Journal of Strategic Information Systems 33 (2024) 101861

Contents lists available at ScienceDirect

Journal of Strategic Information Systems

journal homepage: www.elsevier.com/locate/jsis

The whole of cyber defense: Syncing practice and theory

Kristel M. de Nobrega [a], Anne-F. Rutkowski [b], Carol Saunders [c,d,*]

[a] Central Bank of Aruba, J.E. Boulevard 8, Oranjestad, Aruba
[b] Tilburg University, Tilburg School of Economics and Management (TiSEM), Warandelaan 2, 5000 LE, Tilburg, The Netherlands
[c] University of Pretoria, Pretoria, South Africa
[d] University of Central Florida College of Business Administration, 4000 Central Florida Blvd, Orlando, FL 32816, United States

ARTICLE INFO

Keywords:
Cyber defense
Cyber Security
Cyber defense strategies
Cybernetic avenue
Military science
Cyber defense modes
Literature review

ABSTRACT

This review explores the problems Chief Information Security Officers (CISOs) and other cyber professionals face when defending their organization against cyberattacks. Using a Cyber Defense Grid, which was developed based on military science and cybersecurity concepts and terminology, we coded 125 articles published in Information Systems (IS) journals. We also employed three avenues (i.e., lenses) from cybernetic theory to frame the coding results to derive cyber defense strategies. In particular, we propose three strategic cyber defense modes: reactive, heuristic, and proactive. Taken together, these three modes suggest ways in which organizations can react strategically within the whole cyber defense domain.

Introduction

Attackers are regularly and exponentially outsmarting state-of-the-art cyber defenses of businesses, institutions, and governments. Smurf attacks, bot attacks, ransomware, and spear phishing are some terms used by cybersecurity professionals to refer to attacks in cyberspace. Cyberattacks are ill-natured attempts to control a particular computing infrastructure and thereby destroy the integrity of data or steal controlled information.[1] Among all businesses, 32 % (including 69 % of large businesses) reported experiencing cyberattacks in 2023, at an average cost of USD 4.5 million per attack (Protection Group International, 2023). The results of the 2023 Global Risks Perception Survey (GRPS) found that the risk of cyberattacks on critical infrastructures is among the top five risks with the greatest potential impact on a global scale. Also notable is that "widespread cybercrime and cyber insecurity" is a new entrant in the World Economic Forum's top ten risks (2023 Global Risks Report[2]). Malicious activities and cyberattacks are leveraging digital dependencies to become ever more aggressive, persistent, and sophisticated. This leveraging is occurring because cyberattackers are taking advantage of the more widespread exposure of potential targets due to greater internet usage by individuals and organizations, as well as the increasing numbers of networked devices (Sen et al., 2022). Extended networked connectivity enabled the emergence of an especially destructive type of cyberattack called an Advanced Persistent Threat (APT). An example is the SolarWinds supply chain

* Corresponding author.
E-mail addresses: k.denobrega@cbaruba.org (K.M. de Nobrega), a.rutkowski@tilburguniversity.edu (A.-F. Rutkowski), csaunder@ucf.edu (C. Saunders).

[1] The NCSD cybersecurity Glossary defines a cyberattack as "an attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity," extending the definition to "the intentional act of attempting to bypass one or more security services or controls of an information system." Attacks are deemed active (i.e., attempts to alter a system, its resources, its data, or its operations) or passive (i.e., attempts to learn or make use of information from a system, without alteration).

[2] https://www.weforum.org/reports/global-risks-report-2023/.

https://doi.org/10.1016/j.jsis.2024.101861
Received 31 January 2023; Received in revised form 22 August 2024; Accepted 13 September 2024
Available online 25 September 2024

attack that occurred in 2020. Malicious code was inserted into SolarWinds' Orion software, infiltrating tens of thousands of networked government and commercial organizations around the globe and generating major ripple effects worldwide (Wolff et al., 2021).

Cybersecurity professionals are fighting a multi-dimensional cyberwar. As Madnick (2017) states, "The good guys are getting better, but the bad guys are getting badder faster" (p. 4). Cyberattacks have "badder" repercussions not only for organizations, but also for national security and the security of the nation's citizens. The danger of escalating international conflicts in cyberspace by targeting whole nations has become a terrifying reality; in response, NATO has announced that a serious cyberattack on any of its members would trigger collective defense under Article 5 (Tertrais, 2016). Active cyberattacks led by nation-states have been occurring back and forth throughout the unfolding war between Ukraine and Russia (Jakub, 2022; Paganini, 2022), as well as prior to the Russian invasion (Fingas, 2022). In the context of this war, the United States President publicly warned the private sector: "If you have not already done so, I urge our private sector partners to harden your cyber defenses immediately."[3].

The focus of our systematic literature review is on cyber defense as it relates to the struggles encountered, not only by nation-state leaders but also by Chief Information Security Officers (CISOs) and other cybersecurity professionals, when facing cyberattacks. We are particularly focused on all cybersecurity practitioners who, like CISOs, are involved in developing and implementing cyber defense strategies to fight this multi-dimensional war and to deal with the aftermath related to cyberattacks across sectors and industries.

The multi-dimensional cyber defense domain is rooted in the fields of Cyber Security and military science. In academic literature, "Cyber Security," "Computer Security," "IT Security," "Information Security", and "Information Systems Security" are often used interchangeably (Schatz et al., 2017). This can be rather confusing. Schatz et al. (2017) note that the term "cyber security" gained considerable popularity when U.S. President Barack Obama in 2009 proclaimed, "I call upon the people of the United States to recognize the importance of cyber security and to observe this month with appropriate activities, events, and trainings to enhance our national security and resilience" (in Schatz et al., 2017, p. 54). Authors such as Stubley (2013) equate cybersecurity with information security because the "cyber" component involves the use of Information Technology and computers. Other authors, such as Walls et al. (2013), emphasize the ambiguity introduced by the mindless use of the term "Cyber Security" in situations where nuanced definitions such as Information Security (IS) or Information Technology (IT) Security are more appropriate. Dewar (2017) prefers to use "Cyber Security" instead of "Information Security" to denote a superset of security practices. Hence, in the context of our cyber defense research, we use the term "Cyber Security" and distinguish it from "Information Security" and other related terms noted above.

We define "Information Systems Security" (ISS) as "the protection of information handling at the technical, formal or informal levels" (Dhillon et al., 2021, p. 2). ISS typically involves defensive actions taken to protect against damages to the organization's IT assets. The way that firms operationalize their ISS priorities[4] can be seen in their spending patterns: 72 % is spent on identification, protection, and detection, while only 18 % is spent on response, recovery, and business continuity (Coden et al., 2023).

Like ISS, cybersecurity is concerned with defensive actions taken to identify and detect potential cyberattacks, to protect against those attacks where possible, and to respond to and recover from them when they occur. Cyber defense, more so than ISS, is particularly devoted to responding and recovering by taking actions to ensure that tools, policies, and organizational processes are in place to withstand cyberattacks. Cyber defense response can be rapid or timely. Furthermore, cyber defense is more broadly defined than ISS since it forms a shield that not only combines more traditional defensive actions, but also offensive actions involving or relying upon IT and/or operational technology and systems (Walls et al., 2013).Defensive approaches use preventive actions premised on understanding the system and its potential weak points, while "offensive approaches are counterpoint to defensive methods, and proactively predict and remove threats in the system using ethical hacking techniques" (Aiyanyo et al., 2020, p. 2). An example of an offensive tool is DeepLocker for Intelligent Target Profiling/Intelligent Collection. Thus, cyber defense actions, which are rooted in cybersecurity, are consistent with wartime situations that involve defensive and offensive strategies.

