

Advanced Cybersecurity Applications: Solutions to Counteract Cyber Threats

Peter R. J. Trim ^{1,*}  and Yang-Im Lee ^{2,*} 

¹ Birkbeck Business School, Birkbeck, University of London, Malet Street, London WC1E 7HX, UK

² Westminster Business School, University of Westminster, 35 Marylebone Road, London NW1 5LS, UK

* Correspondence: p.trim@bbk.ac.uk (P.R.J.T.); y.lee@westminster.ac.uk (Y.-I.L.)

1. Introduction

This Special Issue is dedicated to developments in cybersecurity and includes a number of theoretical perspectives. The main focus is to highlight current and evolving challenges so that the reader is able to inform themselves of the factors and processes at work that give rise to a rapidly changing landscape of cybersecurity threats and challenges that need to be recognized and addressed. Choo [1] makes reference to this and voices concern regarding the form cyber-attacks take and why a strategic approach is needed to counteract the actions of cyber criminals. By deepening our understanding of the threat landscape, it helps to understand the motives of those carrying out cyber-attacks and also identify and utilize the resources required to counteract such actions. It is clear, however, that those carrying out cyber-attacks may do so as a result of certain motivations [2], which may be economic in nature or rooted in political or socio-cultural factors [3]. Due to the persistent nature and sophistication of those carrying out cyber-attacks, more needs to be done to safeguard society. For example, more attention needs to be given to proactive defense systems that draw on a range of cybersecurity approaches. Establishing how organizations, governments and society can be better protected and withstand current and evolving cyber-attacks is of particular interest to all those concerned with keeping society safe. This suggests that a proactive approach needs to be adopted to counteract cyber-attacks [4]. It can be argued that failing to keep people safe will lead to more disruption and discomfort as those carrying out cyber-attacks gain confidence and become more determined to cause harm. Successful cyber-attacks result in uncertainty and confusion and are assisted by disinformation campaigns. Those affected by cyber-attacks become concerned that the systems and mechanisms in place are insufficient to protect them. They become disoriented in the sense that they question if people in society can place their trust in those responsible for keeping them safe. This highlights the importance and value of cybersecurity research and reinforces the fact that policy makers must not become complacent in terms of what needs to be done to raise the profile of cybersecurity researchers.

In addition, academic researchers and policy makers need to provide attention to intra-organizational and inter-organizational arrangements and how human–technology interaction can enhance cybersecurity from a holistic perspective. A holistic approach will allow the benefits derived from cybersecurity research to be fully utilized, and highlight that organizational staff need to have the required organizational skills, know how to communicate risk and are able to undertake risk management ([5], p. 4). This is because cybersecurity covers a wide and increasingly complex area of study that is further exposing vulnerabilities in connectivity. Interconnectivity is increasing the vulnerability of people and organizations through the misinterpretation of how technology is used. By undertaking



Received: 19 May 2026

Accepted: 22 May 2026

Published: 26 May 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

research into the aspects of cybersecurity and making links with other fields of study, it is possible to uncover solutions to unique and evolving threat-related problems.

Research into cybersecurity can be considered a positive investment from society's point of view. Those carrying out cyber-attacks are developing their knowledge and expertise and translating this into new forms of attack. Hence, cybersecurity intervention is required to counteract the actions of those launching cyber-attacks. Governments around the world are concerned with the nature of such attacks and are keen to support academic research that studies various aspects of the problem and generates solutions. The following quotation from Harknett and Stever ([6], p. 2) reinforces the role of government in terms of cybersecurity provision: "First, is the essential recognition that cyber threats pose a national security challenge. Cyber threats are more serious than a nuisance or crime. Second, intergovernmental management problems are inevitably a part of the cyber challenge. State and local governments are destined to be key actors in meeting future cyber threats. Third, involving state and local governments will facilitate partnerships with the private sector corporations that operate critical cyber infrastructure. Finally, the general population, the end users of computer technology, must be mobilized and involved in any successful cybersecurity".

Accepting that more has to be done to protect people in society, especially the young, the elderly and those deemed vulnerable, means that cybersecurity researchers will in the years ahead be under more pressure to undertake research that is of benefit to society and at the same time is considered value for money. Ensuring that the appropriate countermeasures are developed and put in place is the responsibility of policy makers, company representatives and academic researchers, and requires a collective approach to be successful. To achieve this, cybersecurity guidelines need to be in place that take into account the capabilities and requirements of different users [7]. It is because of this that cybersecurity is not to be thought of as being the priority of a few. The fact that cybersecurity is complex and requires an interdisciplinary and multidisciplinary approach to research is receiving attention. It is with this in mind that we are pleased to make reference to a range of contributions in the Special Issue that emanate from various researchers throughout the world. These cutting-edge research papers are available due to the dedication and commitment of those working hard to produce new knowledge. Without their dedication, this Special Issue would not have been possible. Indeed, the papers in this Special Issue contain a unique collection of insights from various studies that offer practical insights, advances in theoretical understanding, exhibit review-oriented appreciation and critical discourse, and display conceptual appreciation of a rapidly evolving body of knowledge.

