Chapter 1
Introduction and Overview

Marcus M. Keupp

1.1 Next Generation Cyberdefense

Cyber attackers are intentionally violating one or more security objectives an organization has defined for its IT infrastructure or computer networks [31]. By doing so, they inflict significant costs on organizations, businesses, and individuals [7, 10, 15]. While global cybersecurity expenditure grew by 28% from 2015 to 2018, the average cost of cybercrime incidents increased by 73% within the same period [1, 39]. Ransom paid by private firms to hackers is at a historic height. The average cost per data breach for companies was 3.86 million US$ [18]. But cyberattacks also target government organizations and individuals with public exposure, so that state-sponsored hacks, cyber espionage, and cyber sabotage exhibit likewise growth rates [17, 27, 29]. The absolute amount of cyberattacks against private or public organizations has increased by 67% since 2014 and by 11% since 2018 [1]. Investments meant to produce cyberdefense seem to lag attacks, and their effectiveness appears to be limited.

Academic work has trouble finding answers to this problem. In fact, public and private organizations fail so regularly at defending their systems that this failure has become a research object of its own [12]. Over the past three decades, many contributions have proposed technical measures to counter cyberattacks (for an overview, see [38]). However, the success of such technology-based approaches to cyberdefense has been limited, not the least because they ignore the weakest link in the cyberdefense chain—human beings and their fallacies [2, 3, 7]. While numerous models for cyberdefense investment strategies have been developed (e.g., [13, 22, 33]), their significance in the real world is limited due to imperfect information, misaligned incentives, moral hazard, and subjective bias [3, 5, 30].

M. M. Keupp (✉)
Military Academy at the Swiss Federal Institute of Technology Zurich, Birmensdorf, Switzerland
e-mail: mkeupp@ethz.ch

M. M. Keupp (ed.), *Cyberdefense*, International Series in Operations
Research & Management Science 342,
https://doi.org/10.1007/978-3-031-30191-9_1

Why then, one might ask, are organizations so bad at pre-empting, detecting and defending cyberattacks? It appears that contemporary cyberdefense is too slow, lacks technological foresight, and often proves to be ineffective. This book is an attempt to provide answers and applicable analytical tools for all three problems.

1.2 Structure and Overview

1.2.1 Speed

Many cyberattacks are not only successful, but they also go unnoticed for a significant period of time. In 2019, it took companies an average of 230 days to identify security breaches induced by malicious attacks. The average lifecycle of a breach from identification to containment was 280 days [18]. Attackers still have the initiative—the technology landscape is large, and there are many backdoors and zero-day vulnerabilities that can be exploited. Even if all of them would be technologically known, pre-emptively defending all of them by an all-hazard approach may prove to be prohibitively expensive. It is true that many organizations use digital forensics to clarify what has happened once an attack has been finally neutralized, but they are in fact analyzing lost chess games when they do so—players may improve their skills by learning from past mistakes, but they still have to suffer the bitter taste of defeat. A more productive approach should focus on shortening the cyber kill chain as much as possible, and provide fast responses that deny attackers the ability to continue with their attack. Speed is certainly of the essence, so the contributions in the first part of this volume intend to assist defenders with this task.

In Chap. 2, *Gillard et al.* start out with an agent-based model. They investigate how autonomous agents improve their response patterns as they react instantly to exogenous attacks. Moreover, they highlight the role of cooperation and incentive alignment among defenders using a game-theoretic approach, and they show that cooperative defense is both fast and effective.

In industrial control systems, attacks constitute rare events in a stream of permissible commands, and although Pareto or Poisson distributions could be used to model this imbalance, the sheer rareness of exploits makes it hard to attain good accuracy. In Chap. 3, *Su et al.* propose an alternative path. They study how unsupervised clustering algorithms can respond fast to attacks against industrial control systems. They compare the performance of four different algorithms and discuss the implications of their findings for the security of cyber-physical systems.

Both chapters demonstrate how threats can be dynamically captured and dealt with. Note that none of them requires big data analytics, so they should be particularly interesting for operators of SCADA systems which have both security requirements that differ from those of commercial computer networks and low computational capabilities [31].

