Techno-economics of IoT and OT Security

Morten Falch and Reza Tadayoni

Aalborg University, Copenhagen, Denmark

https://doi.org/10.26636/jtit.2025.FITCE2024.2032

Abstract — This paper provides an overview of the techno-economics of cybersecurity in IoT and OT devices. The purpose is to identify and provide justification for regulatory action within the area.

Keywords — cybercrime, cybersecurity, IoT, justification for regulation, OT, techno-economics

1. Introduction

Cybersecurity has become a serious challenge for businesses around the world. PricewaterhouseCoopers (PwC) has reported cybercrime to be the most widespread kind of economic fraud [1]. Cryptocurrencies valued at more than 400 million dollars were paid to ransomware addresses in 2020. This represents a growth of more than 400% in one year. At the same time attacks by malware increased by 358%. Distributed denial of service (DDOS), ransomware and other kinds of cyberattacks are happening more and more frequently, and for businesses this can lead to severe consequences, e.g. interruption of work processes and customer services, loss and compromising of data, violation of data protection and privacy laws, a lot of time wasted, and large additional costs.

The ongoing process of digital transformation is affecting all businesses and organizations, large and small, and this puts further focus on the challenges related to cybersecurity. In the latest global risk report published by the World Economic Forum the issue of cybersecurity reappeared to be among the top 10 global risks, and cyberattacks on critical infrastructure were seen as one of the risks with the largest potential impact on a global scale [2]. This concern is partly due to cyberattacks against Ukraine in 2022. Also cyberattacks jeopardizing privacy of vulnerable citizens is seen as a global risk.

In this regard Internet of Things (IoT) and Operational Technologies (OT) security are becoming still more important. The number IoT devices has exploded within the past decade and many of these are not sufficiently protected. A lot of IoT devices lack built-in capabilities for updating software and this makes it difficult to maintain security. Hackers cannot only hamper their functionality but can also use them as a gateway to other IT systems and devices. Especially badge readers, cameras and printers are devices of concern from a security perspective.

Likewise, OT security has gained in importance, as this is a key issue for securing critical infrastructures. Compared to the number of IoT devices, OT devices are lower in numbers, but more valuable. Many critical infrastructures are highly dependent on OT devices and disruption of their operations may have a detrimental impact on the functions of the society.

Cybersecurity as a policy issue has attracted a lot of attention both from a regulatory perspective and in economic literature. The EU has published a common strategy on cybersecurity [3] and several major initiatives are being launched by the EU to increase awareness and to protect critical infrastructures, e.g., the Network and Information Security 2 (NIS2) directive [4]. Likewise in the US the Executive Order 14028 is issued to protect critical infrastructures. Another legislation, which is relevant for cybersecurity of OT and IoT, is the forthcoming EU Cyber Resilience Act (CRA) [5]. This act will impose demands on cybersecurity for manufacturers of hardware.

The economics of cybersecurity is a relatively new area of research. While much research has been published on development of technical solutions and strategies for implementation, the economic foundation of any regulation or strategy for remedying cybercrime is still under development. This is especially the case when it comes to cybersecurity in IoT and OT devices.

This paper provides an overview of the IoT and OT security challenges, the techno-economic characteristics of possible cybersecurity measures to be taken, and the market failures to be addressed. Finally, the paper identifies the regulatory challenges that follows from this analysis. More specifically the paper discusses cybersecurity issues related to IoT and OT, how they can be addressed by the market, and where regulatory intervention is needed.

First the paper identifies IoT and OT cybersecurity challenges [6]–[8]. Then the economic characteristics of different security measures is discussed. As point of departure, this discussion is based on current research on cybersecurity as an economic good including [9]–[11]. Compared to these contributions, the authors take an approach, where the characteristics of the specific security measures identified in the technical analysis of IoT and OT are taken into account. Based on this, regulatory challenges regarding market intervention are identified.

2. Information Security, ICT Security, and Cybersecurity

Before we discuss the economic characteristics of cybersecurity, we will define the term cybersecurity and compare it with similar terms used in in the literature. Many of the contributions in cybersecurity economics are using a similar approach to what is applied in information security economics

and economics of privacy [11]. Here cybersecurity is seen as a collection of tools, which can be applied to protect information. It is therefore relevant to highlight how cybersecurity relates to these other terms. What are the similarities and differences and what are the implications of this on the economic characteristics?

