Cybersecurity and Strategic Management

Budi Gunawan
Professor, Cyber Security Study Program, budigunawan@stin.ac.id

Barito Mulyo Ratmono
Deputy Governor, Technology of Intelligence Study Program, barito.mr@stin.ac.id

Sekolah Tinggi Intelijen Negara, 9VQQ+6J2, Sumur Batu, Kec. Babakan Madang, Kabupaten Bogor, Jawa Barat 16810, Indonesia

Ade Gafar Abdullah
Professor, Technological and Vocational Education Study Program, ade_gaffar@upi.edu

Universitas Pendidikan Indonesia, Jl. Dr. Setiabudi No. 229, Isola, Kec. Sukasari, Kota Bandung, Jawa Barat 40154, Indonesia

Abstract

Against the backdrop of rapidly evolving technologies and increasingly complex communications networks, cybersecurity is becoming a key aspect of strategic planning. Protecting information, financial, reputational and other assets from increasingly frequent and sophisticated cyberattacks depends on the ability to develop and continually update a comprehensive, proactive approach that takes into account a wide range of factors. The state of national cybersecurity has become one of the key indicators of the level of development along with «classic» indicators (GDP, etc.). The recently emerged research area of «cybersecurity economics» is constantly being enriched with new knowledge and approaches.

The article analyzes the risks to the cybersecurity system at different levels and the main measures to strengthen it, and assesses the dynamics of management trends. Key competencies relevant for professionals in this field are outlined.

Keywords: cybersecurity; intelligence; strategic management; risk management; bibliometrics analysis

Citation: Gunawan B., Ratmono B.M., Abdullah A.G. (2023) Cybersecurity and Strategic Management. *Foresight and STI Governance*, 17(3), 88–97. DOI: 10.17323/2500-2597.2023.3.88.97

Introduction

As more and more businesses move their operations online, cybercriminals are beginning to stake their claim in the digital realm, which imposes high costs on the economy[1]. Cyber security emerged as a countermeasure to protect the online environment from cyber-attacks, damage, improper use, and economic espionage. The perception of cyber security has shifted from being just an "IT issue" alone to being a "strategic management issue" and to being a "techno-legal-management issue" due to the ever-increasing sophistication of cybercrime in its attack approaches and techniques (Mantha, García de Soto, 2021). Even though technology is developing rapidly, human is still the primary doer and plays a vital role in controlling the process of securing a country from attacks and threats. We cannot fully depend on technology because of its drawbacks such as false decision, lack of transparency, or overreliance. It is in line with the goal of "Society 5.0", a strategic model that has been initiated in Japan and focuses on balancing human and technology. A "5.0 society" is an "intelligence society" in which physical space and cyberspace are highly intertwined. The relation between Industry 4.0 and Society 5.0 are related ideas that talk about how cutting-edge technologies are used in business and in society as a whole. Society 5.0 calls for a deeper integration of technology to create a human-centered society that addresses social issues and creates new economic value. Industry 4.0, on the other hand, focuses on digitizing and automating manufacturing processes. Balancing social and societal problems is a complex and ongoing challenge that requires a multifaceted approach. The first solution to be concerned is stakeholder engagement. Engaging with stakeholders, including customers, employees, investors, and community groups, can help organizations to understand the social and societal issues that matter to them. Overall, balancing social and societal problems requires a comprehensive approach that considers the impact of an organization's actions on a wide range of stakeholders.

The previous studies analyzed the relationship between cyber security and management but focused on the era of industry 4.0, cyber-physical systems, enterprises, and public policy implications (Alahmari, Duncan 2020; Kharchenko et al. 2019; Kure et al., 2018). However, this study will try to emphasize the relationship between cyber security in management and society 5.0. In addition, the inclusion of new technologies in cyberspace, such as artificial intelligence (AI), machine learning (ML), data analytics, cloud computing, quantum cryptography, and the Internet of Things (IoT), has made cybersecurity a complex domain that requires more in-depth research in order to keep up with the growth of cybercrime (Sobb et al., 2020). As a result of ongoing trends and difficulties, the global market for cyber security has expanded dramatically, and it is anticipated that it will reach approximately 259 billion USD by the year 2025 (Dhawan et al., 2021). The nature of research into cyber security technologies, systems, and concerns has shifted to become more interdisciplinary and international in scope since the national threats mostly come from outside the countries. In a broader sense, the following are some of the areas that fall under the theme of cyber security research: management; critical infrastructure; risk assessment; risk management; economics; investments; information services; public works; decision-making; human resources; and education. When searching for prior research on cyber security in management through the Scopus database, it becomes clear that the body of written work in this field is seeing a rapid expansion. Therefore, the author has been constructed the following research questions:

1. What is the relationship between the keywords of cybersecurity and management in terms of co-occurrence?
2. What are the dynamics of the concept in the field of cybersecurity?

Methods

This study employed a quantitative method by using the bibliometrics analysis technique. This study's analysis and mining process would draw on the Scopus database as one of the most extensive incredible databases (Mongeon, Paul-Hus, 2016).nIn the search strategy, the author divided the keywords into two topics. The first keyword typed in the Scopus database was relevant to "Cyber security". Afterward, it was followed by the "management" keyword in the next topic. Before the filter was applied, the search result revealed that there were 3.285 documents. However, since the author was only interested in the advancement of cyber security in management from articles and because the language was filtered into English, the author additionally focused on narrowing the keywords in the final articles of a journal to tighten the results. The final result was 780 articles found in the Scopus database. The following keywords were constructed to explore the data through the aforementioned database on the 23rd of August 2022 and gained 780 data from Scopus:

(TITLE-ABS-KEY ("cyber security") AND TITLE-ABS-KEY (management*)) AND (LIMIT-TO (PUBSTAGE, "final")) AND (LIMIT-TO (DOCTYPE , "ar")) AND (LIMIT-TO (LANGUAGE , "english")) AND (LIMIT-TO (SRCTYPE , "j"))*

[1] The term "cybercrime" refers to a broad category of online offenses that includes breaking into information systems, spreading computer viruses, stealing identity information, stealing political and industrial secrets, spreading misinformation, and attempting to influence global opinions and election results. Cyberattacks may employ various techniques, including viruses, worms, botnets, ransomware, and social engineering. Individuals who commit crimes online may do so as part of a more extensive, more coordinated operation, as is the case of institutions that support cyberattacks or states that sponsor cyberattacks.

