Economic Perspective of Cybersecurity: Principles and Strategies

Fei Xu[1] and Jing Xu[2(✉)]

[1] China Center for International Economic Exchanges, CCIEE, Beijing, China
[2] Beijing University of Science and Technology, Beijing, China
xj2018@ustb.edu.cn

Abstract. An economic perspective is essential but often neglected for understanding the state of cybersecurity, especially when security is increasingly viewed as a matter of national security. Analyze and learn the core economic principles of cybersecurity can help interpret many security phenomena and various challenges we are facing, as well as help to improve cybersecurity industry moving forward. In this paper, we will outline in greater detail the economic characteristics and principles plaguing cybersecurity: Invisibility of benefits, Trade-offs between security and other values, Asymmetries of defend and attack, Dynamic and uncertainty situations, social gains and losses. Then we discuss the pros and cons of the strategies that commonly used now to overcome these economic barriers in the cybersecurity context. Finally, we make several actionable policy recommendations for policy changes and market directions to improve cybersecurity.

Keywords: Cybersecurity · Economic · Public goods · Government intervention

1 Introduction

Today, our dependence on inter-networked computing systems means that virtually every move of daily life—whether personal or commercial, public or private, civilian or military—is intermediated by computer systems. But none of these systems are trustworthy and many are actively under real-time attack today [1]. Cyber threats are escalating in frequency, impact and sophistication [2]. Persistent and increasingly sophisticated malicious cyber campaigns are threatening the public sector, the private sector, and ultimately people's security and privacy [3]. While efforts and investment to improve cybersecurity continue to grow, security developments lag behind the pace of the malicious use of digital technologies. Although all parties are aware of the seriousness of the cybersecurity problem, it remains far from resolved.

Cybersecurity comes with the application of information technology. 'Cyber' is a constitutive elements of information societies, it is interwoven with the physical, economic, social and political elements, and its security it is essential to foster societal development, technological progress [4]. It is impossible to consider cybersecurity without information technology, and it is impossible to consider cybersecurity without the specific scenarios of information application. Cybersecurity has been considered as a

C. Su and K. Sakurai (Eds.): SciSec 2022 Workshops, CCIS 1680, pp. 119–130, 2022.
https://doi.org/10.1007/978-981-19-7769-5_9

very complex social issue, which integrates both science technology, sociology and jurisprudence.

There have been many discussions about the inherent nature of security itself and the characteristics. An economic perspective is essential for understanding the state of cybersecurity, especially when security is increasingly viewed as a matter of public and national security. However, most of the cybersecurity economic research is conducted from a microeconomic perspective. Many studies [5, 6] aiming to provide effective analytical models and frameworks for Cybersecurity Economics and Analysis (CEA), help to increase the economic and financial viability, effectiveness and value generation of cybersecurity solutions for organization's strategic, tactical and operational imperative. We will analyze cybersecurity from a macroeconomic perspective and agree with the idea that cybersecurity qualifies as "public affair", with can be better improved by government intervention and more participation of the public.

In this paper, we will outline in greater detail the economic characteristics and principles plaguing cybersecurity in the next section. Then we discuss the pros and cons of the strategies that commonly used for cybersecurity in Sect. 3. We make several principal policy recommendations for policy changes and market directions to improve cybersecurity in Sect. 4. Finally, we conclude this paper and give out future works in Sect. 5.

2 Economic Principles of Cybersecurity

Admittedly, cybersecurity investment has become an increasingly complex one, since information systems are typically subject to frequent attacks, whose arrival and impact fluctuate stochastically. Decisions are often made with imperfect knowledge, threats are persistent and adaptive, and rapidly changing technology is the norm. Methods to measure economic return in the cybersecurity domain are in their infancy. We now discuss the basic characteristics of cybersecurity from an economic perspective to better understand the causes of those dilemmas.