Many definitions of cybersecurity are based on the so-called CIA triad: confidentiality, integrity, and availability of information. The CIA triad dates back to the 1970s, where it was introduced in [12]. The triad is also included in the definition provided by The International Telecommunications Union (ITU) [13]. This definition also specifies the kind of assets to be protected, namely connected computing devices, personal infrastructure, applications, services, and telecommunications systems. The CIA triad has later been complemented by non-repudiation, accountability, authenticity, and reliability of information. However, it is argued that this definition needs to be updated to include broader aspects of cybersecurity than just the technical protection of information [14].

Paper [13] makes a distinction among information security, ICT security, and cybersecurity based on the kinds of assets to be protected. Information security deals with the protection of information. Information might be stored or transmitted using ICT, but this is not necessarily the case. ICT security deals with the protection of the ICT system, which is used to store and handle the information. In contrast to this, cybersecurity is not always about confidentiality, access, or integrity of information. It also encompasses protection of non-information assets such as home automation systems and public utility infrastructures. Thus, cybersecurity can be defined as [13]:

"the protection of cyberspace itself, the electronic information, the ICTs that support cyberspace, and the users of cyberspace in their personal, societal and national capacity, including any of their interests, either tangible or intangible, that are vulnerable to attacks originating in cyberspace".

Article [14] argues that cybersecurity is more than just protection, and refers to the NIST framework, that includes five different activities: identify, protect, detect, respond, and recover. In this framework cybersecurity is more than just a product and includes an organizational framework to be implemented in order to protect the assets. This calls for a human-inclusive approach including sociological and psychological aspects, challenging the machine focused definition of cybersecurity [15]. Here the definition offered by [16] becomes relevant, as it offers a process-oriented view. Here cybersecurity is defined as "standard practices that involve the people, processes, and technologies in an organization, in a group, or stand-alone environments in which the computers and cyber-physical systems with valuable data are connected to cyberspace".

It follows that although there is a considerable overlap one must distinguish between the terms information security and cybersecurity. Information security deals with all kinds of information, also information not stored in a digital format. Cybersecurity deals only with digital information, but it includes as well also other kinds of assets such as computer systems and non-digital assets, which depend on the functioning of ICT based systems. Moreover, cybersecurity is not only about technical measures for protection. It is also about human and business processes [17].

Privacy is another term that is used in connection with cybersecurity. Privacy deals with personal information only and can be considered as a subset of information security. Moreover, privacy focuses on the confidentiality aspect and to a certain degree on the integrity aspect of the CIA triad. Still the economics of the three areas cybersecurity, information security, and privacy are closely related areas although they present distinct areas of research.

3. OT and IoT Security

OT and IoT technologies are facing a number of challenges when it comes to security and privacy issues. There are some specific risk factors and requirements related to these types of devices. It can be due to the limited computing and storage capacities and constrains on the power supply and battery capacity in the lightweight devices, when it comes to IoT, or in the way the equipment is integrated into the IT systems, when it comes to operational technologies (OT). The computing capacity and limited power supply make it difficult to develop advanced encryption protocols in the devices and the lack of integration in the IT systems makes it difficult to update OT devices and other IT equipment.

One important security and risk issue of IoT and OT is the standardization and regulation [18], [19]. This can relate to both protocols and the way the default set up of devices are configured. Many IoTs come with a minimum of security functions implemented and some come with default login and passwords without any requirement from the vendors that the user must change this default password before the use of the devices. This induces a big security risk. To avoid these security challenges, harmonized standards and regulatory initiatives at device and operator levels can be essential.

Another challenge is the legacy issues. The use of open access networks has exposed the supervisory control and data acquisition (SCADA) systems to cyber attacks [20]. Many IoT and OT devices are based on old software and hardware frameworks, which are difficult to update to adopt to modern security and privacy standards and requirements without allocation of enormous financial resources. For example, when it comes to the OT, the SCADA systems, which are used in many critical infrastructures, are old and imply significant security risks. This issue was raised already back in 2006 "the increasing interconnectivity of SCADA networks has exposed them to a wide range of network security problems" [21]. One of the major vulnerabilities of the OT systems based on SCADA is the growth of connectivity of internal company networks to the outside word resulting in possibilities for cyberattacks etc. Many OT devices are not updated properly as this will demand down time in the line of production, and in some cases the device and equipment are not integrated in the IT environment of the company, which makes it difficult to be updated.