In this analysis, the chosen number of documents was 5, and the result of thresholds was 314 out of 5663 keywords. Similar to the co-occurrence network analysis, this quantitative analysis will deeply analyze the evolution of thematic words used since the first research linked with "cyber security" and "management".

In the method section, the data will be refined using software named Openrefine to filter and unite similar terminology but in different spellings. Furthermore, the data visualization will use VOSviewer, R programming, and Draw.io to highlight the results. Through the VOSviewer visualization process, the author found some similar words which could be united into one terminology. The table 1 gives a list of words that have been associated.

Table 1. **Thesaurus in VOSviewer**

Label	Replace by
Cybersecurity	Cyber security
Cyber-attacks	Cyber attacks
IoT	Internet of things (IoT)
humans	human

Source: authors.

The next section will portray the scope of keywords related to cyber security in management based on the co-occurrence, thematic evolution, publication distribution, and co-citation analysis to decipher the research development contribution.

Results

Co-occurrence analysis (network analysis)

The following visualization describes the clusters shown by cyber security, which are divided into 7 clusters based on colors such as yellow, sea blue, dark blue, green, purple, orange, and red. The author observed from figure 1 that the term "cyber security" widely spreads in the yellow and red clusters, with the highest number of items. Based on the figure, the keyword "Cyber security" is highly and closely linked with "Network security." "Cyber security" occurred up to 532, and "network security" reached 172 occurrences. Along with the co-occurrence result, the total link strength of "Cyber security" was also the highest, up to 2930, and the total link strength of "network security" was up to 1334. The aforementioned clusters were connected to many interesting links to other keywords such as investments, human, critical infrastructure, information services, decision-making, public policy, risk management, and economics. It provided sophisticated previous research about risk management in cyber security. With the previous research statement, every country and scientist agree that a cyber security management model is needed to secure critical infrastructures such as internet voting systems, banking systems, and energy infrastructure. There is no role model of the cyber security management paradigm, yet many governments recognize the necessity to secure their essential resources (Katsikeas et al., 2021).

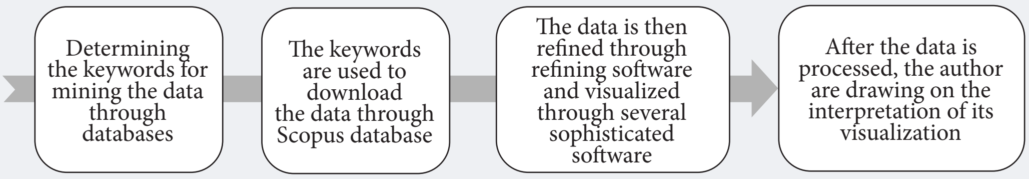
To this end, the keyword "cyber security" was also highly linked to "human," which will relate to human management in handling cyber security. The role of human management in handling cyber security focused on the decision of how to handle cyber threats in the right way or strategy. Over 39% of security concerns are tied to the human aspect, and 95% of successful cyber-attacks are generated by human error, mostly insider threats. Lack of user understanding of cyber risks is a severe cybersecurity issue (Alsharif et al., 2021). However, the author will also highlight the keywords.

Thematic evolution of Cyber Security in Management

This study will analyze the keywords' trends based on co-occurrence and thematic evolution in the field of cyber security in management. The author was analyzed with thematic evolution visualization and three field plots of visualization. It stated that the words' evolution mainly occurred in computer security, cyber security, and electric power transmission networks, and the themes correlate to computer security, female, human, network security, automation, cyber security, information systems, and air traffic control.

In conformity with the results, the author could dissect that cyber security now has automation, computer security, information systems, and network security and is still correlated with cyber security. The relation of cyber security (1999-2019) and cyber security (2020-2022) in the Scopus database were resulting several words such as cyber security, cyber threats, personal computing, internet of things, risk perception, security management, resource allocation, and complex networks that highly occurred up to 203 occurrences. It

Figure 1. **Bibliometric Process**


Determining the keywords for mining the data through databases
The keywords are used to download the data through Scopus database
The data is then refined through refining software and visualized through several sophisticated software
After the data is processed, the author are drawing on the interpretation of its visualization

Source: authors.

raised the overview that the development of technology hit up the topic of cyber security (Marcantoni et al., 2022; Morgan et al., 2022).

The discussions of Cyber security issues started near 1980[2]. The first start theme in Scopus related to cyber security was in 1999 and continued hitherto. Furthermore, cyber security is in tandem with the word “security management”. Cyber security management is concerned with reducing uncertainties and managing risks perceived by a security system (Mouti et al., 2022). One of the key objectives of cybersecurity management is to reduce uncertainties associated with security risks. This involves identifying potential risks, evaluating the likelihood of their occurrence, and assessing the potential impact on the organization. By doing so, cybersecurity managers can prioritize risks and allocate resources to those areas that are most vulnerable or likely to be targeted by attackers.