2.1 Invisibility of Benefits

Investment in cybersecurity is an important financial and operational decision for both governmental agencies and private enterprise. Typical business and government investments aim to create value or improve productivity, whereas cybersecurity investments aim to minimize loss incurred by cyber threats. As a result, cybersecurity is a market of insufficient motivation for investors inherently. To make things worse, due to the uncertainty of threats, the benefits of investing in cybersecurity is almost invisible. Which makes the efficiency and effectiveness of security investments can often be hardly determined due to the invisibility of their benefits.

When implementing IT-security measures, the predicted outcome, e.g. prevented losses, is uncertain in two ways. First of all, it is not certain that one measure and the corresponding investment will prevent a certain risk to occur in the future unless the risk turns out to be damages. Second, the seriousness and damage of the prevented incident is hard to calculate. People have difficulty reasoning about extremely low-probability

events. Estimating the likelihood of a certain type of cyber attack is extremely uncertain and depends on unquantifiable psychological factors like dissuasion and deterrence. Were there some ways to analyze a system mechanically and obtain a quantity that indicates just how secure that system is, then we could have a basis for assessing what is gained from specific investments made in support of cybersecurity. But effective cybersecurity metrics do not exist even today. Quantities derived entirely from empirical observations also don't work for justifying investments. The absence of detected system compromises could indicate that investments in defenses worked, attacks haven't been attempted, or the compromise escaped notice. So whether or not prior security investments were well targeted is impossible to know, leaving security professionals to justify investments based solely on non-events.

Even if an organization already decided to invest in cybersecurity, the uncertainty of threats and invisibility of benefits makes it very hard to choose which type of security products and services to buy. They may not even be able to fully understand their organization's specific security demand, which makes demand-driven technology innovation and industrial development impossible. It is just not possible whether we want or not.

2.2 Trade-off Between Security and Other Values

Cybersecurity, like security in so many other contexts, involves tradeoffs with other values [10]. A tradeoff is a situation that involves losing one quality or aspect of something in return for gaining another quality or aspect. Conflicts is common and will have to be considered and resolved between public cybersecurity and other values or interests of specific individuals, entities, and society at large.

First of all, there is the trade-off between security and efficiency. Security is not perfect. There is a trade-off between ensuring system efficiency and improving cyber security. There is a natural tension between efficiency and resilience in the design of IT systems. Implementation of security products and methods consumes the resources of the system. Each system working with an optimal level of insecurity, where the benefits of efficient operation outweigh any reductions in risk brought about by additional security measures. Reconciling short-term incentives to reduce operating costs with long-term interest in reducing vulnerability is hard. Worse still, the party making the security-efficiency trade-off is not the one who loses out when attacks occur in most of the situations.

Second, there is the trade-off between security and individual rights. Surveillance of network traffic and online identity could be a powerful potential source of information about certain attacks and vulnerabilities. However, surveillance raises massive privacy concerns. There may be trade-offs: societal values as well as potential benefits for the collective versus constraints on activities by individuals and business. Systems' resilience hinges on a delicate trade-off between security and individual human rights. It poses serious risks of undermining and breaching users' privacy, users' exposure to extra risks, should data confidentiality be breached, and may have a mass-surveillance effect.

There are other trade-offs, such as security and technical innovation, etc. Even faced with so many trade-offs, there are really not much metrics and mechanisms suitable and be able for measuring them. Which makes the trade-off decision even more difficult, even if not possible.

2.3 Asymmetries of Attack and Defend

Cybersecurity is a confrontation between the attacker and defender which demonstrate a clear asymmetry characteristic. In the process of network attack and defense, the attacking party constantly innovates and always occupies the initiative in the confrontation process, while the defender falls into a passive situation of being tired of coping. The deterministic and static nature of the traditional network gives the attacker the advantage of time and space, and can repeatedly probe and analyze the vulnerability of the target system and conduct penetration tests, even social engineering, and then find a breakthrough path. The similarity of traditional networks and software structures gives attackers an advantage in attack costs, and the same attack methods can be applied to a large number of similar targets.