The physical accessibility is another challenge when it comes to the IoT and OT devices, as the devices may be easily accessible from outside and often without proper surveillance [22]. Of course, proper security strategies and allocation of the necessary financial resources to prevent physical accessibility can be restricted to critical devices, but legacy systems have not prioritized this aspect and continue to be a challenge.

Another important security risk, which is a hot topic for the time being, is supply chain attacks, which can be made by comprising the software or hardware in a specific vulnerable part of the value chain. Vulnerabilities can come from the physical access to part of the value chain or weak access mechanisms when uploading software or introducing new hardware. SolarWinds hack is a prime example of a supply chain attack [23], [24].

Furthermore, the regular cyber security risks like ransomware attacks, where critical IoT or OT devices are locked by criminals [25], and DDoS attacks, where huge amounts of IoT devices are used to send great quantities of requests and thereby overload the receiving systems and put them out of function [26], are examples of exploitation of the vulnerabilities of IoT and OT systems.

A last thing we want to mention is the privacy issues [27]. The IoT devices gather huge amount of data. Some of these may be sensitive company data or include personal information of users or customers.

Solutions to all the abovementioned problems include an interplay of technological, economic and regulatory aspects. We need new technologies and security strategies at device and infrastructure levels. But we also need financial resources and new business models as well as policy and regulatory interventions to create mandatory security standards and practices.

4. Research in Economics of Cybersecurity

Article [16] provides an extensive literature review of different research directions on cybersecurity economics. The review is based on 28 studies selected among more than 600 models identified by the authors:

1) Budgeting finding the optimal level of investments in cybersecurity
   - Investment,
   - Externalities,
   - Insurance.
2) Economic efficiency
   - Misallocation of resources,
   - The type of good (private, common, club, public).
3) Interdependent risks
   - Network effects,
   - Lock-in effects,
   - Supply-chain risks.
4) Information asymmetry
5) Governance
6) Cybercrime
7) Sustainability

There is a considerable overlap between most of these topics. While the first point deals with cybersecurity at the micro-level, where the possible action of the individual organization is the point of departure, the remaining points address issues at the meso and macro levels.

Although the list includes diverse research issues, the overall theme is how to decide the optimum level of investments in cybersecurity and the scope for public intervention. These issues are related to the economic characteristics of cybersecurity and the lack of transparency of the market.

The issue of cybercrime looks in principle at the same issues, but here the focus is on the market, where the cybercriminals act. How is the market for cybercrime structured and what are the economic characteristics of the products offered on this market?

The economic characteristics are especially related to research on externalities of cybersecurity products. Investments in cybersecurity may imply strong positive externalities, as they may prevent spreading of malware etc. beyond the stakeholder financing the investment.

Borrowing from information economics, Samuelson's concept of public good is often used for describing the economic characteristics of cybersecurity. Samuelson distinguishes among four types of goods according to two parameters (rivalry and exclusivity (Fig. 1): normal goods, club goods, common goods, and public goods. Tangible goods such as foodstuff, cars, computers etc. are rivalrous as they can be consumed only once. They are also excludable as access is limited. These goods are termed normal goods.

Information on the other hand can be used many times. Therefore, information goods are seen as being non-rivalrous. Depending on the context, information goods are in principle also non-exclusive, as they can easily be copied and made available to everybody, as soon as the information is revealed. Information is therefore termed as a public good, along with a range of public services offered by the government. National defense is the most prominent example of a public good. It is however possible to restrict access to certain information goods. In this case they can be termed as club goods.

When it comes to cybersecurity, several authors see this as a product with strong public good characteristics [16], [28].

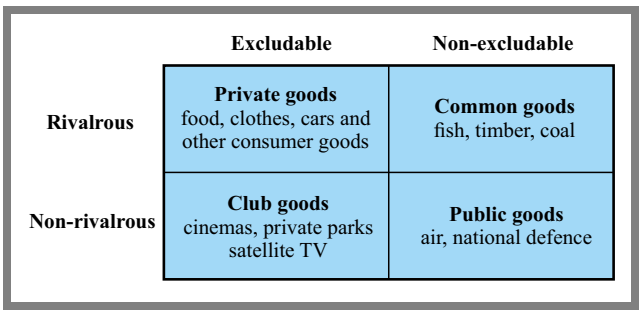

Fig. 1. Private goods, common good, club good, and public goods.

