Guest Editorial: Cyber-Attacks, Strategic Cyber-Foresight, and Security

I. Introduction

REPORTS of cyber-attacks against individuals, organizations, and businesses are on the rise. Attackers usually have a deliberate and malicious intent and may involve the criminals taking advantage of flaws in software code, using tricks to get around antivirus tools, and or exploiting unsuspecting users into divulging sensitive information [10], [11]. Often launched by isolated amateurs, or criminals that belong to often well-structured organizations, with money, motivation, and an agenda, such attacks are frequently designed to temporarily or indefinitely disrupt services of a host connected to the internet or simply grind institutional systems to a halt [4], [8].

Popular among social engineering, malwares employed in such attacks are what has come to be known as a distributed denial-of-service attack, which affect the infrastructure of websites, computer servers, and other network resources resulting in the compromise of critical personal or institutional data [14], [17]. Across the globe, these attacks are growing in sophistication, and they tend to have serious economic and security consequences for their targets. The chaos they precipitate can be life-threatening, and their cost can be considerable to target organizations or nations [5], [16]. Such features also affect the dynamics of collaboration among firms, thus posing negative effects on innovation dynamics [15].

While modern computer security technologies may be helpful in protecting users and walling off critical infrastructures from cybercriminals [6], strategic cyber-foresight is what is required to keep a step ahead of these criminals [19]. Strategic cyber-foresight is an institution's ability to identify, analyze, and defend from or counter against potential cyber-attacks within the contingency of organizing. For some critics, cyber-attacks have become a moving target, and technology and engineering management is struggling to catch-up with this growing threat [7], [21]. In particular, available systems employed in vulnerability assessment, analyzing, disrupting, and countering against stealthy deception attacks have been found to be inadequate.

II. Approaches to Cyber-Foresight and Security

Organizations continue to speed up innovation activities to renew themselves and remain competitive [A10], with many deeply integrated along multiple value chains, including data sharing [A3]. In this regard, it is more than single company that need to be prepared for protection against cyberattacks, but entire value chains [A12]. Especially for small companies, such professional preparedness is a challenge due to resources constraints [3], a critical aspect associated with the capacity of triggering entrepreneurial events [12].

Among the most frequently referenced challenges to innovation management is the quest for a seamless integrated innovation process for many years already [9]. This involved reshaping companies' organizational and business models under the umbrella of digital transformation [A7]. This "seamless paradigm" arises from the transparency that results from companies' digitalization efforts, ultimately impacting the visibility of information flows in an organization. In these organizations, weaknesses become more obvious and transparent to management, thus requiring a revised digital mindset across the organization. At the same time, the risk of outsiders taking the chance to attack the virtual infrastructure purposefully increases, as well as the risks of organizations members leaking valuable information to outsiders [A5].

Thus, organizations are faced with developing cyber strategies that are well in line with business strategies, adjusting business processes to the respective threats of cyber-attacks, and enhancing organizational culture toward resilience [A7]. Organizational performance is at least partially determined by the trust between employees (people) and their trust in the organization relating to people, technology and routines (processes) [A9]. Trust is a very human feature that is driven by many determinants, such as experiences, sharing of attitudes with others, and level of communication openness. The latter requires taking into account different elements and forms of trust that are defined by Rodgers et al. [A9] as follows:

1) rational-based trust,
2) rule-based trust,
3) category-based trust,
4) third-party-based trust,
5) role-based trust,
6) knowledge-based trust.

Obviously, these forms (or combination thereof) are important features of the overall organizational work climate that influences individuals' professional performance. In turn, it also shapes the dynamics of organizational knowledge production and sharing, along with sustainable innovativeness and competitiveness. In other words, trust forms a part of an organizations' intellectual assets—although it is hardly quantifiable. Managing

Date of current version 1 November 2022.
Digital Object Identifier 10.1109/TEM.2022.3204165

trust in this context is essential when it comes to making decisions regarding the organizations' strategic and operational development. Such decisions are frequently based on information and data collected, processed, and prepared by the organizations' employees. Of course, firm management is usually under reasonable time pressure when it comes to decision-making. Thus, there is a certain level of trust in the information base (and as such in the employees preparing the information). The security-by-design principle is a software development approach that in the first instance aims at making software solutions as secure as possible by taking into account all potential threats on software solutions [A2]. This, however, requires an organizational setup and culture that enhances employees thinking "out of the box" or, in other words, thinking the unthinkable. Secure solutions require developers accepting the trial-and-error approach from the beginning of the development work. There is hardly another way to prepare a full picture of potential security threats well in advance.