In Chap. 4, *Fischer and Gillard* discuss novel security information sharing platforms that have recently emerged as an alternative to ISACs. Using a hierarchical simulation model that is informed by real user data from such platforms, they discuss the trade-offs between the value of information units and the speed with which they are shared.

1.2.2 Foresight

As organizations face budget constraints, they must maximize the efficiency of any investment they make in cyber security processes, products, or services [33]. Prior research has produced quantitative models that propose to optimize such investment, and also many recommendations that instruct firms about how to invest in particular technologies or systems (e.g., [16, 34, 41]). However, these models are deeply rooted in microeconomic and behavioral assumptions that need not apply to actual investment problems. Firms must protect their systems today against future attacks. Therefore, investments often lag actual threats since vendors must first commercialize defense technology to market maturity, particularly so if the technology in question is only just emerging. The media report about attacks that have been discovered, but knowledge of past incidents is not necessarily a predictor for future threat vectors. Hence, firms must forecast technological trajectories and prioritize investments accordingly.

Just as contemporary economists attempt to replace static ex-ante predictions with ‘nowcasting’ (e.g., [4, 24]), firms must learn to preempt rather than react to technological developments if they want to neutralize the attacker’s advantage. While traditional forecasting methods and big data analytics are costly in terms of resources and computing power, the contributions in the second half of this book offer parsimonious yet efficient solutions that work with open source data.

In Chap. 5, *Percia David et al.* propose a reproducible, automated, scalable, and free method for bibliometric analysis that requires little computing power and informs managers about the maturity and likely future development of technological domains. They also show how timelines of expert sentiment about these domains can be generated. They illustrate their approach with an analysis of the `arXiv` repository and suggest how even larger databases can inform investment decisions about future cybersecurity technologies.

In Chap. 6, *Mezzetti et al.* propose a novel recursive algorithm that analyzes publicly available data and ranks the relative influence that companies and technologies have in a technology landscape. The results provide investors with an optimal ranking of technologies and thus help them to make more informed decisions about companies and technologies.

In Chap. 7, *Tsesmelis et al.* develop a lean recommender system which predicts emerging technology by a sequential blend of machine learning and network analytics. They illustrate the capabilities of this system with a large-scale patent data analysis and discuss how it can help organizations make more informed decisions.

Since patent data are public and freely available, organizations can obtain objective advice at very little cost.

In Chap. 8, *Aeschlimann et al.* map the landscape of cyberdefense capabilities among public, private and academic organizations in Switzerland. They also study the extent to which these organizations exchange capabilities with each other, and they produce a map of their informal networks. The results suggest that the ecosystem under study is a scale-free network that hosts many but unevenly distributed capabilities. Further, inter-organizational cooperation is limited although opportunities to cooperate exist.

While this contribution focuses on the question of where cyberdefense capabilities are located right now, in the subsequent Chap. 9, *Moreno et al.* show how job offers can be analyzed to predict future capability requirements. Their link prediction approach features a parsimonious algorithm which crawls publicly available job offer databases and predicts which capabilities firms will require up to six months in the future. They compare the efficiency of this method across several unsupervised learning algorithms as well as against a supervised learning method.

1.2.3 Effectiveness

Any investment in cyberdefense is wasted unless it provides organizations with effective protection against attacks. However, all too often effectiveness is confused with ticking off boxes in bureaucratic checklists. Formal certifications and regulatory requirements certify the proper implementation of risk management processes, but not the existence of effective defense [8, 19, 35]). Moreover, 'stress tests' are often limited to penetration testing exercises [9, 36] or bug bounty programs [25]. Moreover, formal performance indicators often fail to capture the effectiveness of cyber defense systems first [14, 32]. The third part of the book therefore explores how organizations realize effective defense.

First, they need to understand how and why attackers act. Therefore, in Chap. 10, *Fischer et al.* discuss the selection problem attackers face when they attempt to exfiltrate information from a computer network: They must identify valuable information units among many irrelevant ones. The authors model such attacks as a repeated urn draw under different distributional patterns and use prospect theory to model risk aversion and overconfidence among attackers. Their findings are particularly relevant to 'silent' attacks and computer network exploitation operations which prefer to gather intelligence over blocking or damaging a system, and they propose a number of measures the defenders can take to thwart attacks.