Defenders are reactive, attackers are proactive. Defenders must defend all places at all times, against all possible attacks, including those not known about by the defender; attackers need only find one vulnerability and one path. Also, they have the luxury of inventing and testing new attacks in private as well as selecting the place and time of attack at their convenience. New defenses are expensive, new attacks are cheap. Defenders have significant investments in their approaches and business models, while attackers have minimal sunk costs and thus can be quite agile. Besides, defenses can't be measured, but attacks can. Since we cannot currently measure how a given security technology or approach reduces risk from attack, there are few strong competitive pressures to improve these technical qualities. So vendors frequently compete on the basis of ancillary factors (e.g., speed, integration, brand development, etc.). Attackers can directly measure their return-on-investment and are strongly incentivized to improve their offerings.

Cyber spaces are consisting of virtual, agile, flexible, but brittle systems. This brittleness favors offence over defense, explaining in part the continued growth of cyber threats and the escalation of their impact. The more digital technologies become pervasive, the wider becomes the surface of attacks, and with it also number of successful attacks grows.

2.4 Dynamic and Uncertainty Situations

Information technology is evolving at a fast speed than we can imagine. Software development is inherently buggy, not to mention those fully functional complicated applications and platforms. Even responsible software companies that rigorously test for weaknesses couldn't find them all before a product ships. To expect all software to ship free of vulnerabilities is not realistic. For systems that incorporate humans as users and operators, we would need some way to prevent social engineering and intentional insider-malfeasance.

Also, the ability to attack will continue to increase along the time. We don't know which breaking technique will come out next minutes. Whenever new technology is introduced, it has the potential to change the system risks organizations face. The nature of risk and resulting harms is such that they can propagate through systems and supply chains. For example, quantum computing has been hailed as one of the next big revolutions. It is not just faster than traditional computing methods, but a fundamentally

different approach to solve seemingly intractable problems. The mathematical operations that most traditional cryptographic algorithms rely on could be cracked with a sufficiently strong quantum computer [7].

Furthermore, cybersecurity measures and improvements, such as patches, become available at random points in time making investment decisions even more challenging [4]. Results indicate that greater uncertainty over the cost of cybersecurity attacks raises the value of an embedded option to invest in cybersecurity. Knowing that countermeasures effective against today's threats can be ineffective tomorrow, decision-makers need agile ways to assess the efficacies of investments in cybersecurity on assuring mission outcomes. Individuals and entities therefore can neither fully reap the benefit of their security investment nor entirely control their vulnerability through investments because of those dynamic and uncertainties [8].

2.5 Social Gains and Losses

The information technology sector already became a significant economic force. Computing, network and digitalization changed how people shopped, worked, communicated and socialized, greatly improved social efficiencies and the social value created is immeasurable. For instance, companies operating critical infrastructures have integrated control systems with the Internet to reduce near-term, measurable costs. Electricity companies have realized substantial efficiency gains by upgrading their control systems to run on the same IP infrastructure as their IT networks. Unfortunately, these changes in architecture leave systems more vulnerable to failures and attacks, and it is society that suffers most if an outage occurs. The control systems regulating power plants and chemical refineries are vulnerable to cyberattack, yet very little investment has been made to protect against these threats. While those raising the risk of catastrophic failure, whose losses will be primarily borne by society.

For example, a single compromised system anywhere in a network can serve as a launching point for attacks on other systems connected to that network. So local investment in defenses not only provides local benefits but also benefits others; and under-investment in defenses elsewhere in the network could facilitate local harms [9]. The society, organizations and individuals are enjoying the benefits of information technology, but neither party is willing to take responsibility of cybersecurity accordingly. Unfortunately, such a misalignment is inevitable for many information security decisions.

The lack of effective cybersecurity measures has a potential knock-on effect on the information revolution, and on the development of information societies around the globe. Its security it is essential to foster societal development, technological progress and also to harness the potential of digital technologies to deliver socially good outcomes.

3 Common Strategies for Cybersecurity

3.1 Laws and Regulations

Dan Assaf argues for greater government responsibility, saying that computer security is a public good. Since there's inadequate incentive for industry to fight cybercrime,

perhaps there's a place for public action. In addition, national security today requires secure cyberinfrastructure; the absence of physical borders to defend makes the problem worse, not easier. Since only the government have the required capacity to deal with the sophisticated cybersecurity. What might government do?

