International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Predicting Future Cyber Threats: Analysing Trends and Predicting Future Cybersecurity Challenges

Richard Aggrey[1], Emmanuel Adjirachor[2], Bright Ansah Adjei[3], Nana Adwoa Dsane[4], Karl Osei Afoduo[5]

[1]Dep. Director, Head of IT, University of Ghana Medical Centre
[2]Director, Security Assurance, New York City Health and Hospitals Corporation
[3]Senior Health Research Officer, University of Ghana Medical Centre,
[4]Dep. Director of Research, University of Ghana Medical Centre,
[5]Senior Health Research Officer, University of Ghana Medical Centre

Abstract

As the sophistication of cyber threats grows, we move from traditional reactive cybersecurity to the implementation of predictive cybersecurity. This paper explores how more advanced technology, integrated systems, and state-sponsored attacks have created a complicated threat landscape requiring predictive threat management. An organisation can foresee future vulnerabilities by analysing trends such as phishing, ransomware, and advanced persistent threats (APTs) through logical correlation. This paper discusses the adoption of predictive models - both quantitative and qualitative methods - and using Artificial Intelligence (AI) and Machine Learning (ML) in real-time threat detection and situational awareness. For instance, the SolarWinds supply chain and the Ukraine power grid attacks show why predictive analysis is needed to deal with the risks. Due to ethical considerations, such as data bias or fairness, developing reliable predictive models is critical. To effectively predict threats, industries, governments, and researchers must collaborate and establish a resilient cybersecurity framework anticipating what is coming next.

1. Introduction to Cyber Threat Prediction

Cybersecurity has become a serious matter over the years, and with the latest strategies, attackers have used. Trickling in bit by bit, the conventional cybersecurity model of attempting to identify and react to threats as they occur is no longer enough. In recent times, the threats are more intricate in terms of the landscape. A greater interest in understanding cybersecurity threats is rooted in this examination of the future (Li, et al., 2021). Learn about threats as they happen, and use this information to predict future cybersecurity threats. An important increase in cyber threats has made prioritising risk management and enhancing information security essential. The rise in cyber risk may stem from several factors, such as technological progress, interrelated and interconnected systems, the escalating complexity of malware, and the higher frequency of incidents caused by advanced attacks (Aslan et al., 2023).

Over time, security research has saturated its foundation. Researchers focus on new and sophisticated ways that an attacker can launch an attack. Next-generation dangers, old challenges in new forms, attacker

inspirations, and other fundamental attributes are included in such research. To uncover future challenges, the analysis examines the behaviour of adversaries. Modern techniques for predictive thinking range widely, from intelligence-driven security awareness systems to strategic corporate risk management (Alkhalil et al., 2021). Two distinct domains fall under the umbrella of threat analysis: trends analysis is based on actual threat intelligence and is used to estimate and quantify scenarios. The psychology of adversarial reasoning is utilised in anticipatory predictive thought. This text takes a bird's-eye view of cybersecurity research before examining trends and predicting future dangers. Simulation methods, credible evaluation methods, attack domain details, and experimental models or behavioural patterns are among the methodologies used in threat foretelling (Alabdan, 2020).

1.1. Importance of Anticipating Future Cyber Threats

It is essential to understand that organisations should not only focus on dealing with the threats and vulnerabilities relating to cybersecurity's current technical and social aspects but also perform deep analysis to find future cybercrime challenges and how we can develop resilience to overcome them proactively. A forward-thinking approach is essential for organisations to anticipate the future of cyber threats and prepare resources such as time, financial assets, and reputation to rebuff the damage caused by various types of cybercrimes. Moreover, all the operational processes running within the system may be studied for any potential flaws or loose ends. In the past, the inability to predict and identify weak areas in the complex network has often been exhibited as a reason for high-impact security breaches. Aligning cybersecurity programmes with the modern trends of anticipating cybersecurity threats can effectively increase the adaptability and resilience of security controls, understanding the risks from a new perspective (Nassar et al., 2021).