The argument is primarily the strong positive external effects that investments in cybersecurity may have on other actors. Another reason may be that cybersecurity can be considered as a kind of information good with similar economic characteristics as other information goods. Therefore, the positive externalities are often taken for granted. When consumption of public goods is up to an individual decision-making on an unregulated market, this will result in underinvestment.

However, it can be problematic to treat cybersecurity as one single homogeneous product. Achieving cybersecurity takes investments in a wide range of different measures, each with their own economic characteristics.

One approach to go a bit deeper into the economic characteristics of cybersecurity is to analyze cybersecurity for different types of actors and how they interact. Bauer and Eeten claim that externalities include spill-over effects among different types of actors and provide a framework for analysis of these spill-over effects [28]. Their analysis focuses on analysis of cybersecurity products implemented at the network level, and their impact on security for other groups of actors. Following groups of actors are included in the analysis: ISPs, application and service providers (App/Svc), hardware and software vendors, users, security providers, and national and international organizations.

The ISPs constitute the core of the ecosystem. ISPs are interconnected and their level of cybersecurity is highly dependent on the security level in those ISPs to which they are connected. Moreover, they depend on application and service providers, security providers, hardware and software vendors, and users. Finally various governance institutions may contribute to the level of security. The point made in this paper is that each actor will decide on the level of investments according to their own costs and benefits, and free riders may occur. Some spill-over effects may be reflected in the prices. For instance, may users be willing to pay for having an ISP they consider offering a high level of cybersecurity. However, the market for cybersecurity is far from being transparent and information asymmetries exist.

With regard to IoT and OT, it is important also to look at cybersecurity achieved at the device level. Here equipment manufactures and standardization bodies are important actors.

Supply chain risk is another kind of spill-over effect. Here companies are attacked via their suppliers. These may include small companies with little protection. Attacks may be made via connections to IoT or OT devices with insufficient protection owned by these companies.

Economic models estimating costs and benefits are made with the purpose of finding the optimum investment level for cybersecurity. Most of these models use security level as an aggregated economic variable [16]). Thus, the models provide little guidance in the kinds of security products, which are the most attractive to invest in.

The research topic cybercrime includes mainly estimation of costs incurred in companies attacked and economic consequences at meso- or macrolevels. This relate to the budgeting, as it relates to estimation of benefits to be achieved by investing in cybersecurity. The economics of the cybercriminals and their business models seem to be a different topic, which is excluded from the framework provided by [16]. The economics of cybercriminals is however important for a study on the economics of cybersecurity, as the key aim of cybersecurity products is to make current business models for cybercrime unviable and prevent creation of new viable business models. Research in this topic, which is truly interdisciplinary as technical and economic analysis needs to be combined, seems to be published primarily in engineering fora.

5. Categorization of Cybersecurity Products

Cybersecurity products include a wide range of activities carried out with the purpose of protecting an organization against cybercrime. The National Institute of Standards and Technology at the U.S. Department of Commerce (NIST) has developed a framework for what to be done in order to be protected [29]. This framework is also used in Europe, where ISO has developed international standards (ISO 27001 and ISO 27002) based on the same principles. The framework includes five core functions, which should be addressed:

- Identify includes identification of the critical processes and resources. This includes all kinds of IT and IoT devices, software, and data. Especially sensitive data, for instance personal information, and data critical to the operations of the company should be included. Moreover, roles and responsibilities for employees, vendors, and others with access to sensitive data must be identified.
- Protect includes protection of the facilities and sensitive data identified above. Some protection is built into the standard software applied by companies. Still many security measures in particular organization and human measures are up to the individual organization to implement. Email filters with blacklisting or even whitelisting can help to avoid phishing and emails with harmful content to be opened, but awareness of employees is even more important in this respect. Moreover, access to any system should be restricted as much as possible.
- Detect includes detection of cybersecurity attacks. IT systems must be monitored in order to detect any cybersecurity events as early as possible. This includes unauthorized access and unusual traffic patterns.
- Respond includes guidelines for how to react if a cybersecurity attack is detected. and how to limit damages. An early response from the user of an infected machine may prevent potential damages to be spread to other parts of the IT system itself, as well as damages in of facilities hosted by trading partners or elsewhere. Trading partners and authorities should be informed about cybersecurity event.
- Recover includes guidelines for reestablishment of damages made in an attack, and reestablishment of data, systems, and business processes.