In this article, we use military terminology when we define cyber defense as "capabilities and processes to synchronize in real-time the ability to detect, analyze and mitigate threats and vulnerabilities, and outmaneuver adversaries to defend designated networks, [and] protect critical missions" (Cyber warfare Lexicon 2011, p. 7). We also adopt a multi-level perspective on cyber defense capabilities derived from military science[5]: *strategic* cyber capabilities concern high-level coordination and comprehensive infrastructures; *operational* cyber capabilities refer to achieving major objectives; *tactical* cyber capabilities point to specific, smaller objectives (Schulze, 2020). These cyber defense strategies at the operational and tactical levels include specific actions involved with risk mitigation, contingency planning, legal protection, and offensive/competitive positioning (e.g., innovating to maintain a competitive edge). Collectively, these defensive strategies (along with offensive strategies) form a cyber defense shield. The effectiveness of the cybersecurity controls and precautionary measures depends on the combined strengths of all elements of a cyber defense shield.

While some reviews of the ISS literature exist (e.g., Baskerville, 1993; Dhillon and Backhouse, 2001; Dhillon et al., 2021; Siponen, 2005), we know of no reviews of cyber defense in the IS literature. Recently, Dhillon et al. (2021) conducted a review of ISS research. As part of their research, they performed a Delphi study with CISOs which found that their concerns are focused on ISS attack issues. Notably, the CISOs ranked different types of attacks as the top four most important ISS issues: APTs, malware, hacking, and phishing attacks. CISOs are most concerned about the preponderance of data breaches. The CISOs ranked Security Policy Misalignment last out of seventeen concerns. Dhillon et al. (2021) also reported that academic ISS research has focused instead on ISS Behaviors and Privacy Concerns, as well as Security Compliance and Management. Thus, they concluded that "current academic research and practitioner

[3] https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/statement-by-president-biden-on-our-nations-cybersecurity/.

[4] Based on the National Institute of Standards and Technology's (NIST) Cybersecurity Framework.

[5] Note that business administration and information management commonly refer to strategic-tactical-operational. We adhere to the military conceptualization of strategic-operational-tactical.

concerns are out of sync" (Dhillon et al., 2021, p. 13). Researchers' and practitioners' perceptions about the value of the others' contributions have also been found to be out of sync (Hyatt et al., 1997).

Consequently, our review of cyber defense topics within the IS literature is designed to see the extent to which IS researchers are considering cyber defense concepts that are of the most concern to cybersecurity professionals who are busy planning for, dealing with, and recovering from cyberattacks. In particular, our research question is the following: *How can cyber defense concepts be used for developing strategies to help CISOs and other cybersecurity professionals who are engaged in cyber warfare?* Answering this research question can identify highly relevant topics for ISS researchers, as well as respond to the call for "more high-quality review papers that synthesize available knowledge for professional practice" (Templier and Paré, 2015, p. 114). Later, based on the knowledge garnered from our review, we explain how cyber defense is an important strategic tool that cybersecurity practitioners can use in their organizational war chests.

Theory

We begin by presenting a framework that we call the Cyber Defense Grid which reflects frequently mentioned terminology borrowed from practitioners in the fields of cybersecurity and military science. The Cyber Defense Grid consists of beneficial cybersecurity concepts that are missing or not fully addressed in the IS literature. Then, we introduce Kline's three cybernetics theoretical lenses (i.e., minimal self-organizing system, simulating human cognition, and Artificial Intelligence (AI)). These three cybernetic lenses, or avenues, help us in examining cyber defense relationships within the IS literature. We use the avenues to theorize about cyber defense strategies that academics can bring to practice in the cyber defense domain.

Cyber Defense Grid based on Cyber Security and Military Science

The Cyber Defense Grid consists of classes of attacks, targets of attacks, vulnerability, payloads, attackers, defenders, taxonomies/frameworks, and countermeasures.

An **attack class** categorizes a cyberattack (i.e., vectors) according to attack method (i.e., multiple, sequential, or parallel) and path. Raiyn (2014) identifies four main classes of attacks. One is Denial-of-Service (DoS), which overloads a computing or memory resource, consequently rendering the resource unable to handle legitimate requests such as user access to a machine (e.g., smurf attack); a popular form of DoS attack is the Distributed Denial-of-Service (DDoS). A second attack class is Remote to Local (User) (R2L), which sends packets to a local host over the internet or network, to subsequently illegally gain access through current machine vulnerabilities (e.g., SQL injection). A third attack class is User to Root (U2R), an attack designed to access a normal user account in the system to gain root access to the system (Alharbi et al., 2018). A fourth attack class is probing attacks, which are a form of "recon" activity (e.g., SATAn) in which a network is scanned to gather information (e.g., mapping IP address space of a target). Interestingly, a fifth type of highly potent attack that emerged from our coding is Advanced Persistent Threats (APTs). An APT is "not a single step attack but it is composed of numerous hacking tools and processes [… requiring a] high level of knowledge and plenty of resources, making APT an even more prominent threat […] The APT tracks its target constantly over a long period of time" (Siddiqi and Ghani, 2016, p. 46). APTs adapt to be resilient against new security measures (ibid.).

The **target** of an attack can be a computer, network logical entity, physical entity, Network Control System (NCS), Cyber-Physical System (CPS), or Industrial Control System (ICS). Modern NCSs (i.e., connecting the cyberspace and the physical space to allow remote task execution) and CPSs (i.e., composed of feedback loops where physical processes affect computations and vice versa) are being used successfully in industry (Kim et al., 2020). NCSs and CPSs, which serve ICSs such as Supervisory Control and Data Acquisition (SCADA), offer increased reliability and decreased wiring (Zhang et al., 2016).

Vulnerability (i.e., attack surface) is defined as "a system susceptibility or flaw in the design of the hardware or software and can be exploited to gain unauthorized access" (Duffany, 2018, p. 5).

The **payload** of the attack is the part of the malicious software (i.e., malware) that actually damages the target's system. It includes information leakage (data theft), spying (activities monitoring), destruction (corrupting or deleting files), propagation (worms), blackmail (ransomware), and the inability to service others (Hansman, 2003). Notably, multi-stage APT attacks may involve different payloads tailored for specific classes of attacks. APTs also have hidden entry points (backdoors) into the infected system which allow attackers to return remotely to execute their payload at will (Ahmad et al., 2019). In short, the malware is the delivery mechanism, and the payload is the malicious content which it is designed to deliver.

Attackers include insiders, hackers, terrorists, and nation-state-sponsored attackers. Edward Snowden, Bradley Manning, and Robert Hanssen are notable examples of insiders who posed a serious threat to their organizations/nation by revealing or exposing sensitive information (Kim et al., 2020). Insiders can cause great harm to their organizations, either unintentionally or through deliberate activities such as those enacted by disgruntled employees and/or espionage. In their review, Oliver and Randolph (2022) define a hacker as "as a user who wishes to gain access to an identified target (e.g., a company, group, or network) in hopes of learning more about the target, exploiting the target for attack or benefitting society" (p. 402). Attackers are commonly referred to as "black-hat" and "gray-hat," depending upon their degree of criminal intent (Maurushat, 2019; Silic and Lowry, 2021). Interestingly, black-hat hackers performing APT attacks are generally sponsored by a nation-state or corporate entity (Ahmad et al., 2019; Wen et al., 2017).