A deeper understanding can also aid in predicting how tactics from the arsenal of potential attackers could evolve and how threat surfaces, and vectors may alter to launch new forms of attacks. Predictive modelling in cybersecurity has become more relevant and operational than just theoretical due to the increased attacks from emerging technologies in computing and communication. It is also essential to develop a functional plan of action for raising cybersecurity awareness that engages organisations, private and public sectors to build a resilient cybersecurity culture against future cyber threats. Furthermore, mirroring such security awareness in policymaking can revolutionise national cybersecurity capabilities and readiness. Anticipating cyber threats is a prime step which sets the foundation for other elements to curb cybercrimes (Nicholls et al., 2021). A classic real-world example to give credence to this above is the ***SolarWinds Supply Chain Attack*** in 2020 and affected myriad of organisations around the world. Predictive analysis could have thwarted the attack by identifying vulnerabilities before the exploitation (HIMSS, 2021).

2. Analysing Current Cybersecurity Trends

The future challenges of cybersecurity can only be ascertained when current trends are carefully studied to determine its outcome. The threat environment has expanded significantly and increased in complexity, giving rise to sophisticated dangers like targeted phishing, ransomware, and advanced persistent threats (APTs). In addition, there are many more exploratory and offensive phases before actual cyber-attacks are initiated. Another trend is the unique challenge faced by different areas, such as healthcare, research, military, government, enterprise organisations, and the financial sector. We also observe some new and emerging modern threats affecting certain domains (Lallie et al., 2021).

Likewise, some areas are more susceptible to certain attacks simultaneous to the rise of new threats. Nowadays, some sectors, like Defence and Finance, have developed a comprehensive view of their

security perspective. As a result of heightened compliance scrutiny, ensuring a higher baseline of regulatory compliance is also increasing in importance. From a defensive point of view, the firewalls have become difficult to blunt and costlier to ignore, leading businesses to implement more defensive strategies. There is a high impetus to enhance current regulatory regimes and the capacity to address significant concerns. The global complexity of servers, email systems, and applications has improved dissemination models that rely on sharing information. Many of the basic security principles are subject to cyber threats. Firewalls, antivirus applications and cryptography are prevalent security tools used with some adaptation to protect services. There is an increasing need for continuous enhancement in defensive strategies and techniques practices. Threat intelligence community research also suggests that companies are breaking down their protection barriers to open the sharing of their respective indicators of compromise for more extensive collections of valuable data. Lastly, cloud services are gaining more priority in modern organisations, which raises security issues (Berdik et al., 2021).

Table 1:Sector-Specific Threats

Sector	Common Threats	Example
Healthcare	Ransomware, Data Breaches	UHS Ransomware Attack (2020)
Finance	Phishing, Fraudulent Transactions	SWIFT Payment System Breach (2016)
Government	State-Sponsored Espionage, APTs	SolarWinds Supply Chain Attack (2020)
Defence	Cyber Espionage, Supply Chain Attacks	Chinese APTs Targeting Defence Contractors

2.1. Global Cybersecurity Landscape

Recent years have shown a considerable spectrum of cybersecurity challenges to individual countries and industries across the globe. Regional differences do indeed exist in attacking behaviour and motives, yet underlying systemic forces influence activity that touches almost every part of the globe. The Ukrainian conflict has led to a flurry of cyber activity, with many major countries raising their 'cyber defence' posture (Genschel, 2022). This has consequently led to a significant increase in state-level Directed Denial of Service attacks. Increasingly, these attacks are wider, looking to exert pressure on critical infrastructure and damaging target websites and servers. The conflict's chaos has allowed cyber to mix with kinetic activity, with widespread state-level cyber espionage uncovered globally. This often leads to using the same information about publicly discovered exploits by the attackers for their ends. As such, zero-day exploits are a rarity and are indeed treated as very valuable commodities by attackers (Akoto, 2021).

The general increase in criminal actors will naturally increase the variety and scope of attacks. The global security environment continues to pose difficult situations for defenders and improve the capabilities of cyber attackers. Data breaches increased in both the US and EU during this time. It is now estimated that over 120 countries have state hacks in effect. The Global Cybersecurity Index benchmarks cyber readiness in each country. They break down readiness into five categories: legal, technical, organisational, capacity building, and international cooperation. Notably, the 'technical' index score also tracks readiness according to economic development. While 138 countries are now implementing cybersecurity strategies or plans, some countries are rated as leaders in cybersecurity readiness. This indicates an 80–90% implementation rate with high resource commitment, cooperation, and coordination among government bodies (Argaw et al., 2020).