Cybersecurity as a product possesses some obvious positive external effects, as it is stated in most papers dealing with economics of cybersecurity. However, when looking at the different kinds of cybersecurity measures an organization can invest in, it follows that only a few of them possess notable externalities or spill-over effects, which relate to protection of other actors. These effects are in particular related to protection of facilities and detection of attacks, and concerns attacks of other organizations for instance through dissemination of malware.

In addition to these effects, substantial externalities may be related to possible interruptions in operations. This is a key issue for public utilities, for other public services, and even some private companies. Interruption in service delivery may be caused by many different kinds of incidents of which cybersecurity is only one.

6. The Market for Cybercrime

Looking at the market for cybercrime, it is important to distinguish between different types of hackers and their motives. Hackers are not always criminals looking for profit. Hackers can also be motivated by curiosity, recognition or revenge. Many papers on cybersecurity provides definition of the types of hackers and their motivations. [30] provides an extensive overview of the different definitions and suggests a categorization with 15 different types of hackers. In this context, the key issue is whether a hacker attacks a specific company or if they attack any company, which is vulnerable for a cyberattack. Moreover, it is also important, whether the attack harms other parties. If some strategic information is stolen from a specific company, it will probably only harm the specific company and the externalities are limited. However, if financial information on banking customers is stolen, e.g. from a financial institution, this will affect many different actors outside the company.

Hackers are using a wide range of methods to attack companies, and the economic characteristics of cybersecurity depend on the kinds of attacks.

The European Union Agency for Cybersecurity, ENISA has in a report identified the following prime threats [31]:

- ransomware,
- malware,
- crypto jacking,
- e-mail related threats,
- threats against data leaks,
- threats against availability and integrity,
- disinformation – misinformation,
- non-malicious threats.

Ransomware is reported to be the most important thread, here attackers encrypt an organization's data and demand payment to restore access. If ransom money a paid, this may encourage similar attacks on other companies. Malware "intended to perform an unauthorized process that will have an adverse impact on the confidentiality, integrity, or availability of a system" [31]. Malware is also considered to be a prime threat. Malware can be spread from one company to another and this is the primary policy argument for implementing regulatory measures in order to ensure cybersecurity.

Crypto jacking where criminals steal computing power to generate cryptocurrency can hit any owner of a computer. An increase in this type of cybersecurity breach has been observed, but it will only harm the computer infected.

E-mail related threats are reported to be increasing in spite of educational campaigns to increase awareness. Infected e-mails and phishing e-mails can be sent to anybody, but in organizations with less formal procedures for data-handling and updating of filters are the most vulnerable. ISPs and other service providers can protect their customers through installation of various filters. The threat of leaks of sensitive data depends on the kind of data. Leaks of data belonging to companies or private persons imply spill-over effects on other actors, and this is one of the arguments for having rules on protection of personal data.

Availability and integrity of data can be compromised in different ways, of which denial of service and web-based attacks are the most important. According to ENISA, this threat ranks high. Here, the spill-over effects are important, as this kind of attacks involve the use of a botnet using infected devices connected to the Internet such as IoTs. The availability of unprotected devices is therefore a threat also for other actors. Disinformation and misinformation delivered through social media is on the rise. Non-malicious threats include threats, where the malicious intent is not apparent. These do not originate from cyber criminals or other types of hackers but are mostly based on human errors or misconfigurations. These issues go beyond the scope of this paper.

7. Conclusion

A decomposition of cybersecurity in IoT and OT devices into its different components reveals the kinds of externalities and spill-over effects that relate to cybersecurity. In this way the analysis can contribute to identification of regulatory needs and design of the right regulatory measures to be implemented.

Some externalities are caused by the specificities of the concept of cybersecurity, while others are more generic in nature. The latter ones relate to two different kinds of impacts:

- Payment of ransom money may encourage cybercriminals to continue their activities and help funding of investments in developing new tools for cyberattacks.
- Cyberattacks may lead to discontinuation of operations of the company subject to attack. If the target has been a critical infrastructure, this may have severe consequences also for other actors.