However, human fallacies also exist among defenders. In Chap. 11, *Baschung et al.* discuss the extent to which there is a principal-agent problem between the individual career goals of corporate security officers and the effectiveness of their investment decisions. The authors develop a recursive model which simulates the complex relationships between investment dynamics, CSO reputation and inter-firm migration, and cyberdefense effectiveness. Using data from real cybersecurity breaches, they find that a positive (negative) dynamic should exist between high (low) CSO reputation and effective corporate protection.

In Chap. 12, *Muhly* discusses how serious gaming can confront defenders with their own overconfidence and thus improve their resilience to social engineering (which is still one of the major threat vectors by which attackers execute cyberattacks). He reports the results of a randomized experiment that modeled a phishing attack and investigates the extent to which serious gaming can be applied as an immunization treatment. The results suggest that participation in serious gaming reduces the probability to be victimized by social engineering attacks. Overconfident and indifferent users are more likely to fall for such attacks, whereas a more pessimistic stance is negatively associated with failure.

In Chap. 13, *Shrivastava and Mathur* propose how virtualized environments can help operators of industrial control systems to detect and respond to anomalies more effectively. However, they also note that effectiveness requires radical architectural adaptations and a departure from IT security models of the past. They argue how and why zero trust architectures and autonomous mechanisms can not only make industrial control systems safer, but also empower machines to respond faster and more accurately to threats and attacks. Ultimately, such developments may enable industrial plants to defend themselves in a fully automated way.

In Chap. 14, *Gillard and Aeschlimann* expand this path. They discuss automated and scalable procedures that can identify and recombine related indicators of compromise which decentral users provide. In particular, these methods allow system operators to identify incidents which may have been running unnoticed but in fact constitute the root of many other anomalies. The authors simulate these procedures and show how users can control them to generate more accurate threat information which increases the effectiveness of their cyberdefense activities.

In the final Chap. 15, *Pangrazzi and Muhly* remind organizations and governments alike that they need not wait for a global cyberdefense regime to emerge until they can effectively defend their systems. The norms that exist in international law today provide users with powerful tools that can contribute to a more effective national cyber defense as well as to international collaboration—provided nation-states master the transformation of these norms into national contexts. The authors highlight four areas where this transformation would yield productive results.

1.3 Outlook: From Defense to Counter-Attack

The era which left cyberdefense to the technicians is over. What Keupp [21] said about the architectural challenges of next generation critical infrastructures also applies to cyberdefense: Technical knowledge alone does not provide an effective defense. Efforts to systematically advance cyber risk management must draw on not only computer science but also fields such as behavioral studies, economics, law, and management science. In particular, interaction with legal scholars is key here [12, 36]. Without such collaboration, legislators will continue to develop reactive measures that run the risk of rapid obsolescence as newer technologies are more widely adopted, and technicians may fail to understand how international law provides them with institutions that can shape effective defense on a global scale. All in all, this volume firmly subscribes to these perspectives and reiterates earlier initiatives which have called for more interdisciplinary work (e.g., [11, 20, 37, 40]) and for the introduction of economic perspectives into IT security [3, 7].

But there is more to next generation cyberdefense than interdisciplinary cooperation. To date, defense is still seen from a passive perspective: With some desperation, defenders take attacks as a natural evil one has to live with and defended against in the best possible way. It is about time to forego this passive stance.

The next challenge is to push for attribution—defenders must begin to identify the technical and physical locations of attackers and hence master attribution, with an eventual view to neutralizing the technical infrastructure from which attacks are carried out. Again, this 'strike back capability' will require interdisciplinary skills: automated defense algorithms could be trained to not only defend, but also to detect where the attack is coming from, economic perspectives can help calculate if the attack is worth the cost of striking back, and legal perspectives can help judge if retaliation conforms to international law.