Cybersecurity professionals are critical **defenders**. The cybersecurity professionals encompass CISOs who operate mostly at the strategic level and a multitude of others whose roles protect and defend against cyberattacks at the operational and tactical levels. These include ISS analysts, cybersecurity engineers, security architects, IT security consultants, security software developers, penetration testers (e.g., white-hat hackers), and network security architects (Okeke, 2022).

Cyberattack **taxonomies and frameworks** are common in cyber defense and have been used to improve security policy and defend organizational systems. The goal of cyber defense taxonomies and frameworks is to enable researchers and practitioners to gain a comprehensive understanding of attacks against specific targets and adapted defense modes. An example of a research-based taxonomy is Fleury et al.'s (2008) classification of cyberattacks against control systems to assist the energy sector in managing cyber threats. The rise of technological innovations – including but not limited to Machine Learning (ML), natural language processing, and Artificial Intelligence (AI) – support the emergence of new defense frameworks such as the cognitive cybersecurity model (Khan and Parkinson, 2018). Frameworks often are drawn from the field of military science and are widely used by practitioners (Zhang and Thing, 2021). Two common frameworks derived from the military are the Cyber Kill Chain and the MITRE ATT&CK. See Appendix A for a more detailed description of these two intelligence-driven frameworks and their components and mechanisms [e.g., Tactics, Techniques, and Procedures (TTP) and Cyber Threat Intelligence (CTI)].

Countermeasures are rooted in the physical, temporal, logical, and cryptographic principles of separation in computer security (Pfleeger and Pfleeger, 2012). Globally, cybersecurity professionals focus on the protection of the organization through applications of three types of controls (Ahmad et al., 2014). One, technical controls (e.g., firewall, VPN's, IDS, Distributed IDS) are deployed to ensure the basic security standard. Two, formal controls are defined as techniques, processes, and tools for continuous risk management, identification, analysis, governance of risk, and compliance strategies (Dhillon, 2007); these controls are typically based on international standards and frameworks (e.g., COBIT 2019, NIST, ISO/IEC27001) emanating from legal acts (e.g., Sarbanes-Oxley Act, HIPAA). Three, informal controls are defined as behavioral controls, including protection motivation, fear appeals, and sanctions/rewards (Dhillon, 2007).

Klines' Cybernetics Avenues

When studying cyberspace, scholars and practitioners commonly use the abbreviation "Cyber." Semantically, "Cyber" is the contraction of "Cyber(netic) space." However, we too often omit a seemingly detail trivial, i.e., "netic." This detail is necessary to take into account when investigating theoretical approaches and, therefore, potential defense strategies for practitioners. Wiener (1948) defines "cybernetic" as "the scientific study of control and communication in the animal and the machine" (p. 11). Wiener's (1948) theorization focuses on the self-regulating mechanisms of cybernetic systems. He formalizes the notion of feedback mechanism (i.e., loop or circuit) as the source of intelligent behaviors.

Kline (2011) identifies three chief avenues in Wiener's grand theory of cybernetics. The three avenues relate to specific imported theories from cross-reference fields, namely law, organizational behavioral science, computer sciences (i.e., ML, AI), and cognitive sciences (i.e., information processing, decision-making, optimization, heuristics, simulation, gaming). We use these avenues to frame our analysis of the IS literature on cyber defense.

The first avenue of cybernetics originated from the work of Ashby (1957) on the homeostat, one of the first devices capable of self-adaptation in response to modifications in the environment. Ashby's principle of a *minimal self-organizing system* is that a dynamic system, independent of its type or composition, always tends to evolve toward a state of equilibrium or balance (i.e., homeostasis). Ashby (1957) assumed that adaptation to novelty results from system upper-level randomization that can reorganize the lower level.

The second avenue in cybernetics arises from the work of Newell and Simon (1972) on *simulating human thoughts*. Newell et al., (1957) designed and implemented processing languages that incorporate basic human information processes supported by computer programs, such as the Logic Theorist used to solve difficult problems (Newell et al., 1957). Cognitivists reverse-engineered the mind and developed new computational and associative models. As a result, thought processes were no longer considered to be an inaccessible black box.

The third avenue of cybernetics, namely *Artificial Intelligence* (AI), was initiated in 1959 in MIT's Artificial Intelligence Laboratory by McCarthy and Minsky (See Kline, 2011). The aim was to duplicate the cognitive and reasoning abilities of humans when using super powerful computers or robots boasting anthropomorphic cognitive capabilities (Rutkowski and Saunders, 2019). Advances in Graphics Processing Units (GPUs) have made training deeper neural networks possible and partially explain the craze for ML in combination with big data in the field of AI.

Methods

In this section, we describe the research method we used to perform the scoping review (Paré et al., 2015) and the systematic literature review (Jahan et al., 2016; Paré et al., 2015; Rowe, 2014; Templier and Paré, 2015), which resulted in selecting 125 articles from a pool of 544 articles across ten IS journals, using three iterations. As described below, the review method we employed is composed of three stages: (1) planning, (2) conducting, and (3) reporting and disseminating (Clarke and Oxman, 2001).

Stage 1: Planning the Review

The research question and our stated purpose (e.g., synthesizing the literature to share knowledge with and to assist both cybersecurity professionals and IS researchers) guided us in planning our review. We first decided the review period should be for the years 2003–2020; we then extended the period to 2023, based on a reviewer's comment. We started the review in 2003 for two reasons. One, 2003 was the publication year of a seminal conceptual article by Knapp et al. (2003) that used the defense mechanisms of biological cells as a metaphor for network security defense. Two, 2003 was the year in which the SQL slammer worm led to significant cyberattacks on various sectors and industries. Notably, SQL slammer infected the Davis-Besse nuclear power plant's network,

disabling the Safety Parameter Display System. About a decade later, a groundbreaking sophisticated cyber weapon (Stuxnet) compromised the fast-spinning centrifuges of Iran's Natanz nuclear facility, demonstrating cyberattacks' potential to damage and/or disrupt critical infrastructure (Knapp and Langill, 2015). Such a series of cyberattacks led US decision makers to conduct a Cyber Policy Review of formal cyber defense controls: norms, laws, agreements, policy decisions, and others (e.g., Harknett and Stever, 2011).