Law could force system producers and/or purchasers to make the necessary investments on security. There are a host of laws and regulations directly and indirectly govern the various cybersecurity requirements for any given business. For example, the Federal Laws, Federal Regulations & Guidance, the State Laws, and International Laws for cybersecurity.

There are other cybersecurity frameworks that are not codified in law but rather are created and/or enforced by non-governmental entities. For example, the NIST or ISO 27001 cybersecurity frameworks are both widely used standards in many industries and government organizations [20]. Companies might be required to comply with these frameworks by industry dynamics or by organizational partnerships with government or other entities.

Government can also participate in standards—Regulation and liability. The adoption of mandatory standards can be seen as a way to support security. Some standards directly concern what functions an artifact must or must not support, some govern its internal structure, while others concern the process by which the artifact is constructed or maintained, and yet others govern qualifications of the personnel who are involved in creating the artifact. as well as security provisions in information privacy laws. Current market activity suggests that such mandates show value in some areas.

We could certainly use more research, especially on defense techniques. However, government agencies often limited their investments to problems with a short-term horizon. The number of projects supported is relatively small and the funding is often through special one time initiatives.

3.2 Industry Incentives

The cybersecurity market is expanding rapidly in recent years. It surpassed $150 billion in 2019 and is expected to exceed $400 billion and grow at over 15% Compound Annual Growth Rate (CAGR) between 2020 and 2026 [11]. The spike in the cybersecurity market is being seen in all parts of the world. Given the practical difficulties of teaching non-technical users and application sections the principles of adequate security, the logical plan should be to shift the cost to the industries that can do something about it. They might be encouraged to improve security via commercial pressure, regulation, or tort lawsuits. While the demand for cybersecurity is growing across the world, the market is getting increasingly competitive as new cybersecurity products launch, and more major providers form partnerships.

Deloitte reports that financial services companies spend 6 to 7 percent of their IT budget on security, but this is far from sufficient. Many companies probably still think that building in security is either too expensive or too inconvenient for users. Small companies might lack the resources to do security well [5]. Although the industry prefers neither regulation nor liability. Regulation tends to be slow to change, which poses difficulty in a rapidly changing world. Liability causes people to try to evade it and runs a risk that

in the end the responsible party won't be able to pay damages. There is still the need for incentives to help accelerate the growing of cybersecurity market.

Aspects of industry incentives for cybersecurity may include: Cybersecurity Insurance, Grants, Process Preference, Liability Limitation, Streamline Regulations, Public Recognition and Cybersecurity Research, etc. It is important for the industry to promote cybersecurity practices and develop core security capabilities.

3.3 Technology Innovation

Confronted by a problem born of technology, the main focus of cybersecurity doctrine is on developing new detection and defense technologies at the beginning and still now. Government funded organizations and Scientists are investing heavily in technological means for improving cybersecurity. Intuitively this is the right and straight forward way to find the solution. However, Improved technology itself may not be able to solve problems that technology has created. Cybersecurity encompasses a wide set of practices, from risk assessment and penetration tests; disaster recovery; cryptography; access control and surveillance; architecture, software, and network security; to hack-back and security operations, and physical security. Each of these practices requires different techniques, which makes technology innovation even difficult.

Unfortunately, research in cybersecurity is not enough, and has been hamstrung on multiple fronts, therefore, has not been able to develop a much-needed science base to anchor cybersecurity innovations, nor has it been able to produce the range of solutions we require.

Despite the growing value of the cybersecurity market and the increasing efforts of companies and state actors to invest in technical innovation to improve the security of information systems and infrastructures, data on number and impact of cyber-attacks is still escalating. We can learn that technology innovation itself is inadequate to frame and govern cybersecurity.

