2013). ISO/IEC 27002:2013 Information Technology — Security Techniques — Code of Practice for Information Security Controls. Retrieved from https://www.iso.org/standard/54533.html, retrieved April 22, 2020.
[27] F. Jiang, Y. Fu, B.B. Gupta, F. Lou, S. Rho, F. Meng, Z. Tian, Deep learning based multi-channel intelligent attack detection for data security, IEEE Trans. Sustain. Comput. (2018) 1–11, doi:10.1109/TSUSC.2018.2793284.
[28] M. Kaufmann, Cyber-resilience in the EU, Int. Polit. 71 (2) (2013) 274–283.
[29] S. Kishor, D.S. Kim, R. Gosh, Resilience in computer systems and networks, in: Proceedings of the International Conference on Computer-Aided Design, 2009, pp. 74–77.
[30] A. Kott, I. Linkov, Cyber Resilience of Systems and Networks, 1st ed, Cham: Springer International Publishing: Imprint: Springer, 2019.
[31] H. Kunreuther, G. Heal, Interdependent Security, J. Risk Uncertain. 26 (2–3) (2003) 231–249, doi:10.1023/a:1024119208153.
[32] D. Lakdawalla, G. Zanjani, Insurance, Self-Protection, and the Economics of Terrorism, RAND and NBER, Federal Reserve Bank of New York, 2002.
[33] I. Linkov, D. Eisenberg, K. Plourde, T. Seager, J. Allen, A. Kott, Resilience Metrics for Cyber Systems, Environ. Syst. Decis. 33 (4) (2013) 471–476.
[34] I. Linkov, J.M. Palma-Oliveira, Resilience and Risk: Methods and Application in Environment, Cyber and Social Domains, 1st ed, Springer Netherlands: Imprint: Springer, Dordrecht, 2017.
[35] I. Linkov, L. Roslicky, B.D. Trump, Resilience and Hybrid Threats: Security and Integrity for the Digital World, IOS Press, Incorporated, Amsterdam, 2020.
[36] V.A. Memos, K.E. Psannis, Y. Ishibashi, B.-.G. Kim, B.B. Gupta, An efficient algorithm for media-based surveillance system (EAMSuS) in IoT smart city framework, Future Gener. Comput. Syst. 83 (2018) 619–628.
[37] T. Moore, The economics of cybersecurity: principles and policy options, Int. J. Crit. Infrastruct. Prot. 3 (3) (2010) 103–117, doi:10.1016/j.ijcip.2010.10.002.
[38] National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity, V1.1*. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.
[39] NSFNET. (2020). National Science Foundation Network (NSFNET). Retrieved from https://icannwiki.org/NSFNET, retrieved April 22, 2020.
[40] A.P. Plageras, K.E. Psannis, C. Stergiou, H. Wang, B.B. Gupta, Efficient IoT-based sensor big data collection–processing and analysis in smart buildings, Future Gener. Comput. Syst. 82 (2018) 349–357.
[41] Puech, M. (2010). Le Monde du Minitel se Paye Le Monde" [The World of Minitel Pays for 'Le Monde']. Retrieved from https://blogs.mediapart.fr/michel-puech/blog/200610/le-monde-du-minitel-se-paye-le-monde, retrieved April 22, 2020.
[42] Radar Services. (2018). Cyber Attacks and IT Security Management in 2025: Expert Survey 2018. Retrieved from https://www.radarservices.com/study2025/, retrieved April 2, 2020.
[43] A. Refsdal, B. Solhaug, K. Stølen, Cyber-Risk Management, 1st ed, Cham, Switzerland: Springer International Publishing, 2015 2015. ed.
[44] S. Romanosky, L. Ablon, A. Kuehn, T. Jones, Content analysis of cyber insurance policies: how do carriers price cyber risk? J. Cybersecur. 5 (1) (2019) https://doi.org/10.1093/cybsec/tyz1002.
[45] B. Schneier, Insurance and the computer industry, Commun. ACM 44 (3) (2001) 114–115, doi:10.1145/365181.365229.
[46] C. Stergiou, K.E. Psannis, B.-.G. Kim, B. Gupta, Secure integration of IoT and cloud computing, Future Gener. Comput. Syst. 78 (2018) 964–975.
[47] N.N. Taleb, The Black Swan: The Impact of the Highly Improbable, Penguin, London, 2007.
[48] S.A. Talesh, Data breach, privacy, and cyber insurance: how insurance companies act as “Compliance Managers” for businesses, Law Soc. Inq. 43 (2) (2018) 417–440, doi:10.1111/lsi.12303.
[49] A.S. Tanenbaum, Computer Networks, 4th ed, Prentice Hall PTR, Upper Saddle River, NJ, 2003 ed.
[50] Telenor Group. (2020). Internet of Things – Smarter and More Sustainable Societies. Retrieved from https://www.telenor.com/innovation/internet-of-things/, retrieved April 2, 2020.
[51] Turck, M. (2018). Growing Pains: The 2018 Internet of Things Landscape. Retrieved from https://mattturck.com/iot2018/, retrieved April 2, 2020.
[52] United States Department of Homeland Security. (2013). *NIPP 2013 - Partnering for Critical Infrastructure Security and Resilience*.
[53] M.D. Wood, E.M. Wells, G. Rice, I. Linkov, Quantifying and mapping resilience within large organizations, Omega, 87 (2019) 117–126.
[54] D. Woods, I. Agrafiotis, J. Nurse, S. Creese, Mapping the coverage of security controls in cyber insurance proposal forms, J. Internet Serv. Appl. 8 (1) (2017) 1–13, doi:10.1186/s13174-017-0059-y.
[55] D. Woods, A. Simpson, Policy measures and cyber insurance: a framework, J. Cyber Policy 2 (2) (2017) 209–226, doi:10.1080/23738871.2017.1360927.
[56] V. Zemba, E.M. Wells, M.D. Wood, B.D. Trump, B. Boyle, S. Blue, I. Linkov, Defining, measuring, and enhancing resilience for small groups, Saf. Sci. 120 (2019) 603–616.