International collaborative efforts to build cybersecurity typically focus on creating software tools or cooperation documents. These often have an intelligence or forensics remit. A major part of a significant country's cybersecurity is actually in managing public perceptions and what information is fed to the media. The media effect that can raise or calm a situation is often leveraged according to policy and operational decisions. Publicity and perception management are significant concerns in cybersecurity responses, usually shaping operational decisions in response to a current situation. For this reason, secretive operations are necessary to ensure security. Emerging markets require increasing maturity and cybersecurity capability. In least-developed countries, security can be less of a concern compared to other threats (Alexei et al, 2021).

In contrast, emerging markets often have specific, external driver threats such as industrial or state espionage or targeted attacks. Cyber espionage is typically attributed to actions by other states and is a feature of major countries, though it can also be part of inter or intra-state conflict. The nature of the data compromised in these actions is typically trans-border and very sensitive (Buchanan, 2020).

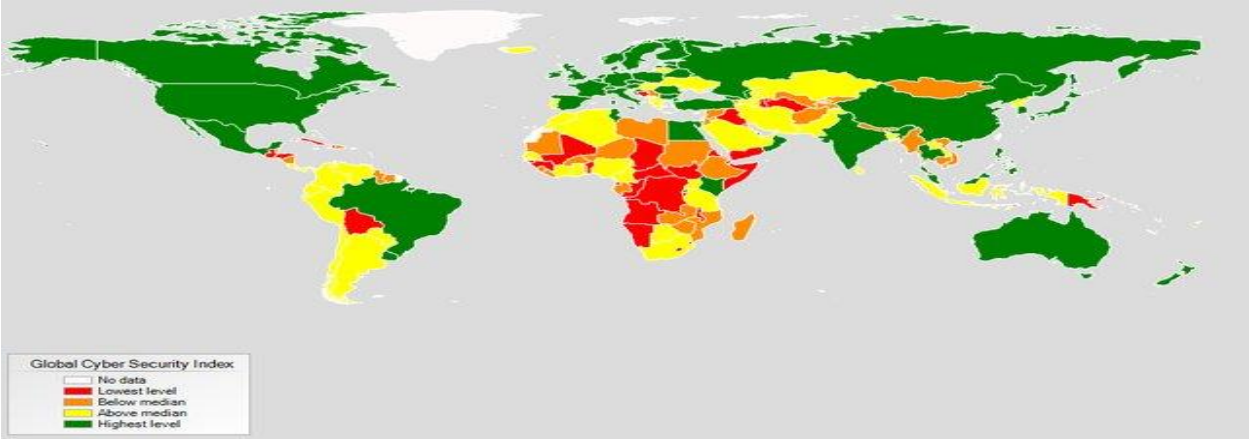

Figure 1:(Global Cybersecurity Index Scores, 2022)
Credit: Antoine Bouveret

3. Methods and Tools for Predicting Cyber Threats

Efficiently predicting the future of cyber threats is essential to achieving effective cybersecurity risk management, as anticipating possible threats helps design appropriate preventative and proactive strategies. Many different methods and tools have been proposed to predict future cyber threats. The approaches used to forecast an attack phenomenon can generally be classified into two major groups: quantitative and qualitative. The integration of threat intelligence feeds can bolster the predictions and trend analysis conducted within cyber threat anticipation tools. Continuous monitoring and data analysis can help identify real-time patterns of interest, which could assist organisations in forecasting activities when fused and correlated with current cyber threat data (Safitra et al., 2023).

Several studies use inadequate, traditional, or inefficient methods to predict the characteristics of attacks or to plan the level of defence to put in place. Several new prediction techniques, such as the social network-based model and mathematical simulation, are gradually gaining attention within the literature. The forecasting methods using expert opinion are attractive. An advanced technique for collaborative prediction associates expert opinion and the social behaviour of a community of domain experts. An advantage of using different prediction strategies is that the consensual prediction of the various techniques increases the accuracy of cyber-attack forecasts and the robustness of decision-making. Group

prediction, especially by domain experts, also reinforces a statistical prediction and leads to an improved success rate for real-world feedback (Mishra et al., 2023).