Stage 2: Conducting the Review

To understand the extent and nature of the research articles on cyber defense, we first conducted a scoping review, which is defined as "attempts to provide an initial indication of the potential size and nature of the available literature on a particular topic," before undertaking a full systematic review (Paré et al., 2015, p. 186). Early in our scoping review we decided to exclude databases such as ABI/Inform, JSTOR and Web of Science since our preliminary search surfaced an extremely large number of non-IS papers that were of limited value for understanding the contributions of IS researchers. To make our review scope and size manageable and to address the quality of the articles in our final sample, we focused our search on articles published in the AIS Senior Scholars Basket of Journals ("Basket of Eight"). We also looked at other prominent IS journals such as Decision Support Systems, Information & Organization, Communications of the AIS (CAIS), and Information & Management (IM) which we thought would be most likely to support our theorizing. To theorize, we needed to study articles that had a theoretical base and/or some depth in conceptual development. Hence, we used the recognition of journal quality and reputation by the AIS Senior Scholars as a proxy for the article quality assessment that is essential when conducting systematic reviews (Rowe, 2014; Templier and Paré, 2015). In the end, we supplemented our Basket journals sample with two other IS journals: CAIS and IM.[6]

Step 1: Cyber Defense Grid

We illustrate the steps in our systematic review of the literature in Fig. 1. According to Fink (2010, p. 3 as quoted in Rowe, 2014, p. 246), "A research literature review is a systematic, explicit and reproducible method for identifying, evaluation and synthesizing the existing body of completed and recorded work produced by researchers, scholars and practitioners." This method requires stating the overarching purpose of the review (e.g., research questions), documenting the search strategy, choosing search terms related to the review purpose and research question, developing and stating inclusion and exclusion criteria, explicitly stating article selection decision rules, and using an explicit framework for capturing data from the articles (Paré et al., 2015; Rowe, 2014; Templier and Paré, 2015). We conducted the initial review using the keywords "cyber defense" and "cyber defence." Our first group of articles totaled 104: i.e., EJIS (n = 12), ISJ (n = 7), ISR (n = 10), JAIS (n = 7), JIT (n = 9), JMIS (n = 1), JSIS (n = 5), CAIS (n = 41), IM (n = 12). We excluded a total of 25 manuscripts, such as commentaries, opinion papers panel reports, tutorials, teaching cases, case studies, editorials, review reports, tributes, introductions to special issues, and research agendas.

After independently reading the abstracts (n = 79), the original two coauthors first computed the numbers of keywords in each article (excluding references) that were highly associated with our research question: cyber defense, threat(s), security(ies), hacker(s), breach(es), vulnerability(ies), attack(s), payload, and counter(−)measure(s). While the term "cyber defense" appears in all 104 articles, only 43 % of the publications yielded these common cybersecurity keywords. The two coauthors then independently preselected the articles to be coded. The coauthors used a double coding approach to reduce selection bias (Hayes and Krippendorff, 2007). The results of the double coding showed convergence for 93 % of the pre-selected manuscripts. To resolve divergence between coders, we used a quantitative screening approach to reject the manuscripts that contain less than 100 occurrences of the search key words. For example, the article by Banks (2009) – which related to internet diffusion and had a total count of 42 occurrences of keywords cyber defense (n = 0), threat(s) (n = 11), security(ies) (n = 5), hacker(s) (n = 9), breach(es) (n = 0), vulnerability(ies) (n = 0), attack(s) (n = 17), and counter-measure(s) (n = 0) – was rejected on the basis of the decision rule specified above. Following the pre-selection phase, 34 articles were excluded. These articles neither relate to cyber defense nor offer extensive discussion of cybersecurity search keywords.

Following the pre-selection, the first two coauthors coded 45 publications based on the Cyber Defense Grid categories [attack class, target, payload, vulnerability, attackers, cyber professionals (i.e., defenders), and countermeasures], which are described above in the Theory section. (The coding table for the Cyber Defense Grid categories may be found in Appendix B.) We also coded taxonomies or frameworks that were used in the articles. Our coding of the 45 articles made it apparent that the IS field has addressed "defense" minimally, so we expanded the search through a second iteration by launching another literature review encompassing all aspects of "cybernetics" in IS.

Step 2: Cybernetics

The second group, which was added to include cybernetics articles, totaled 294 new articles. Following the protocol described in Step 1, 83 manuscripts were excluded, such as commentaries, opinion papers, panel reports, teaching cases, (guest) editorials, review reports, workshops, and research agendas. After reading 211 abstracts, we tabulated the number of keywords in each article (excluding references). Following this preselection process, we coded 41 publications. Again, our double coding showed convergence for 98 % of the pre-selected manuscripts, and we used the quantitative approach described above to reduce selection bias. The journal sources of the articles are displayed in Fig. 2 and Appendix C.

[6] After reading articles in the four IS journals, we considered the DSS articles to be too technical and thought there would be too few relevant articles in I&O.

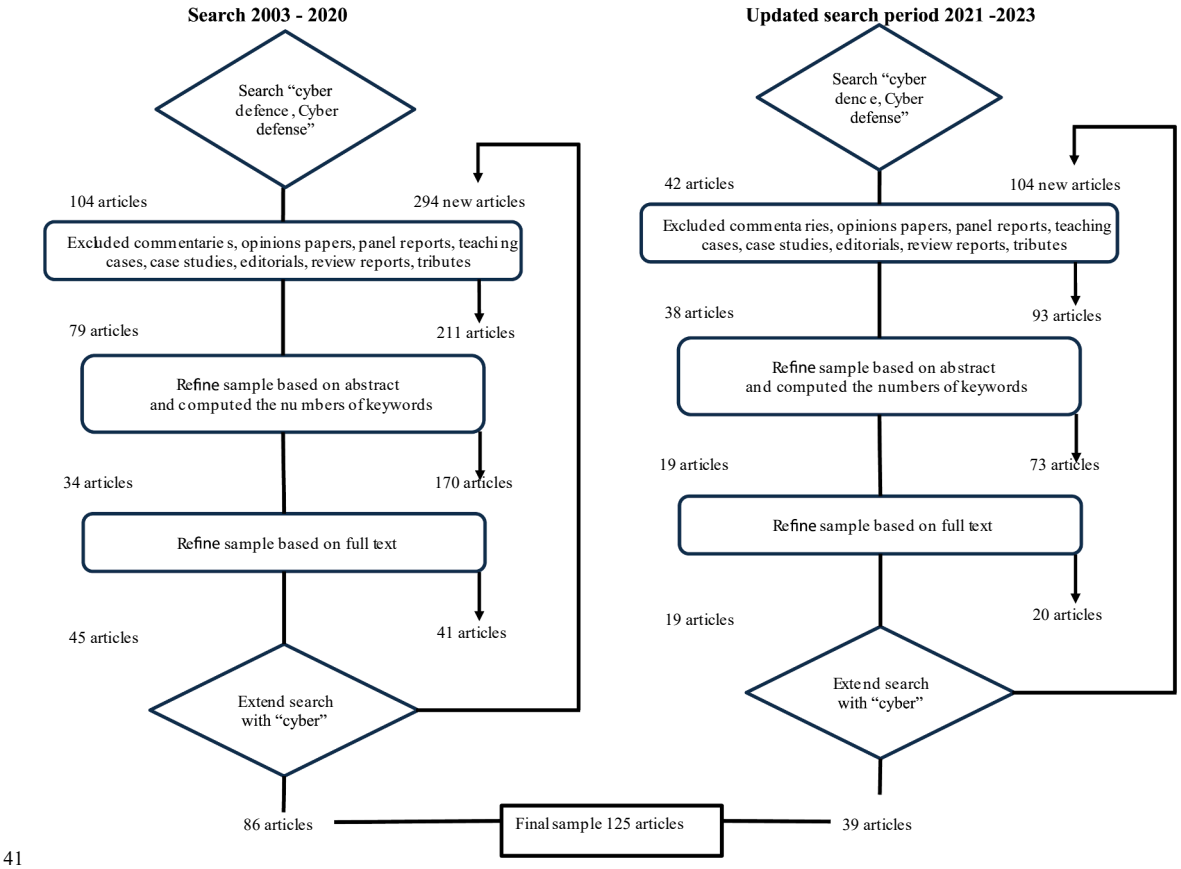


Fig. 1. Steps in the systematic review of the literature.