4 Recommendations for Cybersecurity

4.1 Public Cybersecurity Doctrine

Cybersecurity comes along with information techniques. It is natural to consider cybersecurity as a technical problem and hopefully can be solved by developing security products. Cybersecurity is technical and business problem that has been presented as such in boardrooms for years. As cyberthreats becomes more sever and casing more significant damages, scholars and regulators began to think about the nature of cybersecurity, the cybersecurity doctrine.

Savage and Schneider discussed security is not a commodity in their work [1]. They pointed out that unlike computer and communications hardware and software, security is nota commodity.It cannot be scaled simply by doing more.In this respect, there is a mounting consensus on treating cybersecurity as a public good to be managed in the public interest. The management of a public good requires considering direct and indirect externalities, as well as medium and long-term consequences. This favor approaches

to cybersecurity that focus on interdependencies among the security of different, but connected, technologies, their impact on the context of deployment and on the relevant public interest at stake.

Enhanced levels of cybersecurity can entail tensions involving cost, function, convenience, and societal values such as openness, privacy, freedom of expression, and innovation. Management of cybersecurity as a public good call for collaboration between the private and the public sectors to ensure that systems' robustness is designed to meet the public interest. It is up to the public sector to set standards, certification and testing and verification procedures capable of ensuring that a sufficient level of security is maintained. At the same time, the private sector bears responsibility for designing robust systems and developing and improving new cybersecurity methods for the services and products they offer, as well as for collaborating with the public sector around controlling and testing mechanisms. Envisaging systems' robustness as a public good also places some responsibility on the user in terms of their cyber hygiene practices.

4.2 Facing the "Right" Threats

Cyber threats are constantly changing and evolving with the development of information technology. For example, the frequency of identified Advanced Persistent Threats (APTs) has greatly increased recent years. APT's number one target were always organizations with high value assets and that's always the reason why those attacks are so persistent. In order to protect against this kind of threats, it is very important to understand the reasons and motivations behind these threats. Security is a trade-off, there is no perfect security. Since cybersecurity investments involve decision-making under uncertainty, it is more reasonable to think in terms of deploying defense as appropriate to the threat and to the value of what's being protected. We can't succeed by focusing our defenses on past attacks, and we must move from a reactive stance to a proactive one.

In addition to this, the range and scope of cyber-attacks create the need for organizations to prioritize the manner in which they defend themselves. With this in mind, each organization needs to consider the threats that they are most at risk from and act in such a way so as to reduce the vulnerability across as many relevant weaknesses as possible. So, based on the evaluation of the organization value itself, and understanding the different motivations of cyber threats, facing the right threats is very important. It is needed to define some agreed upon kinds and levels of cybersecurity, characterizing who is to be secured, at what costs (monetary, technical, convenience, and societal values), and against what kinds of threats. The goals might be absolute or they might specify a range of permissible trade-offs.

Basically, the defense of cybersecurity for an organization needs to be based on regulation compliance as the basic requirement of the passing line, and a high-line evaluation mechanism driven by the threat situation. At the same time, while information service provider is responsible for the security of their systems, it is needed for the government to provide the required techniques and supports for the service provider when facing extremely complicated threats, especially those well-organized and weaponized threats.

4.3 Reallocation of Responsibilities and Liabilities

One of the most significant characteristics of cybersecurity is ambiguous accountability. There are also capability gaps between the current cybersecurity approaches and defending ourselves against evolving threats. Investment incentives are missing when costs are borne by third parties, materialize only well after the breach occurs, and causation is difficult to discern much less prove.

In order to solve the problems of growing vulnerability and increasing cyber threats, policy and legislation must coherently allocate responsibilities and liabilities so that the parties in a position to fix problems have an incentive and ability to do so. In many circumstances cyber risks are allocated poorly. For example, it is very common now that the organizations that defend cybersecurity do not bear the full costs of failure. Also, it is unlikely that either vendors or users, left to their own devices, will solve the problems. Government must set the rules of the game; We can't rely on unintelligible and unread end user license agreements to be responsible for security breaches any more.