Moreover, using a single forecasting method has another disadvantage because it may need to pay attention to some specific characteristics or events that only appear before a particular time. A statistical type of assessment for threat prediction should relate to various data sources and constantly changing perspectives. Systematic analyses depend on frameworks and models designed to follow real-time data to support the selection of alternative risk models and the development of effective countermeasures in the fight against cyber threats. Predicting the characteristics of a cyber-attack is an old problem and the numerous strategies that have been implemented yield different results depending on the type of attack. In the past, researchers and cyber experts were used to guessing the nature of threats by hand and gathering information from different sources. At the same time, experts and cybersecurity managers began to believe that threats could be forecasted accurately through a convergence of several models as well as techniques based on behaviour measurement (Duo et al., 2022).

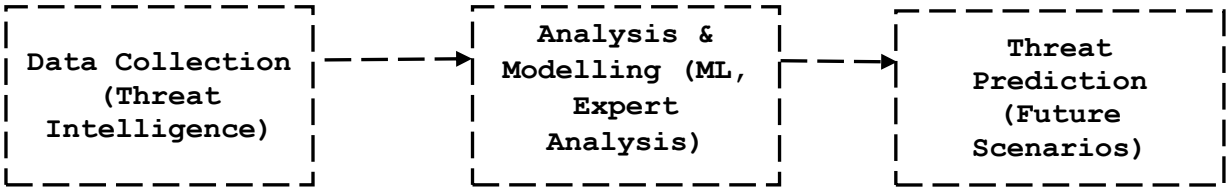

Figure 2: Predictive Cybersecurity Framework

3.1. Machine Learning and Artificial Intelligence in Cyber Threat Prediction

According to Smith et al. (2023) an AI-driven Security Operations Centre (SOC) reduced response times by 40% through automated threat correlation and anomaly detection. One of the main advantages of Machine Learning and Artificial Intelligence in predicting future cyber threats is the capability to analyse massive datasets in near real-time to search for patterns that could indicate an unknown threat. These technologies complement the advanced skills of the Technology Security Team or individual in identifying the content of the internet at scale and enrich the anomaly detection capabilities. More importantly, they empower the team with advanced AI models that could revolutionise incident response (Kaloroumakis et al., 2021). These models enable the team to improve threat hunting by automatically identifying related incidents across broad telemetry when only part of the incident has been observed and provide a statistical measure of confidence for those related cyber operations. This empowerment has practical consequences for the rate at which analysts diagnose and respond to incidents, increasing the breadth and accuracy of intelligent, machine-assisted threat hunting performed in a network. The practical need for automating the identification of related incidents derives from the aforementioned volume of data, which at certain scales exceeds human analysts' ability to hunt for threats manually. A fully human-driven response is quickly becoming untenable given the scale and volume of cyber intelligence that needs to be assimilated and acted on defensively more promptly by individual human analysts can hope to keep up with (Ukwandu et al., 2020). The ability to analyse a network's broad scope for identified activities related to a certain cyber operation is broadly categorised as situational awareness. This capability is an essential aspect of cyber defence, predicated on observing and understanding the operational context of a certain incident across a broad range of potential attack vectors. The presented system, however, via the use of models, makes another leap forward in being able to state with high probability that a series of incidents, which before

were not apparent to be connected, are indeed linked by some everyday operational activity underground and are using related cyber tradecraft. This has a direct consequence for the speed and accuracy of related incident response compared to manually hunting for the same level of connection between diverse security incidents (Agbehadji et. al., 2020).

Notably, the system allows for a ranked and quantifiable demonstration of the confidence of the connection based on a large volume of network telemetries provided by next-generation network sensors. Most of these solutions propose not only the algorithms and models designed to improve detection with a high level of accuracy but also approaches to solve other challenges, such as class imbalance, which commonly occurs for malicious activities.

In all of this, the Security Team delivers essential human supervision, verification, and strategic organisation. When the algorithm detects an anomaly and triggers automated responses (like isolating a breached device), the Security Team assesses the alert to confirm whether the behaviour is genuinely harmful or a harmless anomaly, and then offers contextual analysis informed by the understanding of the organisation's infrastructure and policies. If an incident needs escalation, the Security Team coordinates with the larger team to implement wider containment strategies and reduce impact.

Besides confirming and addressing incidents, the Security Team participates in proactive threat hunting and forensic investigation. They examine irregularities identified by the algorithm, identify attack paths, and evaluate the extent of the effect. Their results are incorporated into the AI systems to enhance future threat identification and minimise false alarms. This ongoing feedback cycle aids in improving security policies and boosts the organisation's overall cybersecurity stance (Ullah et al., 2022).