We coded the second group of 41 articles using the Cyber Defense Grid codes. We also coded the original 45 articles and the second group of 41 articles using the three chief avenues in cybernetics (Kline, 2011): *minimal self-organizing system*, *simulating human cognition*, and *AI*. See Appendix D.

Step 3: Updating the sample

To make our review more complete, we added articles from 2021 to 2023. Using the same protocol described in Steps 1 and 2 above, we found 146 potential articles and selected 39 of them for coding. Appendix C displays the number of articles published each year and the share of articles published in each of the ten IS journals that we selected. The third coauthor used the coding tables in Appendices B and D to demonstrate the reproducibility of the coding. There was 90 % percent agreement between the third author and the first and second co-authors in the coding of a subset of ten of the more recent articles. Most discrepancies occurred in class of attacks, as classification requires specific practitioner knowledge.

Stage 3: Reporting and Disseminating

The third stage reports the results of coding and subsequently synthesizing the findings for IS researchers and CISOs, as well as other cybersecurity professionals. The frameworks used for coding were the Cyber Defense Grid and Kline's Cybernetic Avenues.

Results and Synthesis of Coding

Cyber Defense Grid

In Appendix E, we report the results of the coding related to the Cyber Defense Grid. In this section, we provide some highlights of the synthesis of the coding results. In Appendix F, we provide a more detailed description and synthesis of the coding results.

Attack classes

Our coding revealed four attack classes (DoS/DDoS, R2L, U2R, and APT). The attack class is not easily identifiable in most of the ISS

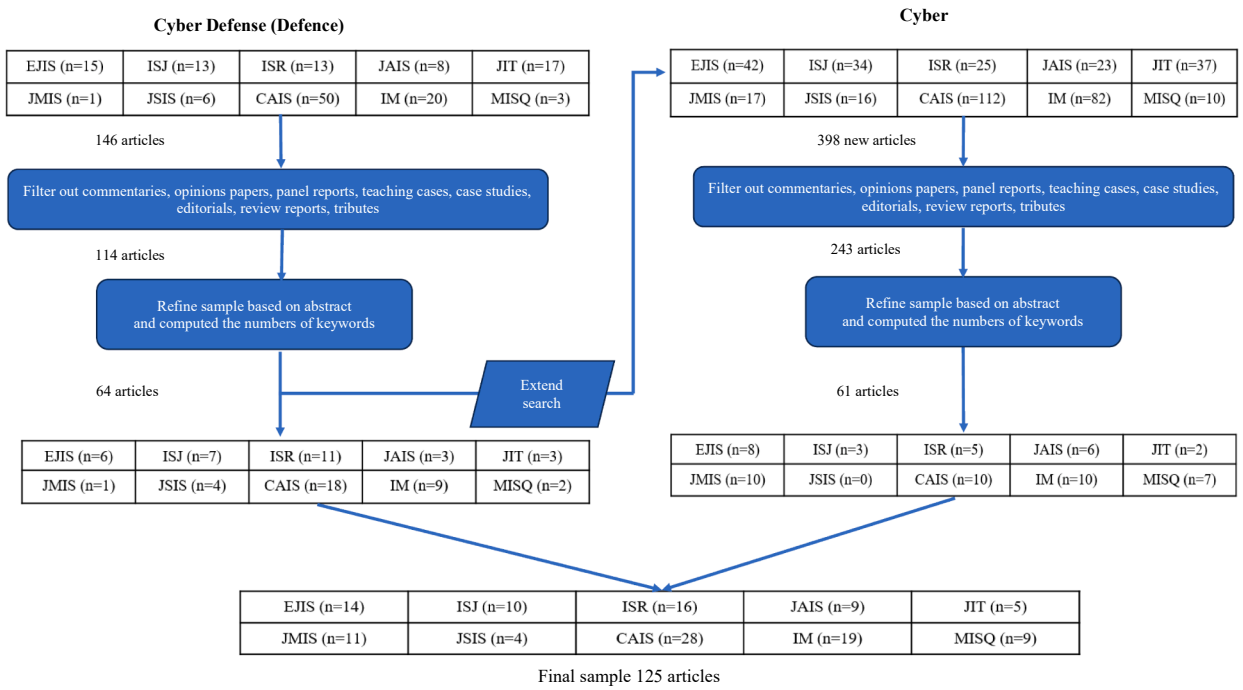


Fig. 2. Detailed description of sample selection from the ten prominent IS journals.

articles we coded. Most articles list many types of attacks in the introduction without further elaboration. R2L is the most frequently specified attack class, even though practitioners appear to be heavily involved in reacting to DoS and DDoS attacks. One article that does focus on DDoS attacks is the research by Hui et al. (2017) on the adoption of international legislation and the effects of DDoS. Almost all articles on targets of cyberattacks are about attacks on computer systems. Despite their importance in terms of the major potential impacts, only a few articles deal with attacks on critical infrastructures. An exception is one by Plachkinova and Vo (2023), who view cyberattacks on critical infrastructures as very likely. Infrastructures are easy targets because they were built decades ago before modern cybersecurity standards even existed and because cyberattacks on these infrastructures can cripple so many businesses, governments, and individuals. Most published attacks are on firms in the financial sector, followed by attacks on retail firms (See Appendix G). Hua et al. (2018) discuss a cyber terrorist attack on financial services and demonstrate the attack's ripple effects on society at large. Sen et al.'s article (2022) is a particularly rich text that not only gives specific examples of and details about all types of attack classes and targets, but also describes challenges and opportunities related to the use of machine language and AI.

Especially noteworthy is that only three papers address APTs (Shin et al., 2018; Kotsias et al., 2023; Plachkinova and Vo, 2023). Kotsias et al. (2023) note that APTs are increasingly sophisticated and aggressive. They are concerned that most organizations are so focused on complying with laws, regulations, and "best practice" cybersecurity standards that they can only react to attacks. Kotsias and colleagues note that organizations find themselves in an asymmetrical arms race against cyber threat actors who are free to act more aggressively and quickly. They urge organizations to adopt a military mindset that employs logic-driven CTI to proactively anticipate which vulnerabilities will be attacked. This mindset typically requires a change in culture about cyber defense and a behavioral transformation of the business users to directly mitigate vulnerabilities across all organizational levels (operational, tactical, and strategic) (ibid.).

Payloads

The payloads of the reported attacks are almost always related to breaches or data theft, which have been of great concern to cybersecurity practitioners since an early publication in 2003 (Bagchi and Udo, 2003). A focus on payloads highlights the real-world effects (e.g., financial loss, reputational damage, data exposure) of cyberattacks. Starting from 2017 (Hui et al., 2017; Samtani et al., 2017), twelve articles introduce an emerging payload of concern: ransomware. Nowadays, attackers not only encrypt the stolen data and scramble the files, but they also blackmail the victim by threatening to publish or sell the data if a ransom is not paid to obtain the decryption key (double extortion tactic).