Another challenge comes from fakes in all thinkable shapes. Detecting fake appears doable in the meantime but fighting fake and responding to fakes is a more challenging task for organizations [A4]. At the one hand, it is costly because it often involves legal action. More importantly, it requires robust evidence, which are costly and time-consuming to gather.

III. Concluding Remarks

In a narrow understanding, cybersecurity covers protection of data, information, networks, and computer applications [13]. Risks increase with the rise of interconnectedness among organizations within and across countries and continents, which is manifest in economic and political terms. This interconnectedness also implies that an attack on a single organization inherits the threat of a broader impact on other organizations and countries on broader scale [A1]. Managing cybersecurity needs to account for incident governance command, incident sharing, escalations, and reporting and incident management [A8]. These aspects are crucial elements for cybersecurity management but require fine-tuning according to the organizations' requirements. In order to respond to cybercrime, sole focus on technological defenses fall short in addressing the true extent of the challenges involved in this scene. The technology dimension needs to be extended by the human factor [A11]. Cybersecurity is not only protecting the technological assets but also monitoring the environment at different levels for people who might impose a threat to the organization for one reason or another [A5], [A13]. Such threat might emerge from technological solutions associated with user capabilities [2]. Furthermore, it is an issue of staff entrusted with these tasks' motivation and attitudes beyond the pure technological and engineering skills [18], [20]. Eventually, this leads to a security attitude that comes in different forms and shapes in organizations [A11]. It appears that, from the technology perspective, there is a certain maturity level reached. Yet, there remains a lack in profound management approaches of cybersecurity [3].

In this respect, "cyber-resiliency" is a special challenge to overcome for organizations since it includes the external relations by means of suppliers, distributors, stakeholders, and other partners. The challenge lies in designing cyber strategies that set standards and protocols but are not too restrictive in that they neglect the personal trust and relations with partners but are not too lax in technical terms and standards. In that respect, it is an important task for organizations to take stock of internal data and information, assess them against their importance for the organization, and prioritize and assign access rights accordingly (including rights to upload, change, download, and similar). Like in any case of change management, effective initiatives to support new processes are required in order to generate effective and sustainable impacts.

The tremendous development of the virtual world caused a similar increasing speed in the development and implementation of technology infrastructure policy [1]. These were mainly initiated by changes in the environment (event driven), focus events (process driven). To meet these demands, policymakers improved understanding of the environment and widespread awareness of political institutions and organizations (representative connection) and consensus conflicts within the political establishment (conflict expansion mechanism) [A6]. Accordingly, over the last decade, there appeared to be a shift in policy responses by governments to cybersecurity challenges. During the twentieth century, governments were rather passive in formulating policies. This has changed considerably during the last two decades towards a proactive policy approach with a more or less holistic focus instead of the previously narrow bounded focus [A6].

We, therefore, for this Special Section invited papers from researchers and practitioners that have the potential to extend our understanding on cyber-attacks, and ways of organizing that can help firms and nation-states to proactively protect themselves from cyber-attacks. We received a broad array of submissions, ranging from conceptual, review, and empirical (quantitative and qualitative) papers, which testifies the growing interest in cyberattacks and security research and the richness of the research and scholarship exploring the phenomenon in practice. Contributing to existing research on strategic cybersecurity and foresight, this Special Section adopts diverse theoretical prisms and methodological approaches, united by their quest to deepen our understanding on the relevance, potentialities and limits of cyber-attacks, strategic cyber-foresight, and security on organizing.

Taken together, the papers contained in this Special Section provide some searing insight into the salient theoretical and empirical foundations underlying cyber-attacks, strategic cyber-foresight, and security. They also indicate the current state of the literature and provide some fruitful directions for future research.

Bruno Fischer
University of Campinas
Campinas, Brazil
HSE University
Moscow, Russia

DIRK MEISSNER
HSE University
Moscow, Russia

RICHARD NYUUR
University of Bradford School of Management
Bradford, U.K.