4. Case Studies and Examples of Successful Predictions

In 2006, Global 2000 enterprises used threat intelligence to predict and automate responses to IT security threats by 2010 was a big prediction. Since then, this prediction has been realised, and threat intelligence is now a focal point of the industry. There is strong investment from companies, and vendors are offering specialised products whereas governments are also involved in the threat intelligence community in managing cyber espionage information (Sarker et al., 2021).

Several examples show the successful use of predictive algorithms in security operations. Predictive algorithms help improve security measures for military applications. Predictions help to mitigate the impacts of severe weather in winter weather alerting systems. Historical data is used by market indexes to forecast trends in the market. The use of predictive techniques is employed by Intelligent Agencies to prevent terrorist activities. Furthermore, the evaluations of mental patient data are analysed with the help of a computer to predict the diagnoses and mental health outcome of a patient. Predictive algorithms used by the United States Department of Defense have also saved millions of dollars a year in preventing hack attempts during election years (Kaur et al., 2023).

However, effective predictions are common in the preparation of major events, drought forecasting, and university class scheduling. The patterns serve as a basis for creating accurate danger predictions. Threat prediction looks like best practices today, and it evaluates historical patterns to predict cybersecurity incidents over an 18-month period. Organisations can better prepare for future cybersecurity challenges by leveraging big data and other resources to improve prediction accuracy (Zografopoulos et al., 2021).

4.1. Case Studies of Notable Cyber Threat Predictions

4.1.a. Case Study: Ukraine Power Gride Attack (2015)

Predictive models identified vulnerabilities in the Ukrainian power grid, highlighting the importance of anticipating state-sponsored attacks (HIMSS, 2022). By identifying vulnerabilities in advance, organisations can mitigate the weaknesses and minimise the risk of a seemingly successful attack.

4.1.b. Case Study: Financial Sector Threat Prediction

In 2020, predictive analysis helped prevent a major phishing campaign targeting global banks, saving millions in potential losses (Lallie et al., 2021).

5. Challenges and Ethical Considerations in Cyber Threat Prediction

Predictive power about general human behaviour is inherently limited, as it has emerged from consistent research across various disciplines. While there may be improvements to the state of predictive power, acting on these predictions can result in false positives, particularly if given privileged weight by analysts in making decisions. Technologically, the models are limited by their technology and data quality. If we rely on a snapshot of the cyber threat or underlying data, we could easily miss crucial adverse events with minor cyber operation impacts on society. Privacy and ethical challenges also occur when using such technology. There are also problems with the reliable testing of predictive algorithms, as it is difficult to determine their recall, precision, bias, and test ground truth. Lastly, many worry that these mechanisms could be used to target individuals or groups because they are seen as a threat in the making. Rather than preventing behavioural harm, this may create a self-fulfilling prophecy. Therefore, predictive algorithms carry with them the power to pick future enemies as much as they do to prevent them (Nowotny, 2021).

Quantitative decision-making has an adverse impact in various areas. There is potential for abuse and privacy threats. Law enforcement and intelligence agencies have tested or used predictive mechanisms for immigration or criminal behaviour forecasting. In reviewing the use of predictive policing algorithms, there are several potential biases. First, predictive algorithms have been found to magnify existing social disparities. They may project a biased, or worse, racist policing model into the future, which has consequences through a feedback loop. The use of big data is also likely to exacerbate this because such data often inherit social disparities (Scatiggio, 2020).

Furthermore, using witness statements in evaluating predictions can create a circularity in validation. This can result in self-fulfilling prophecies: an individual labelled a threat may become one because of the pressures of surveillance. In a predictive policing context, systemic reporting is a problem because targeting already-targeted communities results in an attack on both discrimination practices and fundamental constitutional freedoms. Therefore, fairness and equity should be the primary measurement. Policymakers should not make predictions on any other grounds or ideologies but ensure the same rights for all citizens (Montasari, 2023).

5.1. Bias and Fairness in Predictive Models

The idea that one can predict criminal intent, likelihood of recidivism, or any future occurrence based on past occurrences has deeply ingrained biases at its core. Training predictive models is a human-driven process affected by prejudices at macro, meso, and micro levels. At a minimum, those biases will be reflected in the system, if not heightened, through heavy automation and targeted efforts. It is essential to understand that the collection of ‘anonymised,’ strongly aggregated data can still carry comparative or predictive information for marginalised and underserved individuals (Hong et al., 2020).