Offenders and defenders

A number of articles deal with cyberwarfare combatants: offenders and defenders. Offenders can include insiders, hackers, and nation-state actors. Wang et al. (2022), among others, note that a majority of cyberattacks can be attributed to the intentional and unintentional actions of insiders. Most studies about hackers seek to identify the intentions. Wang et al.'s (2023) study of the Chinese Computer Misuse Act found that the law had a strong effect on the intentions of not only offenders (i.e., black-hat hackers), but also,

unfortunately, defenders (white-hat hackers and cybersecurity professionals). Most recently, Samtani et al. (2022) and Ebrahimi et al. (2022) used both deep learning and cybersecurity analytics to analyze the conversations of black-hat hackers on hacker forums on the international dark web to identify the exploit-vulnerabilities which hackers would be most likely to attack, as well as to build a novel cross-lingual hacker asset detection tool, respectively. Beebe and Rao (2010) present an interesting offender taxonomy (e.g., offender motivation, skill, offender-victim relationship, offender involvement). Another set of articles relate terrorism and espionage to APTs.

Defenders include CISOs and a variety of cybersecurity professionals. Ebrahimi et al. (2022) do a particularly good job describing how their research could assist defenders (i.e., cybersecurity professionals) at multiple levels. At the operational level, their research may assist security management, information security officers (ISOs), and practitioners in cybersecurity analytics organizations. At the strategic level, it may assist ISS Managers (ISSMs) and CISOs.

Taxonomies

Earlier ISS articles provided a relatively limited amount of theorizing about cyber defense using taxonomies from military science. One article by Wolff (2016) offers a taxonomy of perverse effects based on military concepts such as defense-in-depth, a strategy which involves layering defensive mechanisms to protect against multiple types of attacks. Kotsias et al. (2023) encourage adopting and integrating CTI usage as a key enabler for tracking and breaking the attacker's kill chain. Dincelli and Chengalur-Smith (2020) also draw from the military- related work on the cyber kill chain, namely the first phase of reconnaissance, to address design of SETA.

Countermeasures

The ISS literature does a good job of researching countermeasures. Approximately half of the reviewed articles deal with controls, especially formal controls, while informal controls are represented the least.

Kline's Cybernetic Avenues

This section introduces the coding results of Kline's (2011) cybernetics theoretical avenues or lenses: (1) minimal self-organizing system, (2) simulating human cognition, and (3) artificial intelligence (See Appendix H).

First avenue

Most IS articles we coded fall into the first avenue (n = 91). Many could offer contributions to practice. For example, Knapp et al. (2003) propose a framework for network security thinking that draws five analogies between cellular defenses and network defenses. This framework aims to activate critical thinking among groups of cyber professionals. Several publications employ what could be described as a threat response or prevention approach of employees to maintain organizational balance (Boss et al., 2009; Dinev and Hu, 2007; Johnston et al., 2016). Measures have been proposed for the perceptions of situational and dispositional factors (see Johnston et al., 2016) relating to sanctions, fear appeals, or self-efficacy. Other studies converge on the importance of using negative (Orazi et al., 2019) or positive reinforcement (Vedadi and Warkentin, 2020) to actively leverage randomization effects at the organizational level (i.e., upper level) and influence the lower levels involved with managing employees. Also, Wang et al. (2017) use the Extended Parallel Process Model (EPPM) to explore threat appraisals, coping strategies, and "mandatoriness." Chen et al. (2021a) extend the EPPM in their nuanced study of compliance and noncompliance.

Notably, we found from our review that deterrence is considered a way by which one system level can get another level to perform a desired action (Herath and Rao, 2009). For example, Shin et al. (2018) develop a framework of ten Internet Peace Principles based on legal deterrence. They believe that the paradigm of preventive cybersecurity can be established and that the motivations behind cyberattacks can be drastically ameliorated. Salisbury et al. (2011) explore the power asymmetries created by technology and investigate the impact of institutional changes on nation-states in resisting cyberattacks. Green et al. (2020) stress that cybersecurity policies and practices are fragmented across all partners in the critical infrastructure supply chain. However, stakeholders must share a common understanding of critical infrastructure interdependencies to determine the cascading damage that may result from attacks. Kotsias et al. (2023) provide an excellent example of the value of considering levels for CTI. In Kotsias' action-research study of an international finance corporation, the operational level of the corporation's threat intelligence team monitored the threat landscape for intelligence to feed to the Security Operation Center (SOC) (e.g., blocked IPs); the tactical level predicted threats and validated those threats with the more skilled SOC analysts; finally, the strategic level used the information to identify new threat actors and their TTPs, as well as to identify the firm's most exposed vulnerabilities.

Second avenue

We identified 24 articles employing a predominately second avenue lens. IS research extensively uses simulation models based on game theory and mathematical models to uncover complex heuristics related to decision-making and uncertainty (Benaroch, 2018). Roumani and Nwankpa (2020) apply game theory to analyze historical vulnerability data using the Cox proportional hazard model (i.e., they identify hackers' strategic choices when deciding which vulnerability to exploit). The same approach has been applied in studying accidental breaches in healthcare (Kim and Kwon, 2019) and the "survival" of active cybercriminals on the dark web (Benjamin et al., 2016). Sen et al. (2022) suggest that game theory could be used to model the interaction between AI-enabled controls and adversarial AI (i.e., when AI models are manipulated into making incorrect inferences) that is trying to find weaknesses in these controls so that Artificial Intelligence can attack those weaknesses. Another game theory example is by Gal-Or and Ghose (2005) who model information sharing benefits and the impact that collaborations of government agencies with universities and/or industry (e.g., Computer Emergency Response Team, InfraGard) have on reducing breaches. An example of mathematical modeling using

combinatorial optimization is provided by Temizkan et al. (2017), who propose a novel software diversity index based on Shannon's entropy to mitigate the rate at which the virus spreads. Mathematical models are also applied to assess the impact of malicious hackers on the competitive software market (Sen et al., 2020) and to identify emerging hacker threats (Ebrahimi et al., 2022; Li and Chen, 2022).

Third avenue

The third avenue of cybernetics, namely AI, is under-represented in our review, with only ten studies. For example, Syed (2020) uses Python NLP framework and a ML model to generate the cyber threat intelligence ontology that serves as a knowledge base for alert information. Sharma et al. (2020) apply ML techniques to samples of different Android malware data sets to determine discriminating features such as permissions and intents. Li et al. (2016) use social media analytics and text mining to identify key online sellers and then profile them using topic modeling of advertisements to help prevent future financial crimes. Samtani et al. (2017) analyze hacker tooling for timely identification of cyber threats. Sen et al. (2022) survey applications of AI and ML in cybersecurity, observing three major challenges: obtaining quality data to train ML algorithms and evaluate their performance; retraining ML models in active industrial use such as those identifying and classifying malware; and dealing with adversarial machine learning.

Discussion

Recommendations for Future Research Related to the Cyber Defense Grid

Our systematic literature review learned that the MIS literature on cyber defense provides interesting insights for practice. In fact, some understudied ISS research areas could be especially useful to CISOs and cybersecurity practitioners. We identified nine potential contributions for practice suggested by theory in academic IS publications.

First, although DDoS attacks are the most commonly observed in practice as reported by DBIR (2024), only twelve reviewed articles studied this attack class. Studying these attacks may help to better assess system resilience and robustness when the network system capacity is overwhelmed. Future research might explore traffic pattern anomalies or mitigation strategies such as traffic limit or load balancing. More articles like that of Salisbury et al. (2011) would be beneficial.