Those instigating cyber-attacks are known to fall within various categories ranging from ideologically driven and disruptive to highly organized and harmful. It is the objective of this Special Issue to make clear how research into cybersecurity can be used to solve existing and recurring cybersecurity problems. It can be noted, therefore, that some contributions draw extensively on cross-border working relationships and the pooling of knowledge. Some contributions are derived from specific research groups that have critical depth in a known area of study. It is hoped that the collection of papers will stimulate further research and result in new research collaborations. Indeed, by extending the boundaries and identifying new and related bodies of knowledge, it should be possible to provide cybersecurity solutions that integrate distinct and new areas of knowledge such as business continuity management, crisis and emergency management, organizational resilience, and risk management.

2. An Overview of the Published Articles

The collection of articles does much to advance our knowledge of the developments in cybersecurity, and it is pleasing to see the range and depth of material, evidencing a vibrant research community. It is with great pleasure, therefore, that we start with the first contribution, which is in fact a review. Hossain et al. focus on the issues and challenges confronting the local government and outline a framework that provides an understanding of how local government representatives can view the cybersecurity landscape. The work makes clear the knowledge gaps that need to be filled and places cybersecurity within the context of security domains. The PRISMA protocol is made reference to and of particular interest is the classification of data that local government representatives deal with. Cyber-attacks on local governments do much to deepen our understanding of the problem and thus the barriers are given attention. The cybersecurity tools made reference to can be considered solutions to overcome the challenges cited. Of particular interest are the assessment frameworks and standards, and insights relating to cybersecurity policies. The recommendations provided for local governments should allow relevant policies to be devised and implemented.

The second contribution is by Ryu et al. Reference is made to the cybersecurity vulnerabilities of IT infrastructures with specific attention given to rapid digital transformation and network expansion. Specific malware threats, such as Industroyer, Triton, NotPetya, and BlackEnergy3, are studied and a layered security architecture is proposed that has a unified defense strategy. The researchers argue for an integrated approach to counter the actions of cyber attackers and offer much depth in terms of analyzing major cybersecurity threats in relation to SCADA and SIS systems.

Alabdulatif presents a hybrid ensemble learning-based intrusion detection framework that integrates deep learning and traditional ML algorithms with explainable artificial intelligence vis-à-vis real-time cybersecurity applications. An artificial neural network and support vector machine are used and so is a random forest to improve detection performance. Reference is made to network-based cyber-attacks and detail is provided regarding the model's construction.

Next, Al-Zubaidie and Jebbar inform us about a security protocol in relation to digital cryptocurrency wallets, which are protected by the XSalsa20 algorithm. Reference is made to traditional security techniques for lending systems and security in blockchain-based lending systems. This is followed by greater insight into the security of the lending system and the core concepts of loans. The XSalsa20 algorithm is outlined, and this is followed by the proposed lending protocol process. An assessment is offered and this is followed by concluding remarks.

Qiu et al. add to our understanding of network theory by proposing a quantitative analysis method for the influence of power cyber-physical cross-domain attack paths based on graph knowledge. They detail electric power cyber physical coupling characteristics and follow up with a method for constructing an attack graph. A comprehensive cascading failure analysis is provided. This is followed by the coupling relationship between networks in the power cyber-physical integration system. Following an experimental simulation analysis is a discussion. Of interest is insight into the cascading failures of the physical space system, which the reader can gain much knowledge about.

Park et al. pay attention to the constraints of isolated network environments and bring to the fore the limitations of existing security frameworks. The authors adopt an international focus by comparing and analyzing multi-level security (MLS) models in the US and Korea. An outcome of the research is MLS classification criteria and a proposed zero-trust-based MLS model. Park et al. substantiate their work by outlining the risks they

include and go on to substantiate their approach by including proposed security controls. Further depth and insight is provided through the inclusion of attack scenarios.

The seventh contribution is authored by Pu and Wan. Their focus is on Advanced Persistent Threat (APT) malware, and more specifically an APT malware detection model that is based on heterogeneous multimodal semantic fusion (HMSF-ADM). A DPCFTE module is provided to enhance local semantic representations and two models are referred to.

A systematic investigation into vulnerabilities of event-based person Re-ID models is provided by Woo and Lee. The authors undertake research into Re-ID modes operating on five-channel event voxels. Their findings suggest that due to the certain nature of event-based person Re-ID, there is susceptibility in terms of gradient-based exploits. The authors put forward the view that robustness-aware design and defense mechanisms in event-based surveillance systems need to be given consideration.

The volume concludes with a paper by Alabdulatif and Thilakarathne relating to threat hunting. Taking cognizance of the threat landscape in healthcare, the authors summarize cybersecurity of the smart health domain, consider deception technology within smart health ecosystems and advocate the design of the cyber threat-hunting platform. The results and analysis of threat intelligence data leads to a number of recommendations.