Another important aspect of cybersecurity management is risk management. This involves developing strategies to manage risks associated with cybersecurity threats. Risk management strategies can include implementing security controls, such as firewalls, antivirus software, and intrusion detection systems, to prevent or detect security breaches. It can also include developing incident response plans to ensure that the organization can respond effectively to a security incident.

Based on the findings of the three field plots, a three-field plot, also known as a Sankey diagram, is used to illustrate the most influential authors, the most popular keywords plus, and the most influential affiliations. Based on the Scopus database, this graph demonstrates a sequence of links between data in a flow. It describes the association between the strongest and heaviest linkages between factors such as journals, keywords, and the most influential or relevant researchers in the field. Liu Z., Wang I., and Masacci F. were the individuals who had the most vital links to the keyword “cyber security,” which is notable. These three authors all have contributions in the same second heavier link; one of those contributions has the keyword “risk management.” The connection between “cyber security” and De Montfort University is the most robust one, which suggests that the university is responsible for including the vast majority of publications that contain this keyword. It is something that can be seen by following the flow from the keyword field to the section of the journal. Because of this, it is possible to emphasize the growth of cyber security research by using the primary bibliometric findings, which served as the basis for a literature analysis that zeroed in on the most significant concerns. Additionally, the bibliometric data revealed increased interest in studying cyber security and risk management strategies to protect against cyberattacks.

Discussion

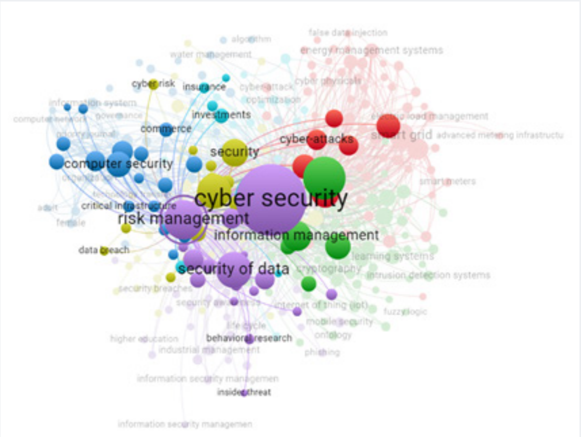
This section will draw on the discussions of the result analysis vis-à-vis the most contemporary issues flanked on the topic of cyber security and management.

The prior results slightly portrayed the relationship between cyber security and strategic management, including investments, humans, critical infrastructure, information services, decision-making, and economics.

Cyber Security and Investments

A country’s investment in cyber security is crucial since cyber-attacks could come physically or digitally (Li, Liu, 2021). Currently, most economic, commercial, cultural, social, and governmental activities and interactions of countries at all levels, including individuals, non-governmental organizations, government, and governmental institutions, are carried out in cyberspace of micro-grid. These activities and interactions can be dissected into several categories: commercial, cultural, social, and economic (Aghajani, Ghadimi, 2018). The focus of national security in investments is on optimizing the work units and how the country could secure itself from a cyber-attack. This issue created a particular unit for handling cyber security as a crucial investment. Before the establishment of cyber security unit, cyber-attacks’ cases are the responsibility of an intelligence agency in technological deputy. Nevertheless, the technological deputy in intelligence is very opponent with the deputy of cyber security in intelligence. It could be stated that technological unit is only responsible for the technical technology problems but cyber security deputy covers and blends the cyber security of national intelligence.

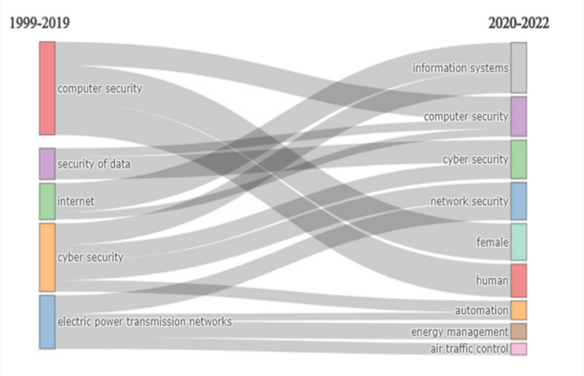
Figure 2. **Risk Management Co-occurrence Analysis**



Source: authors.

[2] https://blog.avast.com/history-of-cybersecurity-avast, accessed 14.06.2023.

Figure 3. **Thematic evolution map and three fields plot**



Source: authors.

Another reason for establishing cyber security deputies is the spread of fake news in society, especially in a political context. Fake news and its relevance held the importance of altering numerous aspects of diverse entities, ranging from a city problem to a country's global relativity. Various approaches are available to collect and determine fake news (Dutta et al., 2023). Primary research stated that the rise of fake news is begun from digital sources and social media (Alsuliman et al., 2022; Isa et al., 2022). Many studies have been developed on methods to improve rumor classification, particularly misinformation detection on social media, with promising results in recent years.

Cyber security has seven pillars of cyber resilience: patient, persistent, preserving, proactive, predictive, preventive, and preemptive (Carayannis et al., 2021). Preventive and preemptive measures are critical cornerstones of cyber resilience. Both attempt to mitigate cyber threats and secure an organization's essential assets and systems, but their approaches differ. Preventive measures are intended to keep cyberattacks from happening in the first place. These procedures seek to detect vulnerabilities and put in place security safeguards to keep cybercriminals from abusing them. Firewalls, access controls, encryption, and antivirus software are examples of preventive measures. These techniques contribute to reducing the attack surface and making it more difficult for cybercriminals to breach an organization's defenses.

Preemptive are intended to anticipate and prevent cyberattacks before they occur. These are more proactive methods that entail taking action based on intelligence and threat assessments. Threat hunting, penetration testing, and vulnerability assessments are examples of preventive approaches. These techniques assist firms in identifying and mitigating possible vulnerabilities before cybercriminals may exploit them. In summary, preventative measures are intended to avert assaults, whereas preemptive measures are intended to anticipate and prevent attacks before they occur.