These two externalities are not related to a specific technology or a method applied by cybercriminals only to the outcome of the attack. Other kinds of impacts are more specific and depends on the kinds of attack:

- An organization may be possession of information, which is sensitive to other actors. Most important in this regard is personal information of private customers. In this case the costs of intrusion by cybercriminals may not be borne by the organization itself, but by their customers. This externality relates to information security, which overlaps with cybersecurity, and is addressed by privacy regulation, e.g. GDPR.
- Malware can be spread from one organization to another, if not properly protected. Therefore, there is a common interest in having a minimum level of protection in all devices connected to the Internet. This includes IoTs and networks operated by SMEs or private citizens.
- A special version of this is DDoS, where cybercriminals utilize their control of a large number of infected devices to create overload on specific systems. As discussed in this paper IoT and OT devices are often used for this type of attacks.
- Another variation is supply-chain attacks, where a business partner with a vulnerable network is used as a gateway for infecting well-protected systems.
- ISPs play a special role in this context, as they can offer improved protection to their customers. Thus, there are spill-over effects from one type of actors to another. This may be an argument for regulation if the market cannot provide the right incentives, for instance by having cybersecurity defined as a parameter for competition.

Finally, it should be noted that cybersecurity includes organizational as well as human factors in addition to technology. For instance, creation of awareness is a key tool when fighting against fishing. In this case information campaigns may be more efficient than regulation.

References

[1] PricewaterhouseCoopers, "PwC's Global Economic Crime and Fraud Survey 2022", *PricewaterhouseCoopers*, 2022 (https://www.pwc.com/gx/en/services/forensics/economic-crime-survey/2022.html).

[2] World Economic Forum, "Global Risk Report 2024", World Economic Forum, 2024 (https://www.weforum.org/publications/global-risks-report-2024/in-full/).

[3] European Commission, "Joint Communication to the European Parliament and The Council: The EU's Cybersecurity Strategy for the Digital Decade, JOIN (2020) 18 final", Brussels, 2020.

[4] European Commission, "NIS2 Directive", Brussels, 2020.

[5] European Commission, "EU Cyber Resilience Act, Shaping Europe's Digital Future", Brussels, 2022.

[6] M.M. Noor and W.H. Hassan, "Current Research on Internet of Things (IoT) Security: A Survey", *Computer Networks*, vol. 148, pp. 283–294, 2019 (https://doi.org/10.1016/j.comnet.2018.11.025).

[7] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures", *10th International Conference for Internet Technology and Secured Transactions (ICIT)*, London, UK, 2015 (https://doi.org/10.1109/ICITST.2015.7412116).

[8] W.A. Conklin, "IT vs. OT Security: A Time to Consider a Change in CIA to Include Resilience", *49th Hawaii International Conference on System Sciences (HICSS)*, Koloa, USA, 2016 (https://doi.org/10.1109/HICSS.2016.331).

[9] I. Brown, "The Economics of Privacy, Data Protection and Surveillance", in: *Handbook on the Economics of the Internet*, Edward Elgar Publishing, pp. 247–261, 2016 (https://doi.org/10.4337/9780857939852.00020).

[10] H. Asghari, M. van Eeten, and J.M. Bauer, "Economics of Cybersecurity", in: *Handbook on the Economics of the Internet*, Edward Elgar Publishing, pp. 262–287, 2016 (https://doi.org/10.4337/9780857939852.00021).

[11] A. Odlyzko, "Cybersecurity is Not Very Important", *Ubiquity*, pp. 1–23, 2019 (https://doi.org/10.1145/3333611).

[12] J.P. Anderson, "Computer Security Technology Planning Study", Technical Report for USAF, 1972.

[13] R. von Solms and J. van Niekerk, "From Information Security to Cyber Security", *Computer and Security*, vol. 38, pp. 97–102, 2013 (https://doi.org/10.1016/j.cose.2013.04.004).

[14] J. van der Ham, "Toward a Better Understanding of 'Cybersecurity'", *Digital Threats: Research and Practice*, vol. 2, pp. 1–3, 2021 (https://doi.org/10.1145/3442445).

[15] M.G. Cains *et al.*, "Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context Using Expert Elicitation", *Risk Analysis*, vol. 42, pp. 1643–1669, 2022 (https://doi.org/10.1111/risa.13687).