Enterprises should be fully responsible for their own security, bear most of the responsibility for their own security and the social governance security supported by themselves, and bear part of the responsibility for their own security and the public/national security associated with themselves. And to some point, defense of its citizens is a clear responsibility of government. Because in essence, responsibility is not simply a stipulation, responsibility means technical capabilities and the ability to invest. Those abilities are carried by the implementation of large projects, advanced technologies and products, and sophisticated teams. Cybersecurity for the State and public society is not something that can be achieved with enterprise-level investments, nor is it achieved through individual effort. It is not enough to only have the public attention or regulatory requirements. Reasonable reallocation of responsibilities and liabilities is the fundamental and starting point for ensuring cybersecurity.

4.4 Government Intervention and Policies

Conflicts and trade-offs will have to be resolved between public cybersecurity and other values or interests of specific individuals, entities, and society at large. This requires the government to make the overall adjustments due to the political nature of cybersecurity. Government policy interventions are required that incentivize responsibility allocation, accountability and collaboration on the part of both individuals, organizations and governments. Also, policy that incentivizes higher standards of care in regulation, technology and service delivery is needed.

Various government agencies themselves perform research and development, incident response, and forensic analysis in cybersecurity in many countries around the world. Although government funded projects seems to need massive financial investments, this is not a simple economic gain, but also involves political gain, and industrial driven gain. Yet it is difficult to calibrate the right nature and scale of investment in cybersecurity. Government leadership need to develop a set of policy actions that incentivize take-up of security solutions and that underpin greater trust and transparency between different components of the ecosystem. Possible solutions may include: government giving more finical support, clarifying issues of liability, reducing friction in current assurance and

regulatory models, and addressing the security of new technology, invention and application scenarios changes. Clearly, some additional funding by the state is needed to help the state build a more effective, dynamic and elastic defense mechanism.

Besides, Government also needs to managing cyber risks in the face of the major technology trends taking place in the near future. However, security is not usually being considered as an integral component of technology innovations and as such, proper investment needed to be made into support (knowledge, guidance, research investment) and incentives (market forces, regulation) for developing emerging technologies securely [12].

4.5 Collaboration and Information Sharing

One future feature of cybersecurity is collaboration. The success of industry ISACs is indicative of a greater acceptance of the security community that collaboration is cheaper and more effective means of security than the alternative [13]. For example, NSA Cybersecurity Collaboration Center harnesses the power of industry partnerships to prevent and eradicate foreign cyber threats to National Security Systems [14]. The EU Information Sharing and Analysis Centers (ISACs) foster collaboration between the cybersecurity community in different sectors of the economy [15]. Cybersecurity collaboration also exists between nations. Such as, US-EU collaboration on cybersecurity and joint Statement of Intent Between the U.S. Department of Homeland Security and the Israel National Cyber Directorate [16]. When it comes to tackling these global cyberthreats, working with international partners can have benefits for resilience [17]. Particular attentions need to be taken of the needs of developing countries and the need for collective efforts to reduce cross-border cybercrime.

Cybersecurity defenses should reflect a proactive strategy that leverages from diverse areas of expertise and information. Information Sharing is increasingly important for addressing growing systemic risks. Sharing of information about vulnerabilities of different systems involved in the same supply chain, for example, will become essential for the private sector to guarantee system robustness and learn from peers. At the same time, the public sector may support this practice by including information sharing and collaboration as part of capabilities building initiatives and procedures. These practices can facilitate patching procedures and may reduce the zero-day and exploits market. In turn, this could slow down the cyber arms-race and weaponization dynamics of cyberspace.

Cyber threat information is any information that can help an organization identify, assess, monitor, and respond to cyber threats. Cyber threat information includes indicators of compromise; tactics, techniques, and procedures used by threat actors; suggested actions to detect, contain, or prevent attacks; and the findings from the analyses of incidents. Organizations that share cyber threat information can improve their own security postures as well as those of other organizations [18].