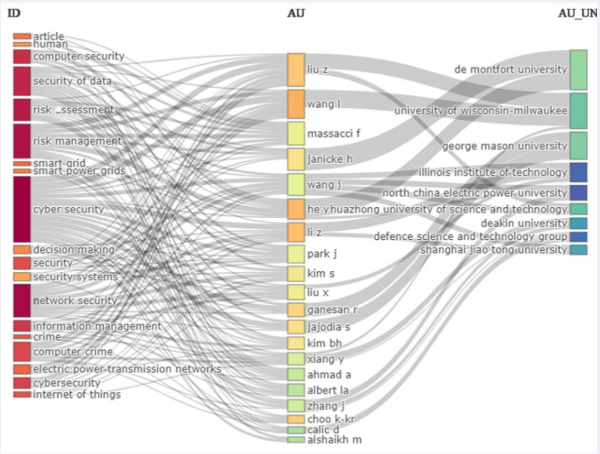
The implementation of ambidextrous cybersecurity involves balancing the need for strong cybersecurity defenses with the need for agility and flexibility in responding to cyber threats. This can be achieved by incorporating the seven pillars (7Ps) of cyber resilience into an organization's cybersecurity strategy. To implement ambidextrous cybersecurity, organizations should first assess their current cybersecurity posture and identify areas where they may be vulnerable to cyber threats. They should then develop a comprehensive cybersecurity strategy that incorporates both defensive and adaptive measures, using the 7Ps framework as a guide. Table 2 lists some key steps to implementing ambidextrous cybersecurity.

Table 2. **Key Steps to Implementing Ambidextrous Cybersecurity**

Action	Description
Develop a risk management plan.	This involves identifying critical assets, systems, and data, and assessing the risks associated with them. This information can be used to develop a risk management plan and prioritize cybersecurity investments.
Implement security controls.	This involves implementing security controls, such as firewalls, access controls, and encryption, to prevent or mitigate cyber threats. This pillar focuses on protecting critical assets and systems from unauthorized access or use.
Implement monitoring and detection tools.	This involves implementing tools and processes to detect cybersecurity incidents as they occur. This can include intrusion detection systems, security monitoring tools, and incident response plans.
Develop an incident response plan.	This pillar focuses on developing and implementing an incident response plan to contain, mitigate, and recover from cybersecurity incidents. This involves developing procedures for responding to incidents, such as isolating affected systems, preserving evidence, and notifying relevant stakeholders.
Develop a recovery plan.	This involves developing a recovery plan to restore systems and data following a cybersecurity incident. This may involve restoring data from backups, rebuilding systems, or implementing new security controls to prevent future incidents.
Continuously assess and update cybersecurity strategies.	This pillar focuses on continually assessing and updating cybersecurity strategies to address new and emerging threats. This may involve updating risk management plans, implementing new security controls, or providing employee training to address new threats.
Develop a communication plan.	This involves developing a communication plan to inform stakeholders about cybersecurity incidents, risks, and responses. This may involve communicating with employees, customers, partners, and regulators to ensure that they are aware of cybersecurity risks and measures in place to address them.

Source: authors.

Figure 4. **Three field plots**



Source: authors.

Previously the police department of cyber security and corporate security services prevented the development of majority cyber-attacks. However, the main focus of police agencies is on the function of repressive prevention or law enforcement, yet in cyber security, intelligence will focus on preemptive function (Kopotun et al., 2020). Therefore, the cyber security deputy in intelligence is a step of strategy to secure all the attacks on the nation[3].

Cyber Security and Human Resource

The strong connections between cyber security and human resource are fundamental (Mitrofanova et al., 2017). The rising digitization of most technologies we use in our personal and professional life makes cyber-attacks a hazard for governments or corporations and ordinary people. It is common practice to consider humans the weakest link in the cyber security chain. It is because any technical security solution is still susceptible to failures caused by human mistakes (Gratian et al., 2018). The human resource in cyber security must master not only technology, including software or hardware, but also cyberspace and cyberculture and should be trained under the intelligence agency (Pollini et al., 2022). Meanwhile, the recruiting procedure used in the national Cyber Security Intelligence agency is considered too academically oriented. It places a greater emphasis on academic qualification than on the overall quality of a candidate, and it does not consider academic qualifications. The requirements of the human resource who work with cyber security are gaining a bachelor's degree, especially in informatics. However, since the era's development, human resource requirements have expanded to the soft skills of visual communication design, culture studies, and culture and media studies that require the staff to combine some skills and academic backgrounds (Furnell, Bishop 2020; Scanlan et al., 2020). Figure 5 presents the overview of the skills required for the intelligence staff in the cyber security department.

In the recruitment process of cyber security staff, the phases of tests are various, starting from medical check-ups, academic tests, competence tests, psychological tests, and ideological mental tests. It will then relate to the training after being recruited as cyber security staff. The following examples are the summary of intelligence education focusing on cyber security (AlDaajeh et al., 2022; Stephanidis, Eds, 2020):

- Strengthening intelligence's mental and moral
- Intelligence basic knowledge
- Relevant materials and activities related to intelligence
- Scanning cyber threats and ensuring cyber security
- Knowledge integration between report progress and research

Human resources can contribute significantly to cybersecurity by educating and raising awareness, recruiting and hiring qualified personnel, creating effective policies and procedures, ensuring compliance, and participating in incident response. By working together, human resources and cybersecurity teams can create a robust cybersecurity culture that helps prevent cyber attacks and safeguard critical infrastructure.