The Tallinn manuals have tried to develop a perspective in cyberspace that is akin to article 51 of the United Nations charter—a nation that is unlawfully attacked has not only the right to defend itself, but it can use all force necessary to neutralize the aggression, reestablish the status quo, and preserve the integrity of its territory and statehood. This perspective, long established in the international law of warfare and the fundament of the post-WWII peace order, should be expanded to the cyberspace. Defense is therefore not limited to responding to attacks—it can even include striking the aggressor's territory as long as a state of war exists. Once this principle is adapted for the cyberspace, there is no more need to simply tolerate attacks.

Finally, states or state-sponsored parties have begun to use offensive cyber operations to realize military or political goals. For example, `stuxnet` disabled Iranian centrifuges which were enriching uranium, probably the first offensive cyber operation in military history [23]. Russia tried to influence the 2016 U.S. presidential elections by cyber and information operations [28], and China has been using cyber intelligence activities to realize commercial advantages [26]. These attacks constitute a new level of aggression whose damage goes far beyond ordinary cybercrime. Next generation cyberdefense will have to deal with this increased intensity of violence in the cybersphere. Defenders will continue to lead a difficult life, but they have no alternative but to stand their ground in the face of adversity.

References

1. Accenture. (2019). *The cost of cybercrime: Ninth annual cost of cybercrime study*. Accenture Security with Ponemon Institute LLC, Traverse City MI: Research report.
2. Anderson, R. J. (2010). *Security engineering: A guide to building dependable distributed systems*. Wiley.
3. Anderson, R., & Moore, T. (2006). The economics of information security. *Science, 314*(5799), 610–613.
4. Barbaglia, L., Frattarolo, L., Onorante, L., Maria Pericoli, F., Ratto, M., & Tiozzo Pezzoli, L. (2022). Testing big data in a big crisis: Nowcasting under Covid-19. *International Journal of Forecasting*, forthcoming.
5. Baron, J., & Ritov, I. (2004). Omission bias, individual differences, and normality. *Organizational Behavior and Human Decision Processes, 94*(2), 74–85.
6. Beal, B. (2005). IT security: The product vendor landscape. *Network Security, 5*, 9–10.
7. Böhme, R. (2013). *The economics of information security and privacy*. Berlin, Heidelberg: Springer.
8. Böhme, R. (2012). Security audits revisited. In A. D. Keromytis (Ed.), *Financial cryptography and data security* (pp. 129–147). Berlin, Heidelberg: Springer.
9. Böhme, R., & Félegyházi, M. (2010). Optimal information security investment with penetration testing. In T. Alpcan, L. Buttyan, & J. S. Baras (Eds.), *Decision and game theory for security* (pp. 21–37). Berlin, Heidelberg: Springer.
10. Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security, 11*(3), 431–448.
11. Cresson Wood, C. (2004). Why information security is now multidisciplinary, multi-departmental, and multi-organizational in nature. *Computer Fraud & Security, 2004*(1), 16–17.
12. Falco, G., et al. (2019). Cyber risk research impeded by disciplinary barriers. *Science, 366*(6469), 1066–1069.
13. Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). Externalities and the magnitude of cyber security underinvestment by private sector firms: A modification of the Gordon-Loeb model. *Journal of Information Security, 6*(1), 24–30.
14. Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market value of voluntary disclosures concerning information security. *MIS Quarterly, 34*(3), 567–594.
15. Gordon, L. A., Loeb, M. P., Lucyshin, W., & Richardson, R. (2005). CSI/FBI computer crime and security survey. *Computer Security Journal, 21*(3), 1.
16. Herath, H., & Herath, T. (2008). Investments in information security: A real options perspective With Bayesian post-audit. *Journal of Management Information Systems, 25*(3), 337–375.
17. Hunter, L. Y., Albert, C. D., & Garrett, E. (2021). Factors that motivate state-sponsored cyberattacks. *The Cyber Defense Review, 6*(2), 111–128.
18. IBM. (2020). Cost of a data breach report. (2020). *IBM Security*. Armonk NY: IBM Corp.
19. Islam, M. S., Farah, N., & Stafford, T. F. (2018). Factors associated with security/cybersecurity audit by internal audit function: An international study. *Managerial Auditing Journal, 33*(4), 377–409.
20. Kam, H. J., Mattson, T., & Goel, S. (2020). A cross industry study of institutional pressures on organizational effort to raise information security awareness. *Information Systems Frontiers, 22*(5), 1241–1264.
21. Keupp, M. M. (2020). *The security of critical infrastructures* (pp. 1–14). Cham: Springer Nature.
22. Lelarge, M. (2012). Coordination in network security games: A monotone comparative statics approach. *IEEE Journal on Selected Areas in Communications, 30*(11), 2210–2219.
23. Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. *Security Studies, 22*(3), 365–404.
24. Macias, P., Stelmasiak, D., & Szafranek, K. (2022). Nowcasting food inflation with a massive amount of online prices. *International Journal of Forecasting*, forthcoming.