[16] M. Kianpour, S. Kowalski, and H. Øverby, "Systematically Understanding Cybersecurity Economics: A Survey", *Sustainability*, vol. 13, art. no. 13677, 2021 (https://doi.org/10.3390/su132413677).

[17] A. Sarri, V. Paggio, and G. Bafoutsou, "Cybersecurity for SMEs - Challenges and Recommendations", European Union Agency for Cybersecurity (ENISA), Heraklion, Greece, 2021.

[18] P. Radanliev *et al.*, "Future Developments in Standardisation of Cyber Risk in the Internet of Things (IoT)", *SN Applied Sciences*, vol. 2, art. no. 169, 2020 (https://doi.org/10.1007/s42452-019-1931-0).

[19] I. Brass *et al.*, "Standardising a Moving Target: The Development and Evolution of IoT Security Standards", *Living in the Internet of Things: Cybersecurity of the IoT*, London, UK, 2018 (https://doi.org/10.1049/cp.2018.0024).

[20] S. Ghosh and S. Sampalli, "A survey of security in SCADA networks: Current issues and future challenges", *IEEE Access*, vol. 7, pp. 135812–135831, 2019 (https://doi.org/10.1109/ACCESS.2019.2926441).

[21] V.M. Igure, S.A. Laughter, and R.D. Williams "Security Issues in SCADA Networks", *Computers and Security*, vol. 25, pp. 498–506, 2006 (https://doi.org/10.1016/j.cose.2006.03.001).

[22] E. Schiller *et al.*, "Landscape of IoT Security", *Computer Science Review*, vol. 44, art. no. 100467, 2022 (https://doi.org/10.1016/j.cosrev.2022.100467).

[23] R. Alkhadra, J. Abuzaid, M. AlShammari, and N. Mohammad, "Solar Winds Hack: In-depth Analysis and Countermeasures", *12th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, Kharagpur, India, 2021 (https://doi.org/10.1109/ICCCNT51525.2021.9579611).

[24] M. Willett, "Lessons of the SolarWinds Hack", *Survival. Global Politics and Strategy*, vol. 63, pp. 7–26, 2021 (https://doi.org/10.1080/00396338.2021.1906001).

[25] M. Al-Hawawreh, E. Sitnikova, and N. Aboutorab, "Asynchronous Peer-to-peer Federated Capability-based Targeted Ransomware Detection Model for Industrial IoT", *IEEE Access*, vol. 9, pp. 148738–148755, 2021 (https://doi.org/10.1109/ACCESS.2021.3124634).

[26] R. Vishwakarma and A.K. Jain, "A Survey of DDoS Attacking Techniques and Defence Mechanisms in the IoT Network", *Telecommunication Systems*, vol. 73, pp. 3–25, 2020 (https://doi.org/10.1007/s11235-019-00599-z).

[27] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IoT Privacy and Security: Challenges and Solutions", *Applied Sciences*,

vol. 10, art. no. 4102, 2020 (https://doi.org/10.3390/app10124102).

[28] J.M. Bauer and M.J. van Eeten, "Cybersecurity: Stakeholder Incentives, Externalities, and Policy Options", *Telecommunications Policy*, vol. 33, pp. 706–719, 2009 (https://doi.org/10.1016/j.telpol.2009.09.001).

[29] M.P. Barrett, "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1", NIST, 2018.

[30] S. Chng, H.Y. Lu, A. Kumar, and D. Yau, "Hacker Types, Motivations and Strategies: A Comprehensive Framework", *Computers in Human Behavior Reports*, vol. 5, art. no. 100167, 2022 (https://doi.org/10.1016/j.chbr.2022.100167).

[31] ENISA, "ENISA Threat Landscape 2021", 2021 (https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021).

Morten Falch, Ph.D., Assoc. Professor
Department of Electric Engineering
https://orcid.org/0000-0002-2649-215X
E-mail: falch@es.aau.dk
Aalborg University, Copenhagen, Denmark
https://www.en.aau.dk

Reza Tadayoni, Ph.D., Assoc. Professor
Department of Electric Engineering
https://orcid.org/0000-0003-2217-0919
E-mail: reza@es.aau.dk
Aalborg University, Copenhagen, Denmark
https://www.en.aau.dk