Cyber security and critical infrastructure

Even though the public and private sectors spend millions of dollars a year on technologies, security software, and hardware devices that will raise the level of cyber security within their companies, these companies are still susceptible to cyber-attacks. The primary issue with the current state of affairs is that computer network security is still typically regarded as a technical component or piece of technology that can be readily installed within an organization. That implementation will guarantee computer network security. This mentality needs to shift since, in today's world, ensuring network security involves more than just using the appropriate technologies (Limba et al., 2017).

Modern Industrial Control Systems (ICS) manages many vital activities worldwide. A typical ICS incorporates computerized devices, control systems, and networking appliances to manage industrial processes over broad geographic areas. ICS supports vital national infrastructures like water treatment, energy production, and transportation. A successful attack

[3] Indonesia already has a framework and policy in place for cyber security, which are managed by government agencies and the official community. Cyber security policies are coordinated by the Ministry of Communications and Information Technology (MCI). The Information Security Coordination Team, the Directorate of Information Security, and the Indonesia Security Incident Response Team on Internet Infrastructure are three government bodies involved in cyber security in Indonesia (ID-SIRTII).

Table 3. **Some applications of cybersecurity for protecting vital infrastructure**

Application	Description
Stopping cyber assaults	Cyber attacks can damage critical infrastructure systems and create widespread outages, jeopardizing individual and community safety and security. Cybersecurity measures can assist avoid these attacks by identifying vulnerabilities and putting mitigation measures in place.
Ensure system availability	To protect the safety and well-being of individuals and communities, critical infrastructure systems must be available and operational at all times. Cybersecurity measures can assist in ensuring that systems are available and secure against cyber threats.
Safeguarding sensitive data	Vital infrastructure systems frequently contain sensitive data that hackers value, such as personal information and intellectual property. Cybersecurity measures can help safeguard this information against illegal access and disclosure.
Regulation compliance	Critical infrastructure systems are subject to a variety of regulations, including the NIST Cybersecurity Framework, which provides guidance for implementing cybersecurity safeguards to protect critical infrastructure systems. In the case of a cyber attack or other cybersecurity issue, a well-designed incident response plan can help guarantee that critical infrastructure systems are safeguarded and the incident's impact is reduced.

Source: authors.

can shut down the infrastructure, causing industrial stoppages or safety issues for people, the environment, and assets. Similarly, operating a process when the infrastructure is under assault or corrupted has potentially catastrophic safety implications (Catota et al., 2019; Firoozjaei et al., 2022). Hence, a country must develop a good critical infrastructure for security, such as building advanced laboratories (de Soto et al., 2022). In this case, Cyber-Physical Systems (CPS) are the world's critical infrastructure and could affect human life in the future. In recent years, CPS has seen a rise in connections, which has raised cybersecurity concerns. Aside from classic information system vulnerabilities, CPS has new issues due to heterogeneous devices and protocols and stringent reliability requirements (Michalec et al., 2022).

The critical infrastructure could be formed as laboratories for practice, intelligence school and training, qualified departments and materials, and cyber-physical systems (Qi et al., 2018; Quincozes et al., 2022). In developing the critical infrastructure, establishing a new school department, innovative campus, and medical intelligence could strengthen national security from cyber-attacks or national threats. Therefore, the development of critical infrastructure needs a system of Public-private Partnership (PPP) to mitigate the risk against critical infrastructure and manage the quality of the infrastructure. Critical infrastructure is also related to how governments and private businesses understand their roles in raising the degree of national cybersecurity. It discovered a disjunction between what each side expects from the other side in building advanced national security (Carr, 2016; Watanabe, 2019).

Cybersecurity is vital for safeguarding critical infrastructure against cyber assaults. Critical infrastructure refers to physical and digital systems that are necessary for civilization to function, such as power grids, transportation systems, water supply systems, and communication networks. These systems are interrelated and interdependent, and disturbances in one can have serious consequences in others. Table 3 provides some examples of how cybersecurity might help secure vital infrastructure:

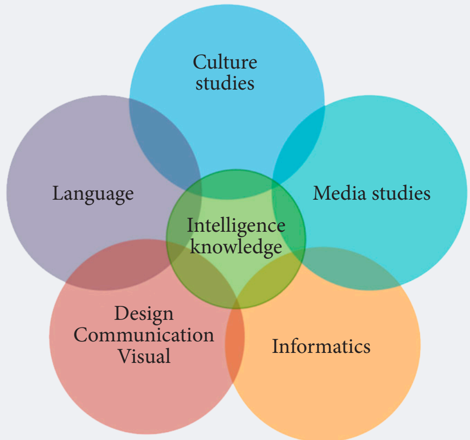
Cyber security and information services

IT implementation in most areas of the state, economy, and society offers various potentials for automating management operations and increasing the efficiency and quality of rendered services (Boiko et al., 2019; Rahiman et al., 2021). Unawareness of reverse socio-technical dangers can lead to an unsuspecting employee leaking critical corporate data or compromising information security. Even though programmed systems can detect phishing emails and websites, they are not 100% accurate (Mantha, García de Soto, 2021). Technological solutions will not guard against cyber dangers or attacks like phishing. Hence, companies must acquire procedures to protect individuals from phishing risks, attacks and strategies to raise awareness. Information and data security awareness help prevent social engineering attacks. Information and data security management need constant vigilance (Rajan et al., 2021).

Cyber security and decision making

Information flows in cyber security are now considering the use of decision-making from artificial intel-

Figure 5. **Skills Needed for Cyber Security Staff**



Source: authors.