DAVID SARPONG
Brunel University
London, U.K.

ACKNOWLEDGMENT

The work of Bruno Fischer and Dirk Meissner was supported by HSE University through Basic Research Program.

APPENDIX: RELATED WORK

Developing technologies have enabled us to gain further insight into the future threats through technology intelligence mining [A14].

[A1] H. Nasser Alshabib and J. Tiago Martins, "Cybersecurity: Perceived threats and policy responses in the gulf cooperation council," *IEEE Trans. Eng. Manage.*, early access, Aug. 6, 2021, doi: 10.1109/TEM.2021.3083330.

[A2] F. M. Awaysheh, M. N. Aladwan, M. Alazab, S. Alawadi, J. C. Cabaleiro, and T. F. Pena, "Security by design for big data frameworks over cloud computing," *IEEE Trans. Eng. Manage.*, early access, Feb. 8, 2021, doi: 10.1109/TEM.2020.3045661.

[A3] O. Durowoju, H. K. Chan, and X. Wang, "Investigation of the effect of e-platform information security breaches: A small and medium enterprise supply chain perspective," *IEEE Trans. Eng. Manage.*, early access, Aug. 5, 2020, doi: 10.1109/TEM.2020.3008827.

[A4] B. Hammi, S. Zeadally, Y. C. E. Adja, M. D. Giudice, and J. Nebhen, "Blockchain-based solution for detecting and preventing fake check scams," *IEEE Trans. Eng. Manage.*, early access, Jul.1, 2021, doi: 10.1109/TEM.2021.3087112.

[A5] J. Jian, S. Chen, X. Luo, T. Lee, and X. Yu, "Organized cyber-racketeering: Exploring the role of internet technology in organized cybercrime syndicates using a grounded theory approach," *IEEE Trans. Eng. Manage.*, early access, Jul. 14, 2020, doi: 10.1109/TEM.2020.3002784.

[A6] Z. Li, X. Guo, and Q. He, "A study of Chinese policy attention on cybersecurity," *IEEE Trans. Eng. Manage.*, early access, Oct. 20, 2020, doi: 10.1109/TEM.2020.3029019.

[A7] J. Loonam, J. Zwiegelaar, V. Kumar, and C. Booth, "Cyber-resiliency for digital enterprises: A strategic leadership perspective," *IEEE Trans. Eng. Manage.*, to be published, doi: 10.1109/TEM.2020.2996175.

[A8] C. Onwubiko and K. Ouazzane, "SOTER: A playbook for cybersecurity incident management," *IEEE Trans. Eng. Manage.*, early access, May 5, 2020, doi: 10.1109/TEM.2020.2979832.

[A9] W. Rodgers, R. Attah-Boakye, and K. Adams, "Application of algorithmic cognitive decision trust modeling for cyber security within organisations," *IEEE Trans. Eng. Manage.*, early access, Sep. 16, 2020, doi: 10.1109/TEM.2020.3019218.

[A10] S. K. Singh, M. Del Giudice, M. Nicotra, and F. Fiano, "How firm performs under stakeholder pressure: Unpacking the role of absorptive capacity and innovation capability," *IEEE Trans. Eng. Manage.*, early access, Dec. 9, 2020, doi: 10.1109/TEM.2020.3038867.

[A11] T. F. Stafford, "Platform-dependent computer security complacency: The unrecognized insider threat," *IEEE Trans. Eng. Manage.*, early access, Mar. 9, 2021, doi: 10.1109/TEM.2021.3058344.

[A12] G. R. T. White, R. A. Allen, A. Samuel, A. Abdullah, and R. J. Thomas, "Antecedents of cybersecurity implementation: A study of the cyber-preparedness of U.K. social enterprises," *IEEE Trans. Eng. Manage.*, early access, Jun. 10, 2020, doi: 10.1109/TEM.2020.2994981.

[A13] V. A. Yerdon, J. Lin, R. W. Wohleber, G. Matthews, L. Reinerman-Jones, and P. A. Hancock, "Eye-tracking active indicators of insider threats: Detecting illicit activity during normal workflow," *IEEE Trans. Eng. Manage.*, early access, Jul. 1, 2021, doi: 10.1109/TEM.2021.3059240.