5 Conclusion

Society as a whole do not allocate sufficient attention, researches or resources to cybersecurity. Cybersecurity shows significant economic characteristics. Right understanding

of public cybersecurity doctrine, appropriate architecture design and interventions that consider cybersecurity as a whole system and public affair can significantly improve our cybersecurity posture. Though cybersecurity problem resides in technologies, the solution requires concept changes, policies, interventions and collaboration. We believe that by partially alter the focus of cybersecurity from technical to economical will help to improve it moving forward. Our designed recommendations are to raise awareness to cybersecurity and assign responsibility for action within the society as a whole so that cyber risks to society may be mitigated.

References

1. Savage, S., Schneider, F.B.: Security is not a commodity: the road forward for cybersecurity research: a white paper prepared for the computing community consortium committee of the computing research association. http://cra.org/ccc/resources/ccc-led-whitepapers/
2. Taddeo, M., Bosco, F.: We must treat cybersecurity as a public good. Here's why. World Economic Forum, Centre for Cybersecurity (2019)
3. The White House. Executive Order on Improving the Nation's Cybersecurity (2021). https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
4. Floridi, L.: The Fourth Revolution, How the Infosphere is Reshaping Human Reality. Oxford University Press, Oxford (2014)
5. Moore, T.: Introducing the economics of cybersecurity: principles and policy options. In: Proceedings Workshop Deterring Cyber Attacks: Informing Strategies and Developing Options for US Policy, Nat'l Academies Press (2010). www.cs.brown.edu/courses/csci1950-p/sources/lec27/Moore.pdf
6. Kobayashi, B.H.: An economic analysis of the private and social costs of the provision of cybersecurity and other public security goods. Supreme Court Econ. Rev. **14**, 261–280 (2006)
7. Subramanian, V.: Quantum and the Future of Cryptography. National defense magazine (2021)
8. Chronopoulos, M., Panaousis, E., Grossklags, J.: An options approach to cybersecurity investment. IEEE Access **6**, 12175–12186 (2018)
9. Lesk, M.: Cybersecurity and economics. IEEE Secur. Priv. **9**, 76–79 (2011)
10. Anderson, R., Moore, T.: The economics of information security. Science **314**(5799), 610–613 (2006)
11. Borchart, L.: The cybersecurity market is rapidly growing. highlights from a 2020 global market insights report on the growing cybersecurity market. https://techchannel.com/Trends/03/2021/cybersecurity-market-growing
12. World Economic Forum in collaboration with the University of Oxford. Future Series: Cybersecurity, emerging technology and systemic risk. https://www.weforum.org/reports/future-series-cybersecurity-emerging-technology-and-systemic-risk
13. Nissenbaum, H.: Where computer security meets national security. Ethics Inf. Technol. **7**(2), 61–73 (2005). https://doi.org/10.1007/s10676-005-4582-3
14. Ford, K.: The future of cybersecurity is collaboration. https://www.cybergrx.com/resources/research-and-insights/blog/the-future-of-cybersecurity-is-collaboration
15. NSA Cybersecurity Collaboration Center. National Security Agency/Central Security Service. https://www.nsa.gov/About/Cybersecurity-Collaboration-Center/
16. Cybersecurity Policies. Shaping Europe's digital future. European Commission. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies

17. Joint Statement of Intent Between the U.S. Department of Homeland Security and the Israel National Cyber Directorate. Homeland Security (2022). https://www.dhs.gov/news/2022/03/02/joint-statement-intent-between-us-department-homeland-security-and-israel-national
18. To counter cyber risks to critical sectors such as aviation we need international collaboration. World Economic Forum. https://www.weforum.org/agenda/2021/04/cybersecurity-aviation-international-regulation/
19. Johnson, C., Badger, L., Waltermire, D., Snyder, J., Skorupka, C.: Guide to cyber threat information sharing. NIST Special Publication 800-150
20. Baadsgaard, J.: Cybersecurity Laws & Regulations. https://www.ipohub.org/cybersecurity-laws-regulations/
21. Assaf, D.: Government intervention in information infrastructure protection. In: Goetz, E., Shenoi, S. (eds.) Critical Infrastructure Protection, vol. 253, pp. 29–39. Springer, Heidelberg (2008). https://doi.org/10.1007/978-0-387-75462-8_3