Table 4. **Steps of filtering information by using artificial intelligence to decide the final information**

Step	Description
Collecting information	The intelligent members gained information from two sides: available information from any sources such as social media, media, news, and societal issues and close information from its agents or intelligence members (Hautamaki, Kokkonen 2020). It should be noted that intelligence information must have three patent prerequisites: fast, precise, and accurate.
Artificial intelligence	An artificial intelligence machine will then process it to learn and decide from the collected data.
Expert judgments	The decision-making of information processing is considered and filtered by the experts before deciding the final information.
Situational awareness	Since the ever-increasing complexity of the dynamics of cyber threats, it is currently more complicated than it has ever been for enterprises to acquire in-depth insights into their current state of cyber security. As a result, businesses rely on Cyber Situational Awareness (CSA) to assist them in gaining a deeper comprehension of the dangers posed by cyber events and the consequences these threats can have (Jiang et al., 2022). Situational awareness is one of the re-checking phases of information. The head of intelligence will analyze referring the current urgent situation. If the information that has been decided is not urgent or possibly inaccurate, the information processing will be refined through a similar process.

Source: authors.

ligence to result in the information (Zyoud, Fuchs-Hanusch, 2017). Intelligence experts use behavioral decision theory to improve intelligence and counter-intelligence decision-making. Orthodox and behavioral decision theory also presents decision as a prioritization effort inside a demarcated problem space where the probability of sum to one (Alemany et al., 2023; Misuri et al., 2019; Phillips, 2022). Based on the presented results, the information services are highly related to decision-making, situational awareness, information sharing, risk assessment, and artificial intelligence. It gives an overview of the information processing in the cyber security field that there are several cycle steps of filtering information by using artificial intelligence to decide the final information (Table 4).

Cyber security with risk management and assessment

To this end, the relation of cyber security and risk management and assessment field are closely related since it is relevant to considering critical infrastructure and policy decisions. In planning an infrastructure for cyber security, the head of intelligence examines the risk assessment and management to build economic dynamics, intelligence applications, or education. Risk assessment methods are widely used to analyze the prediction of future dynamics situations, especially in cyber-attacks or threats such as in cyber-physical systems, cyber safety, human resource, and economic activities (Kure et al., 2018; Michalec et al., 2022; Mitrofanova et al., 2017b; Rosado et al., 2022).

One of the examples of the relationship between cyber security in this risk assessment and management is in economics. Cyberspace indicators are a big part of the indicators used to measure a country's progress and GDP. The economics of cyber-security analyzes cyber-security challenges, such as PACS (Privacy and Cyber Security) adoption. Most evaluations focus on cost-benefit trade-offs encountered by rational market participants, strategic behavior, and market outcomes regarding participant welfare. Cyber-security risk assessment encompasses firms, customers, government, and adversaries. It also analyzes market mechanisms, market failures, and the economic impact of regulation on cyber-security. Security risks drive cyber-security economics (Jentzsch, 2018).

Risk management strategy could also defend the national threats which consist of conflicts that include multiple nation-states, political protesters, insider trading, espionage that is supported by a state. (McEvoy, Kowalski, 2019)

In analyzing and defeating the cyber security risks, various risk management tools are applied[4]. These methods can be a further recommendation for further research related to cyber security and management in empirical research.

Conclusion

Cyber security is a crucial issue that must be addressed by all enterprises, regardless of size, industry, or location, according to the conclusion of the cyber security and its strategic management topic. In order to defend their assets, data, and reputation from the increasing frequency and sophistication of cyber attacks, organizations must adopt a comprehensive and proactive approach to cyber security. Successful cyber security necessitates a comprehensive and unified strategy that incorporates people, procedures, and technology.

Our article analyzes the trends in the evolution of research on cybersecurity and its relationship to key aspects of strategic corporate management, including investments in infrastructure and human capital. It is shown that a key aspect of cybersecurity remains dealing with people as the most vulnerable link in the

[4] For example, CRAMM (CCTA Risk Analysis and Management Method), OCTAVE Allegro methodology, Infosec Standard 1, FAIR (Factor Analysis of Information Risk), MEHARI (MEthod for Harmonized Analysis of RIsk), STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of privilege), SABSA (Risk), Attack Path Analysis, and IRAM (Information Risk Assessment Methodology).

chain. Key areas of action include both training cybersecurity professionals with a wide range of universal competencies and informing ordinary users about potential cyber threats.

Cybersecurity is an ongoing process that requires regular monitoring, examination, and improvement. Companies must undertake regular risk assessments, identify vulnerabilities, and establish measures to limit cyber attack threats. This needs collaboration between several departments and parties, including IT, legal, human resources, and upper management. In conclusion, cyber security is a strategic concern that necessitates the focus and resources of companies at all levels. By taking a proactive and comprehensive strategy to cyber security, firms may reduce the likelihood of cyber attacks and safeguard their precious assets and reputation.

The limitation of this study is aimed for a specific review that the authors only use cyber security in a global context. Then, we only limitated the language into English since we want to give an overview of the previous research with a general understandable language. However, we recommend that the future studies make an expanded and larger context of research related to cyber security and strategic management so that the research will be more comprehensive and related to the current situation.

The authors declare no competing interests. The data of this research could be accessed through the Scopus database. For the approval, it does not need any approval as long as we have authorized access to the database. No informed consent needed in this research since this is a literature review research.