Second, a critical infrastructure is unlikely to operate nowadays without any ICS. ICSs facilitate the interconnectedness of systems in the critical infrastructure sector. Given the escalating challenges from APTs, ISS scholars need to pay more attention to cyberattacks on critical infrastructures, hence ICSs. A good place to start would be to test the TRACI critical infrastructure risk assessment framework developed by Plachkinova and Vo (2023). Their theory-backed taxonomy for risk assessment of cyberattack on critical infrastructure (TRACI) considers attacker motivation, risk management, and assets. In addition to the more typical incentive of economic gain, they suggest attacker motivations can be socio-cultural, thrill-seeking, and political (as when cyberterrorists engage in APT attacks on another country's energy grid or voting machines).

Third, the ISS literature focuses predominantly on the financial sector. This focus is aligned with the actual threat landscape. All over the world, financial institutions face a significant increase in the amount of cyberattacks (IMF, 2021). The European Central Bank (ECB) recently warned that cyberattacks could trigger serious economic shocks (ECB, 2021). The greater focus on the financial sector may also be related to a greater transparency in data breaches than exists in other sectors. Indeed, the finance and insurance sector, the second-most-regulated, has approximately 128,000 regulated restrictions for soundness of financial institutions (e.g. SOX compliance, IFRS19, PCI-DSS). This greater focus may be explained by the sensitive nature of data in most cyber incidents and the challenges of collecting data during such events. Sectors where NCS and CPS have been successfully implemented, such as energy and transportation, would be good candidates for exploring ways to improve collaborations to mitigate cyberattacks.

Fourth and related to the third point, while it is important to gather the opinions of C-level managers about cyber defense (e.g., Wang et al., 2023), other participants should be surveyed. Information obtained from stakeholders in other sectors critical to digital ecosystems (e.g., airports) or organizational units (i.e., business units) could also be useful for more fully understanding effective cyber defense strategies.

Fifth, the few articles in the ISS literature published on vulnerabilities relate directly to vulnerability management, and most appear to be a reaction to specific attacks. Severe vulnerabilities received considerable media attention in 2017 (Citrix vulnerability). This extra attention might have spurred interest in research on vulnerabilities, given that two-thirds of the articles focused on vulnerabilities were published in 2020 or later. Moreover, there is a growing interest in ISS literature on CTI to ferret out vulnerabilities (Samtani et al., 2022; also, Ampel et al., 2024).

Sixth, defensive and offensive capabilities may be increased via better comprehending the multifaceted relationships between payloads and cyberattacks. For example, recognizing the payload allows SOC teams to identify the attackers' objectives and, hence, to respond quickly (defense). The teams can deploy IDS technical controls to block the threat, as well as collect, store, and analyze the attackers' signature to predict future attacks. Understanding attackers' payloads of choice helps with adopting an offensive stance to deploy detection and prevention tools.

Seventh, APT campaigns are woefully understudied even though they often target critical infrastructures and nation-states. Cyberattacks on nation-states can have frightening consequences. To defend against the APTs' ever-emerging, asymmetrical cyber threat landscape, Kotsias et al. (2023) urge commercial organizations to adopt military-originated principles of cyber defense.

Eighth, the literature on formal controls appears to be well represented in our sample, while the articles on informal controls are not as well represented as they could be. Formal controls may prove problematic: despite its intent to limit malicious hacking, legislation such as the Computer Misuse Act may actually impede cybersecurity professionals from successfully predicting harmful hacking

cyberattacks. The ISS literature proposes an interesting path to improve such formal controls. For example, "mandatoriness" could be understood at the granular level as a form of informal control: "if individuals believe that management watches, they will comply" (Boss et al., 2009, p. 151). Notably, Liang and colleagues (2023) make an intriguing observation, suggesting that the use of terminology such as "policy compliance", "precautions taking", and "policy violation" may uncover behavioral ISS research idiosyncrasies. Diesch et al. (2020) emphasize that "a higher security standard does not necessarily lead to a higher security level" (p. 2). In the field of forensic investigations, more certifications are being developed (Lim, 2008). These new certifications may heighten the feeling of security burnout experienced by cyber-professionals (Pham et al., 2019). Moving forward, ISS researchers could theorize about and explore how to use informal controls more effectively. The interdisciplinary IS field could contribute not only to the technical and analytical aspects of cyber defense research, but also to cognitive aspects such as underlying motivations for adhering to policies to make cyber defense more effective, or to self-imposed controls such as those related to fear appeals.

Ninth and finally, our review found a relatively limited amount of theorizing about cyber defense in the earlier ISS literature. However, a few articles have appeared more recently in the 2020 s, which could prove useful to cyber defense practitioners if they can be convinced to use these articles. In particular, ISS articles are surfacing which are based upon military science frameworks such as the Cyber Kill Chain (Dincelli and Chengalur-Smith, 2020; Kotsias et al., 2023). However, most ISS literature only touches upon intelligence-driven frameworks. In contrast, the cybersecurity literature has a plethora of taxonomies and frameworks that are used by cyber defense practitioners. Basing more ISS research on the practice-oriented intelligence-driven cyber defense frameworks may make the research findings extra relevant to practitioners in adopting a military mindset that is more conducive to dealing with sophisticated cyberattacks. Furthermore, frameworks or taxonomies for offenders such as those found in the cyber defense literature could assist practitioners.

Using the Cyber Defense Grid as an indicator of cybersecurity professionals' interests leads us to suggest several areas where IS researchers could focus their attention more fully to benefit cyber professionals. These areas of research are summarized in Table 1, along with some examples of possible research questions.

Kline's Three Cybernetic Avenues and Strategic Cyber Defense Modes

A closer examination of the reviewed papers through the lens of Kline's three cybernetic avenues leads us to propose a model of three major strategic modes: reactive, heuristic, and proactive. These modes, portrayed in Fig. 3, can be used by organizations

Table 1
Recommendations for Future Research.

No.	Nature of Future Research	Examples of Research Questions
1	More research on DDoS attacks	- How do cybercriminals identify vulnerabilities for their DDoS attacks? - What strategies can be employed to keep systems experiencing DDoS attacks resilient and robust?
2	More research on CPS and NCS attacks; ICS	- Which control systems are the most vulnerable to cyberattacks, and why? - How effective is the application of the TRACI framework for risk assessment (Plachkinova and Vo, 2023) in averting attacks to critical infrastructures?
3	Expand focus of research beyond financial sector	- How can collaboration be fostered across organizations/nations to mitigate cyberattacks on critical infrastructures? - How can information be shared among organizations in the energy and transportation sectors to mitigate cyberattacks and their ripple effects?
4	Include a broader range of study participants (and not just C-level executives or students)	- How do leaders of nation-states budget for and deal with the dangers of cyberattacks? - How can defenders with different professional backgrounds collaborate to develop more effective cyber defense shields?
5	More research on vulnerabilities	- How can Cyber Threat Intelligence systems be successfully deployed in production environments across the tactical and operational levels? - Why do hackers target specific vulnerabilities?
6	Distinguish between attacks and payloads	- What payloads are used the most frequently in APT attacks? - How can SETA training be revised to increase awareness of payloads and distinguish them from attack classes?
7	More research on APT attacks	- How can cybersecurity professionals effectively change over to a military mindset to deal more effectively with APT attacks? - How can devasting ripple effects of APT be mitigated through collaborative means?
8	More research on informal controls as countermeasures	- How can gaming and simulation training be designed and deployed to reduce cognitive biases of defenders and employees in the organization? - What motivates the various stakeholder groups to adopt new informal controls?
9	Strengthen theorization on cyber defense to include more taxonomies familiar to cyber defense practitioners and other theoretical models and conceptualizations	- How can the cyber kill chain be used in defending against ransomware attacks? - How can a multi-level understanding of cyber threats be increased across the different organizational levels (strategic, tactical, and operational)?

strategically within the broader view of cyber defense, or what we call "the whole of the cyber defense domain".