[A14] L. Ardito, A. M. Petruzzelli, V. Albino, and A. C. Garavelli, "Unveiling the technological outcomes of microgravity research through patent analysis: Implications for business and policy," *IEEE Trans. Eng. Manage.*, early access, Aug. 18, 2020, doi: 10.1109/TEM.2020.3010301.

REFERENCES

[1] M. S. Altayar, "A comparative study of anti-cybercrime laws in the gulf cooperation council countries," in *Proc. 2nd IEEE Int. Conf. Anti-Cybercrimes*, 2017, pp. 148–153.

[2] L. C. Amo, R. Liao, E. Frank, H. R. Rao, and S. Upadhyaya, "Cybersecurity interventions for teens: Two time-based approaches," *IEEE Trans. Educ.*, vol. 62, no. 2, pp. 134–140, May 2019.

[3] C. T. Berry and R. L. Berry, "An initial assessment of small business risk management approaches for cyber security threats," *Int. J. Bus. Continuity Risk Manage.*, vol. 8, no. 1, pp. 1–10, 2018.

[4] B. Brewster, B. Kemp, S. Galehbakhtiari, and B. Akhgar, "Cybercrime: Attack motivations and implications for big data and national security," in *Proc. Appl. Big Data Nat. Secur.*, 2015, pp. 108–127.

[5] R. Gandhi, A. Sharma, W. Mahoney, W. Sousan, Q. Zhu, and P. Laplante, "Dimensions of cyber-attacks: Cultural, social, economic, and political," *IEEE Technol. Soc. Mag.*, vol. 30, no. 1, pp. 28–38, Spring 2011.

[6] B. Genge, I. Kiss, and P. Haller, "A system dynamics approach for assessing the impact of cyber-attacks on critical infrastructures," *Int. J. Crit. Infrastructure Protection*, vol. 10, pp. 3–17, 2015.

[7] J. B. Hong and D. S. Kim, "Assessing the effectiveness of moving target defenses using security models," *IEEE Trans. Dependable Secure Comput.*, vol. 13, no. 2, pp. 163–177, Mar./Apr. 2016.

[8] M. Kadivar, "Cyber-attack attributes," *Technol. Innov. Manage. Rev.*, vol. 4, no. 11, 2014, Art. no. 22.

[9] J. Kratzer, D. Meissner, and V. Roud, “Open innovation and company culture: Internal openness makes the difference,” *Technol. Forecasting Social Change*, vol. 119, pp. 128–138, 2017.

[10] Y. Li, L. Shi, P. Cheng, J. Chen, and D. E. Quevedo, “Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach,” *IEEE Trans. Autom. Control*, vol. 60, no. 10, pp. 2831–2836, Oct. 2015.

[11] T. Rid and B. Buchanan, “Attributing cyber-attacks,” *J. Strategic Stud.*, vol. 38, no. 1-2, pp. 4–37, 2015.

[12] J. Sahut, L. Iandoli, and F. Teulon, “The age of digital entrepreneurship,” *Small Bus. Econ.*, vol. 56, no. 3, pp. 1159–1169, 2021, doi: 10.1007/s11187-019-00260-8.

[13] P. W. Singer, *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York, NY, USA: Oxford Univ. Press, 2014.

[14] T. Spyridopoulos, G. Karanikas, T. Tryfonas, and G. Oikonomou, “A game theoretic defence framework against DoS/DDoS cyber-attacks,” *Comput. Secur.*, vol. 38, pp. 39–50, 2013.

[15] F. Sussan and Z. J. Acs, “The digital entrepreneurial ecosystem,” *Small Bus. Econ.*, vol. 49, no. 1, pp. 55–73, 2017.

[16] R. Walters, “Cyber-attacks on us companies in 2014,” *Heritage Found.*, vol. 4289, pp. 1–5, 2014.

[17] B. Wang, Y. Zheng, W. Lou, and Y. T. Hou, “DDoS attack protection in the era of cloud computing and software-defined networking,” *Comput. Netw.*, vol. 81, pp. 308–319, 2015.

[18] K. S. Wilson and M. A. Kiy, “Some fundamental cybersecurity concepts,” *IEEE Access*, vol. 2, pp. 116–124, 2014.