References

Aghajani G., Ghadimi N. (2018) Multi-Objective Energy Management in a Micro-Grid. *Energy Reports,* 4, 218–225. https://doi.org/1010.1016/j.egyr.2017.10.002

Alahmari A., Duncan B. (2020) *Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence*. Paper presented at the 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, Cyber SA 2020, 15-19 June 2020, Dublin, Ireland). https://doi.org/10.1109/CyberSA49311.2020.9139638

AlDaajeh S., Saleous H., Alrabaee S., Barka E., Breitinger F., Choo K.K.R. (2022) The Role of National Cybersecurity Strategies on the Improvement of Cybersecurity Education. *Computers and Security,* 119, 102754. https://doi.org/10.1016/j.cose.2022.102754

Alsharif M., Mishra S., AlShehri M. (2021) Impact of Human Vulnerabilities on Cybersecurity. *Computer Systems Science and Engineering,* 40(3), 1153–66. https://doi.org/10.32604/CSSE.2022.019938

Alsuliman F., Bhattacharyya S., Slhoub K., Nur N., Chambers C.N. (2022) Social Media vs. News Platforms: A Cross-Analysis for Fake News Detection Using Web Scraping and NLP. In: *PETRA'22: Proceedings of the 15th International Conference on PErvasive Technologies Related to Assistive Environments,* June 2022, pp. 190–196. https://doi.org/10.1145/3529190.3534755 190–96

Amir M., Givargis T. (2020) Pareto Optimal Design Space Exploration of Cyber-Physical Systems. *Internet of Things,*12, 100308. https://doi.org/10.1016/j.iot.2020.100308

Carayannis E.G., Grigoroudis E., Rehman S.S., Samarakoon N. (2021) Ambidextrous Cybersecurity: The Seven Pillars (7Ps) of Cyber Resilience. *IEEE Transactions on Engineering Management,* 68(1), 223–34. https://doi.org/10.1109/TEM.2019.2909909

Carr M. (2016) Public Private Partnerships in India. *International Affairs,* 92(1), 43–62.

Catota F.E., Granger M.M., Sicker D.C. (2019) Cybersecurity Education in a Developing Nation: The Ecuadorian Environment. *Journal of Cybersecurity,* 5(1), 1–19. https://doi.org/10.1093/cybsec/tyz001

De Soto B.G., Georgescu A., Mantha B., Turk Z., Maciel A., Sonkor S.M. (2022) Construction Cybersecurity and Critical Infrastructure Protection: New Horizons for Construction 4.0. *Journal of Information Technology in Construction,* 27, 571–594. https://doi.org/10.36680/j.itcon.2022.028

Dhawan S.M., Gupta B.M., Elango B. (2021) Global Cyber Security Research Output (1998–2019): A Scientometric Analysis. *Science and Technology Libraries,* 40(2), 172–189. https://doi.org/10.1080/0194262X.2020.1840487

Falagas M.E., Pitsouni E.I., Malietzis G.A., Pappas G. (2008) Comparison of PubMed, Scopus, Web of Science, and Google Scholar: Strengths and Weaknesses. *The FASEB Journal,* 22(2), 338–342. https://doi.org/10.1096/fj.07-9492lsf

Firoozjaei M.D., Mahmoudyar N., Baseri Y., Ghorbani A.A. (2022) An Evaluation Framework for Industrial Control System Cyber Incidents. *International Journal of Critical Infrastructure Protection,* 36(C), 100487. https://doi.org/10.1016/j.ijcip.2021.100487

Furnell S., Bishop M. (2020) Addressing Cyber Security Skills: The Spectrum, Not the Silo. *Computer Fraud and Security,* 2020(2), 6–11. https://doi.org/10.1016/S1361-3723(20)30017-8

Gratian M., Bandi S., Cukier M., Dykstra J., Ginther A. (2018) Correlating Human Traits and Cyber Security Behavior Intentions. *Computers and Security,* 73, 345–358. https://doi.org/10.1016/j.cose.2017.11.015

Härtel J.C.R., Härtel C.E.J. (2022) What the Digital Age Is and Means for Workers, Services, and Emotions Scholars and Practitioners. *Research on Emotion in Organizations,* 16, 9–17. https://doi.org/10.1108/S1746-979120200000016003

Hautamaki J., Kokkonen T. (2020) *Model for Cyber Security Information Sharing in Healthcare Sector.* Paper presented at the 2nd International Conference on Electrical, Communication and Computer Engineering, ICECCE 2020, June 12–13, Istanbul, Turkey. https://doi.org/10.1109/ICECCE49384.2020.9179175

Isa S.M., Nico G., Permana M. (2022) Indobert for Indonesian Fake News Detection. *ICIC Express Letters,* 16(3), 289–297. https://doi.org/10.24507/icicel.16.03.289

Jentzsch N. (2018) *State-of-the-Art of the Economics of Cyber-Security and Privacy* (IPACSO Deliverable D4.1). https://doi.org/10.2139/ssrn.2671291

Jiang L., Jayatilaka A., Nasim M., Grobler M., Zahedi M., Ali Babar M. (2022) Systematic Literature Review on Cyber Situational Awareness Visualizations. *IEEE Access,* 10, 57525–57554. https://doi.org/10.1109/access.2022.3178195

Katsikeas S., Johnson P., Ekstedt M., Lagerström R. (2021) Research Communities in Cyber Security: A Comprehensive Literature Review. *Computer Science Review,* 42, 100431. https://doi.org/10.1016/j.cosrev.2021.100431

Kharchenko V., Dotsenko S., Illiashenko O., Kamenskyi S. (2019) Integrated Cyber Safety Security Management System: Industry 4.0 Issue. In: *Conference Proceedings of 2019 10th International Conference on Dependable Systems, Services and Technologies, DESSERT 2019*, June 5–7, pp. 197–201. https://doi.org/10.1109/DESSERT.2019.8770010

Kopotun I., Nikitin A., Dombrovan N., Tulinov V., Kyslenko D. (2020) Expanding the Potential of the Preventive and Law Enforcement Function of the Security Police in Combating Cybercrime in Ukraine and the EU. *TEM Journal,* 9(2), 460–468. https://doi.org/10.18421/TEM92-06

Kure H.I., Islam S., Abdur Razzaque M. (2018) An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System. *Applied Sciences (Switzerland),* 8(6), 8060898. https://doi.org/10.3390/app8060898