Considering these issues, it would be irresponsible to give decision-makers access to predictive system

output without properly examining and rigorously testing its underlying biases and fairness levels with real-world stakeholders and decision-makers. A pressure test, or adversarial test, can be conducted to figure out whether the predictions generated are fair and whether they represent reality. In other domains, there have been efforts to use datasets from underrepresented groups to help recognise flaws in predictive models. We should consider creating or cultivating datasets that challenge unfair assumptions in cyber threat prediction. These datasets can help test adversarial and re-identify biased predictors and help determine new methodologies to increase fairness and reduce decision-making errors with cyber threat predictors (Wang et al., 2022).

There is a notion of bias in decision-making, even for very accurate predictive models, in the cybersecurity community. End users prefer or require their predictive technologies to be fair due to ethical considerations or potential concerns about negative impacts. The predictions will still be biased, but creating ethical guidelines and providing support for making the technologies as equitable as possible provides good stakeholder engagement and increases the ethical posture within the activity. In this way, the larger community can trust and use the models on a grander scale in actual decision-making processes. Furthermore, responsible bias awareness increases the scrutiny under which the developers and users of such technologies operate and discourages collusion to maintain unfair practices. By publicly engaging communities in developing a predictive model's fairness, an understood accountability culture is created that can unfold further scrutiny on emerging technologies (Ahmad et al., 2022).

Conclusion

Predicting future cyber threats is necessary to develop robust and proactive cybersecurity risk management strategies. The aspiration of merely reacting to modern threats needs to be revised in the face of today's complex cyber threats, where advanced technologies and state-sponsored activities are fuelling them. Organizations can enhance their capabilities to predict and counter potential threats by using predictive models that employ a combination of quantitative methods, such as statistical analysis and machine learning, with qualitative methods, such as expert insights-driven approaches. Predictive analysis has been shown to prevent high-impact breaches through real-world examples like the SolarWinds attack and the Ukrainian power grid attack. Furthermore, integrating AI and ML offers real-time threat detection and enhanced situational awareness, facilitating faster and more accurate incident response. Nevertheless, due care must be taken to address the ethical considerations - data quality, bias and fairness - for reliably and equitably predictive models. To build comprehensive cybersecurity frameworks, it is vital to coordinate with industries, policymakers, and international bodies collaterally. Future pathways involve the incorporation of blockchain for data reliability, enhancing international cybersecurity collaboration, and guaranteeing that all technological progress is conducted ethically. These tactics allow organizations to cultivate resilience and make resource distribution choices to stay ahead of cyber threats in the ever-changing cyberspace.

References

1. Agbehadji, I. E., Awuzie, B. O., Ngowi, A. B., & Millham, R. C. (2020). Review of big data analytics, artificial intelligence and nature-inspired computing models towards accurate detection of COVID-19 pandemic cases and contact tracing. International journal of environmental research and public health, 17(15), 5330. https://doi.org/10.3390/ijerph17155330