[19] E. Yip, “ForeC: Designing cyber-physical systems with foresight,” Ph.D. dissertation, ResearchSpace, Univ. Auckland, Auckland, New Zealand, 2015.

[20] S. Zeadally, E. Adi, Z. Baig, and I. A. Khan, “Harnessing artificial intelligence capabilities to improve cybersecurity,” *IEEE Access*, vol. 8, pp. 23817–23837, 2020.

[21] R. Zhuang, S. A. DeLoach, and X. Ou, “Towards a theory of moving target defense,” in *Proc. 1st ACM Workshop Moving Target Defense*, 2014, pp. 31–40.

Bruno Fischer received the dual M.Sc. degrees in economics and innovation management from Universidad Autonoma de Madrid, Madrid, Spain, and in agribusiness from Universidade Federal do Rio Grande do Sul, Porto Alegre, Brazil, and the Ph.D. degree in economics and management of innovation from the Universidad Complutense de Madrid, Madrid, Spain.

He is currently an Associate Professor with the School of Applied Sciences (FCA), University of Campinas, Campinas, Brazil, and a Visiting Scholar with the National Research University Higher School of Economics, Moscow, Russia. His research interests include ecosystems, regional systems of innovation and entrepreneurship.

Dirk Meissner received the first Ph.D. degree in business administration, technology and innovation management, and the second Ph.D. degree in innovation management from Dresden University of Technology, Dresden, Germany, in 1996 and 2001, respectively.

He is currently a Distinguished Professor, the Head of the Laboratory for Economics of Innovation, HSE ISSEK, Moscow, Russia, and the Academic Director of the Master’s Programme Governance of STI. He has 20 years of experience in research and teaching technology and innovation management and policy. He has strong background in policy making and industrial management for STI with special focus on foresight and roadmapping, funding of research, and priority setting. Prior to joining HSE, he was responsible for technology and innovation policy at the presidential office of the Swiss Science and Technology Council. He was a Management Consultant for technology and innovation management with Arthur D. Little.

Prof. Meissner is a Member of OECD Working Party on Technology and Innovation Policy. He is an Associate Editor for *Technological Forecasting and Social Change*, IEEE TRANSACTIONS ON ENGINEERING MANAGEMENT, *Journal of Intellectual Capital,* and *Journal of the Knowledge Economy*, and a Member of Editorial Review Board at *Small Business Economics* and *Journal of Knowledge Management*. He guest-edited Special Issues in *Industry and Innovation Journal*, *Journal of Engineering and Technology Management, Technological Analysis and Strategic Management* among others.

Richard Nyuur received the M.Sc. degree in finance and business management from University of Bedfordshire, Bedfordshire, U.K. in 2005, the M.Res. degree in management and organization studies from Brunel University London, London, U.K. in 2007, and the Ph.D. degree in business management, Swansea University, Swansea, U.K. in 2011.

He is currently a Professor of international business and the Head of International Business, Marketing and Strategy Department, University of Bradford School of Management, Bradford, U.K. He has authored or coauthored papers in journals, such as *Journal of International Management, Journal of Business Research, International Marketing Review, International Human Resource Management Journal, Journal of Small Business Management, Thunderbird International Business Review, International Journal of Business Governance and Ethics, Journal of Strategy and Management, International Journal of Foresight and Innovation, African Journal of Economic and Management Studies* and *Social Responsibility Journal*. His research interests include the intersection of strategy and international business in the broad areas of international business strategy, firm (de)internationalization and strategic adaptiveness, international human resource management strategies, and corporate governance (including ethics and corporate social responsibility).

Prof. Nyuur is on the editorial boards of *Journal of African Business, Critical Perspectives on International Business* and *European Journal of Economics and Management*.

David Sarpong received the MA degree in applied social research and the Ph.D. degree in strategy and innovation management from University of the West of England, Bristol, U.K., in 2007 and 2010, respectively.

He is currently a Professor of strategic management with Brunel Business School, Brunel University London, London, U.K. His research works has appeared in various journals, such as *Technological Forecasting and Social Change, Technovation, R&D Management Journal, International Marketing Review, Journal of Business Research, Scandinavian Journal of Management* and *European Urban and Regional Studies*. His research interests include strategic management, innovation management, organizational foresight, and enterprise.