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

Limba T., Plėta T., Agafonov K., Damkus M. (2017) Cyber security management model for critical infrastructure. *Entrepreneurship and Sustainability Issues*, 4(4), 559–573. http://dx.doi.org/10.9770/jesi.2017.4.4(12)

Mantha B.R.K., de Soto B.G. (2021) Assessment of the Cybersecurity Vulnerability of Construction Networks. *Engineering, Construction and Architectural Management,* 28(10), 3078–3105. https://doi.org/10.1108/ECAM-06-2020-0400

Marcantoni M., Jayawardhana B., Perez Chaher M., Bunte K. (2022) Secure Formation Control via Edge Computing Enabled by Fully Homomorphic Encryption and Mixed Uniform-Logarithmic Quantization. *IEEE Control Systems Letters*, 7, 395–400. https://doi.org/10.1109/LCSYS.2022.3188944

McEvoy R., Kowalski S. (2019) Cassandra's Calling Card: Socio-Technical Risk Analysis and Management in Cyber Security Systems. In: *CEUR Workshop Proceedings,* vol. 2398, pp. 65–80.

Michalec O., Milyaeva S., Rashid A. (2022) When the Future Meets the Past: Can Safety and Cyber Security Coexist in Modern Critical Infrastructures? *Big Data & Society,* 9(1), 205395172211083. https://doi.org/10.1177/20539517221108369

Mitrofanova A., Konovalova V., Mitrofanova E., Ashurbekov R., Trubitsyn T. (2017) *Human Resource Risk Management in Organization: Methodological Aspect*. Paper presented at the International Conference on Trends of Technologies and Innovations in Economic and Social Studies 2017. https://doi.org/10.2991/ttiess-17.2017.114

Mongeon P., Paul-Hus A. (2016) The Journal Coverage of Web of Science and Scopus: A Comparative Analysis. *Scientometrics,* 106(1), 213–228. https://doi.org/10.1007/s11192-015-1765-5

Morgan P.L., Collins E.I.M., Spiliotopoulos T., Greeno D.J,, Jones D.M. (2022) Reducing Risk to Security and Privacy in the Selection of Trigger-Action Rules: Implicit vs. Explicit Priming for Domestic Smart Devices. *International Journal of Human – Computer Studies,* 168, 102902. https://doi.org/10.1016/j.ijhcs.2022.102902

Mouti S., Kumar S., Althubiti S.A., Altaf M., Alenezi F., Arumugam M. (2022) Cyber Security Risk Management with Attack Detection Frameworks Using Multi Connect Variational Auto-Encoder with Probabilistic Bayesian Networks. *Computers and Electrical Engineering,* 103, 108308. https://doi.org/10.1016/j.compeleceng.2022.108308

Pollini A., Callari T.C., Tedeschi A., Ruscio D., Save L., Chiarugi F., Guerri D. (2022) Leveraging Human Factors in Cybersecurity: An Integrated Methodological Approach. *Cognition, Technology and Work,* 24(2), 371–390. https://doi.org/10.1007/s10111-021-00683-y

Qi A., Shao G., Zheng W. (2018) Assessing China's Cybersecurity Law. *Computer Law and Security Review,* 34(6),1342–1354. https://doi.org/10.1016/j.clsr.2018.08.007

Quincozes S.E., Mosse D., Passos D., Albuquerque C., Ochi L.S., Dos Santos V.F. (2022) On the Performance of GRASP-Based Feature Selection for CPS Intrusion Detection. *IEEE Transactions on Network and Service Management,* 19(1), 614–626. https://doi.org/10.1109/TNSM.2021.3088763

Rajan R., Rana N.P., Parameswar N., Dhir S., Sushil S., Dwivedi Y.K. (2021) Developing a Modified Total Interpretive Structural Model (M-TISM) for Organizational Strategic Cybersecurity Management. *Technological Forecasting and Social Change,* 170, 120872. https://doi.org/10.1016/j.techfore.2021.120872

Rosado D.G., Santos-Olmo A., Sánchez L.E., Serrano M.A., Blanco C., Mouratidis H., Fernández-Medina E. (2022) Managing Cybersecurity Risks of Cyber-Physical Systems: The MARISMA-CPS Pattern. *Computers in Industry,* 142, 103715. https://doi.org/10.1016/j.compind.2022.103715

Scanlan J., Thomas T., Tan T., Chen Y.P., Watters P.A., Fieldhouse M., Fung L., Girdler S. (2020) *Neurodiverse Knowledge, Skills and Ability Assessment for Cyber Security*. Paper presented at the Australasian Conference on Information Systems 2020, Wellington. https://www.researchgate.net/publication/350964865_Neurodiverse_Knowledge_Skills_and_Ability_Assessment_for_Cyber_Security, accessed 19.04.2023.

Sobb T., Turnbull B., Moustafa N. (2020) Supply Chain 4.0: A Survey of Cyber Security Challenges, Solutions and Future Directions. *Electronics (Switzerland),* 9(11), 9111864. https://doi.org/10.3390/electronics9111864

Watanabe K. (2019) PPP (Public-Private Partnership)-Based Cyber Resilience Enhancement Efforts for National Critical Infrastructures Protection in Japan. In: *Critical Information Infrastructures Security* (Proceedings of the 13th International Conference, CRITIS 2018, Kaunas, Lithuania, September 24-26, 2018), Heidelberg, Dordrecht, London, New York: Springer, pp. 169–178. https://doi.org/10.1007/978-3-030-05849-4_13

Zyoud H., Fuchs-Hanusch D. (2017) A bibliometric-based survey on AHP and TOPSIS techniques. *Expert Systems with Applications*, 78, 158–181. https://doi.org/10.1016/j.eswa.2017.02.016