2. Ahmad, K., Maabreh, M., Ghaly, M., Khan, K., Qadir, J., & Al-Fuqaha, A. (2022). Developing future human-centered smart cities: Critical analysis of smart city security, Data management, and Ethical challenges. Computer Science Review, 43, 100452. https://doi.org/10.1016/j.cosrev.2021.100452
3. Akoto, W. (2021). International trade and cyber conflict: Decomposing the effect of trade on state-sponsored cyber-attacks. Journal of Peace Research, 58(5), 1083-1097.
4. Alabdan, R. (2020). Phishing attacks survey: Types, vectors, and technical approaches. Future internet, 12(10), 168. https://doi.org/10.3390/fi12100168
5. Alexei, L. A., & Alexei, A. (2021). Cyber security threat analysis in higher education institutions as a result of distance learning. International Journal of Scientific and Technology Research, (3), 128-133.
6. Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. Frontiers in Computer Science, 3, 563060. https://doi.org/10.3389/fcomp.2021.563060
7. Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M. V., Calcavecchia, F., Anderson, D., & Flahault, A. (2020). Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. BMC medical informatics and decision making, 20, 1-10. https://doi.org/10.1186/s12911-020-01161-7
8. Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics, 12(6), 1333. https://doi.org/10.3390/electronics12061333
9. Berdik, D., Otoum, S., Schmidt, N., Porter, D., & Jararweh, Y. (2021). A survey on blockchain for information systems management and security. Information Processing & Management, 58(1), 102397. https://doi.org/10.1016/j.ipm.2020.102397
10. Buchanan, B. (2020). The hacker and the state: Cyber-attacks and the new normal of geopolitics. Harvard University Press.
11. Duo, W., Zhou, M., & Abusorrah, A. (2022). A survey of cyber-attacks on cyber physical systems: Recent advances and challenges. IEEE/CAA Journal of Automatica Sinica, 9(5), 784-800. DOI: 10.1109/JAS.2022.105548
12. Genschel, P. (2022). Bellicist integration? The war in Ukraine, the European Union and core state powers. Journal of European Public Policy, 29(12), 1885-1900. https://doi.org/10.1080/13501763.2022.2141823
13. Hong, S. R., Hullman, J., & Bertini, E. (2020). Human factors in model interpretability: Industry practices, challenges, and needs. Proceedings of the ACM on Human-Computer Interaction, 4(CSCW1), 1-26. https://doi.org/10.1145/3392878
14. Kaloroumakis, P. E., & Smith, M. J. (2021). Toward a knowledge graph of cybersecurity countermeasures. The MITRE Corporation, 11, 2021.
15. Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion, 97, 101804. https://doi.org/10.1016/j.inffus.2023.101804
16. Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & security, 105, 102248. https://doi.org/10.1016/j.cose.2021.102248

17. Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports, 7, 8176-8186. https://doi.org/10.1016/j.egyr.2021.08.126
18. Mishra, N., & Pandya, S. (2021). Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review. IEEE Access, 9, 59353-59377. DOI: 10.1109/ACCESS.2021.3073408
19. Montasari, R. (2023). The application of big data predictive analytics and surveillance technologies in the field of policing. In countering cyberterrorism: the confluence of artificial intelligence, cyber forensics and digital policing in US and UK National Cybersecurity (pp. 81-114). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-21920-7_5
20. Nassar, A., & Kamal, M. (2021). Machine Learning and Big Data analytics for Cybersecurity Threat Detection: A Holistic review of techniques and case studies. Journal of Artificial Intelligence and Machine Learning in Management, 5(1), 51-63.
21. Nicholls, J., Kuppa, A., & Le-Khac, N. A. (2021). Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. Ieee Access, 9, 163965-163986. doi: 10.1109/ACCESS.2021.3134076
22. Nowotny, H. (2021). In AI we trust: Power, illusion and control of predictive algorithms. John Wiley & Sons.
23. Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. Sustainability, 15(18), 13369. https://doi.org/10.3390/su151813369
24. Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. SN Computer Science, 2(3), 173. https://doi.org/10.1007/s42979-021-00557-0
25. Scatiggio, V. (2020). Tackling the issue of bias in artificial intelligence to design ai-driven fair and inclusive service systems. How human biases are breaching into ai algorithms, with severe impacts on individuals and societies, and what designers can do to face this phenomenon and change for the better.
26. Ukwandu, E., Farah, M. A. B., Hindy, H., Brosset, D., Kavallieros, D., Atkinson, R., ... & Bellekens, X. (2020). A review of cyber-ranges and test-beds: Current and future trends. Sensors, 20(24), 7148. https://doi.org/10.3390/s20247148
27. Ullah, W., Ullah, A., Hussain, T., Muhammad, K., Heidari, A. A., Del Ser, J., ... & De Albuquerque, V. H. C. (2022). Artificial Intelligence of Things-assisted two-stream neural network for anomaly detection in surveillance Big Video Data. Future Generation Computer Systems, 129, 286-297. https://doi.org/10.1016/j.future.2021.10.033
28. Wang, A., Ramaswamy, V. V., & Russakovsky, O. (2022, June). Towards intersectionality in machine learning: Including more identities, handling underrepresentation, and performing evaluation. In Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency (pp. 336-349). https://doi.org/10.1145/3531146.3533101
29. Zografopoulos, I., Ospina, J., Liu, X., & Konstantinou, C. (2021). Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. IEEE Access, 9, 29775-29818. DOI: 10.1109/ACCESS.2021.3058403.