25. Malladi, S., & Subramanian, H. C. (2020). Bug bounty programs for cybersecurity: Practices, issues, and recommendations. *IEEE Software, 37*(1), 31–39.
26. NCSC. (2018). Foreign economic espionage in cyberspace. U.S. National Counterintelligence and Security Center, Washington D.C.: Office of the Director of National Intelligence.
27. OECD. (2012). *Cybersecurity policy making at a turning point: Analysing a new generation of national cybersecurity strategies for the internet economy*. Paris: OECD Publishing.
28. Ohlin, J. D. (2016). Did Russian cyber interference in the 2016 election violate international law? *Texas Law Review, 95*, 1579.
29. Osawa, J. (2017). The escalation of state sponsored cyberattack and national cyber security affairs: Is strategic cyber deterrence the key to solving the problem? *Asia-Pacific Review, 24*(2), 113–131.
30. Patt, A., & Zeckhauser, R. (2000). Action bias and environmental decisions. *Journal of Risk and Uncertainty, 21*(1), 45–72.
31. Pliatsos, D., Sarigiannidis, S., Lagkas, T., & Sarigiannidis, A. (2020). A survey on SCADA systems: Secure protocols, incidents, threats and tactics. *IEEE Communications Surveys and Tutorials, 22*(3), 1942–1976.
32. Purser, S. A. (2004). Improving the ROI of the security management process. *Computers & Security, 23*(7), 542–546.
33. Schatz, D., & Bashroush, R. (2017). Economic valuation for information security investment: A systematic literature review. *Information Systems Frontiers, 19*(5), 1205–1228.
34. Shirtz, D., & Elovici, Y. (2011). Optimizing investment decisions in selecting information security remedies. *Information Management & Computer Security, 19*(2), 95–112.
35. Smith, T., Higgs, J., & Pinsker, R. (2019). Do auditors price breach risk in their audit fees? *Journal of Information Systems, 33*(2), 177–204.
36. Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management, 36*(2), 215–225.
37. Srivastava, S. K., Das, S., Udo, G. J., & Bagchi, K. (2020). Determinants of cybercrime originating within a nation: A cross-country study. *Journal of Global Information Technology Management, 23*(2), 112–137.
38. Tselios, C., Tsolis, G., & Athanatos, M., et al. (2020). A comprehensive technical survey of contemporary cybersecurity products and solutions. Springer lecture notes in computer scienceIn A. P. Fournaris (Ed.), *Computer security* (Vol. 11981, pp. 3–18). Cham: Springer International Publishing.
39. Wirth, A. (2019). Reviewing today's cyberthreat landscape. *Biomedical Instrumentation & Technology, 53*(3), 227–231.
40. Yeh, Q. J., & Chang, A. J. (2007). Threats and countermeasures for information system security: A cross-industry study. *Information & Management, 44*(5), 480–491.
41. Zhou, L., Loeb, M. P., Gordon, L. A., & Lucyshyn, W. (2018). Empirical evidence on the determinants of cybersecurity investments in private sector firms. *Journal of Information Security, 9*(2), 720–726.

Marcus M. Keupp is the editor of this volume. He chairs the Department of Defense Economics at the Military Academy of the Swiss Federal Institute of Technology (ETH) Zurich. He was educated at the University of Mannheim (Germany) and Warwick Business School (UK) and obtained his Ph.D. and habilitation from the University of St. Gallen (Switzerland). He has authored, co-authored, and edited twelve books and more than 30 peer-reviewed journal articles and received numerous awards for his academic achievements.