3. Conclusions

This Special Issue achieves much in the sense that it builds on previous work in the field of advances in cybersecurity and provides a firm grounding in advanced cybersecurity applications that will help government, industry, academia and people in society be better protected from cyber-attacks. The approaches outlined by the authors will do much to promote interdisciplinary and multidisciplinary research in the area of cybersecurity, and related areas of study. The work being done on threat detection, for example, will continue to gain momentum from the insights provided by researchers that put effort into devising and running models and cooperating with other researchers to produce frameworks that can yield policy recommendations. Cybersecurity research is vibrant and will continue to expand and give rise to new conceptual and theoretical breakthroughs, which can be considered timely and beneficial for all the stakeholders in society.

Conflicts of Interest: The authors declare no conflicts of interest.

List of Contributions

1. Hossain, S.T.; Yigitcanlar, T.; Nguyen, K.; Xu, Y. Local government cybersecurity landscape: A systematic review and conceptual framework. *Appl. Sci.* **2024**, *14*, 5501. <https://doi.org/10.3390/app14135501>.
2. Ryu, D.; Lee, S.; Yang, S.; Jeong, J.; Lee, Y.; Shin, D. Enhancing cybersecurity in energy IT infrastructure through a layered defense approach to major malware threats. *Appl. Sci.* **2024**, *14*, 10342. <https://doi.org/10.3390/app142210342>.
3. Alabdulatif, A. A novel ensemble of deep learning approach for cybersecurity intrusion detection with explainable artificial intelligence. *Appl. Sci.* **2025**, *15*, 7984. <https://doi.org/10.3390/app15147984>.
4. Al-Zubaidie, M.; Jebbar, W.A. Providing security for flash loan system using cryptocurrency wallets supported by XSalsa20 in a blockchain environment. *Appl. Sci.* **2024**, *14*, 6361. <https://doi.org/10.3390/app14146361>.
5. Qiu, S.; Shao, Z.; Wang, J.; Xu, S.; Fei, J. Research on power cyber-physical cross-domain attack paths based on graph knowledge. *Appl. Sci.* **2024**, *14*, 6189. <https://doi.org/10.3390/app14146189>.
6. Park, J.-H.; Park, S.-C.; Youm, H.-Y. A Proposal for a zero-trust-based multi-level security model and its security controls. *Appl. Sci.* **2025**, *15*, 785. <https://doi.org/10.3390/app15020785>.

7. Pu, C.; Wan, L. APT malware detection model based on heterogeneous multimodal semantic fusion. *Appl. Sci.* **2026**, *16*, 1083. <https://doi.org/10.3390/app16021083>.
8. Woo, J.H.; Lee, E.-K. Query-side adversarial attacks on event-based person re-identification: A first-order robustness analysis. *Appl. Sci.* **2026**, *16*, 2430. <https://doi.org/10.3390/app16052430>.
9. Alabdulatif, A.; Thilakarathne, N.N. A novel cloud-enabled cyber threat hunting platform for evaluating the cyber risks associated with smart health ecosystems. *Appl. Sci.* **2024**, *14*, 9567. <https://doi.org/10.3390/app14209567>.

References

1. Choo, K.-K.R. The cyber threat landscape: Challenges and future research directions. *Comput. Secur.* **2011**, *30*, 719–731. [[CrossRef](#)]
2. Kumar, S.; Carley, K.M. Approaches to understanding the motivations behind cyber attacks. In Proceedings of the 2016 IEEE Conference on Intelligence and Security Informatics (ISI), Tucson, AZ, USA, 28–30 September 2016; pp. 307–309. [[CrossRef](#)]
3. Han, C.; Dongre, R. What motivates cyber attackers? *Technol. Innov. Manag. Rev.* **2014**, *4*, 40–42. [[CrossRef](#)] [[PubMed](#)]
4. Quader, F.; Janeja, V.P. Insights into organizational security readiness: Lessons learned from cyber-attack case studies. *J. Cybersecur. Priv.* **2021**, *1*, 638–659. [[CrossRef](#)]
5. Elmelhem, J.E.L.; Bouras, A.; Ghemri, F. Towards a holistic approach of cybersecurity. In Proceedings of the IEEE 2018 3rd Technology Innovation Management and Engineering Science International Conference (TIMES-iCON 2018), Bangkok, Thailand, 12–14 December 2018; pp. 1–4. [[CrossRef](#)]
6. Harknett, R.J.; Stever, J.A. The cybersecurity triad: Government, private sector partners, and the engaged cybersecurity citizen. *J. Homel. Secur. Emerg. Manag.* **2009**, *6*, 79. [[CrossRef](#)]
7. Nurse, J.R.C.; Cresse, S.; Goldsmith, M.; Lamberts, K. Guidelines for usable cybersecurity: Past and present. In Proceedings of the IEEE 2011 Third International Workshop on Cyberspace Safety and Security (CSS), Milan, Italy, 8 September 2011; pp. 21–26. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.