Most existing cyber defense literature reflects what we call the **reactive** mode, which emphasizes identifying, detecting, and protecting against cyberattacks. This mode does not include an offensive component. What it does include is good cybersecurity practices such as SETA training, passwords, monitoring, and setting up defensive digital perimeters, such as firewalls, to prevent cyberattacks. When organizations employ the reactive mode, they take decisive actions against cyberattackers. This is consistent with the first avenue, where organizations try to secure their boundaries and seek homeostasis after being attacked. The organizations seek to understand the type of attack, the target, and, to some extent, the payload. This avenue tends to explore the role of insiders and defenders most clearly. This tendency is entirely consistent with the idea of internally-focused body self-regulation. This avenue also tends to be the predominant one for the studies of formal and informal countermeasures, which are applied to seek homeostasis to get past the cyberattack so that organizational operations can get back to "normal" and be on the alert for future attacks that interfere with homeostasis. The reactive mode could be employed by the Top Management Team (TMT) using SEC guidelines to make disclosures about breaches (Haislip et al., 2021) or by cybersecurity practitioners in developing formal control checks (SETA training). The reactive mode could even enrich SETA training (Wang et al., 2017) or recruiting of cybersecurity practitioners (Okeke, 2022) by using personality measures developed and validated for the first avenue IS research.

The second strategic cyber defense mode, the **heuristic** mode, is consistent with the second avenue focus on simulating information processing and problem-solving related to cyber defense. In their groundbreaking article, Newell et al., (1957) accounted for the "behaviorist magic" that occurs inside the human mind preceding behavior. Newell and Simon (1972) continued to demonstrate the importance of heuristics in problem-solving and decision-making. Common strategies in the heuristic mode aim to consider hackers', insiders', and cyber professionals' perceptions when building and implementing cyber defenses and responding to cyberattacks. Defenders often focus on what is in the minds of the black-hat attackers (and their view of vulnerabilities). In so doing, these defense strategies may be useful in assessing the highest exploitable vulnerabilities and the rationale for hackers' strategic choices in terms of attacking vulnerabilities (Roumani and Nwankpa, 2020; Li and Chen, 2022). Defenders could also use mathematical modeling to mitigate the spread of viruses (Temizkan et al., 2017).

The third mode, or **proactive mode,** uses advanced technology such as AI and ML strategically to create better defenses against cyberattacks, as well as launch offensive attacks. AI is fast becoming the "next big thing" in cyber defense practice, as many intelligent tools are coming to market, each one promising to solve problems better and faster than traditional approaches. The strategic proactive cyber defense mode, as demonstrated by the articles in the third avenue, employs AI to improve cyber defenses in general, with a main focus on technical countermeasures. AI can identify potential vulnerabilities and types of attacks. As attackers become stealthier at evading common defenses, AI can detect anomalies signaling their cyberattacks. Though our review revealed only a few articles for classification in the third avenue, theoretical frameworks and taxonomies from articles in this avenue ultimately could be highly relevant for (proactive) cyber defense professionals. For example, taxonomies to model offender motivation either within the organization (e.g., Orazi et al., 2019) or from dark web (e.g., Samtani et al., 2017) could be particularly beneficial for cybersecurity professionals. Samtani et al.'s (2022) CTI tool (EVA-DSSM) and device vulnerability severity metric (DVSM) are designed to proactively identify exploits in online hacker communities.

Advanced ML, AI, and time series data processing can be used to develop offensive strategies. For example, researchers were able to predict adversarial movements and stay ahead of dynamic malicious actions, such as removing threats in the system by eliminating vulnerabilities that were identified prior to being attacked.

The proactive mode is well-suited for developing weapons in a quantum world, though admittedly, the arrival time of large-scale quantum computers is difficult to predict. Quantum Computing (QC) is a major catalyst for AI deployments (Gupta et al., 2017;

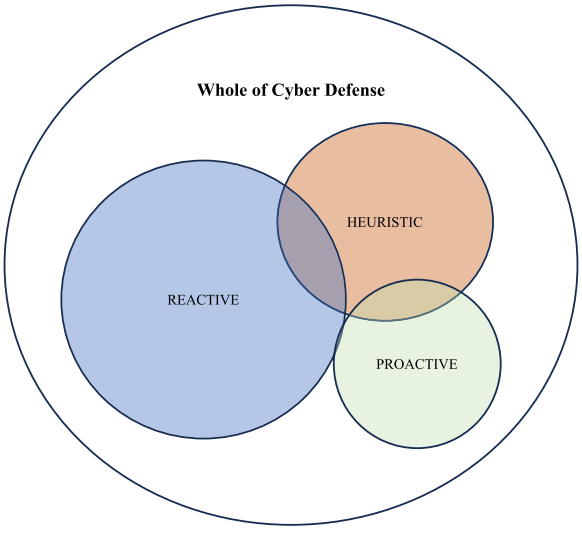


Fig. 3. Modes Within the Whole of Cyber Defense.

Linnhoff-Popien, 2020). It will enable cyber professionals to apply advanced AI technologies to uncover attack patterns and automate some cybersecurity processes (Khooshabeh and Gale, 2018). The recent implementation of quantum algorithms for ML show how QC could be efficient in solving problems in the field of AI, much faster than their classical counterparts (Biamonte et al., 2018; Dunjko and Briegel, 2018; Schuld et al., 2015; Schuld and Petruccione, 2018). New AI technologies will facilitate a data-driven approach, also referred to in the military field as intelligence-driven operations (Dorn, 2009, p. 806). Given technological asymmetry (Salisbury et al., 2011), the risk of being outmatched by an adversary in cyberspace operating at machine-speed will soon become a new challenge for cybersecurity professionals. That said, we assume that both cyberattackers and defenders using AI will gain increasingly high levels of autonomy to execute operations (Johnson, 2019). AI supports the development of interpersonal skills in cyber decision-making and teaming contexts.

Strategies for Cyber Defense

The three strategic modes complement and work in concert with one another in providing an effective defense within the whole of the cyber defense domain. Thus, these modes are shown as overlapping in Fig. 3. Similarly, the theoretical boundaries between the second and third modes are becoming more permeable with astounding technological advances such as AI or QC. Furthermore, there is space in the cyber defense domain circle which indicates that there might be other modes that should be included based on further research and exploration. In Table 2, we summarize key characteristics of the cyber defense modes.

What has not yet been established is how combinations of these three modes should be strategically balanced by organizations, suggesting promising directions for future research. Considerations for balancing and then implementing the strategic modes include the skill levels needed and the organizational sector.

Skill Levels Needed

To date, most IS research about cyber defense has been related to the reactive mode – a mode that has also received the most interest from cybersecurity practitioners. Most cybersecurity practitioners are fully occupied setting up defenses and responding to attacks. Reactive mode strategies can continue to be used by cybersecurity professionals in all types and sizes of organizations, and findings from ISS research can be applied to improve strategies. That said, cybersecurity professionals recognize that advanced technologies are posing ever greater threats. Beebe and Rao (2010) emphasize this point when they state that "technical fortification of information assets is part of an ongoing and possibly never-ending cycle, in which criminals and information security professionals continually try to outdo the others' technologies" (p. 330). Heuristic and proactive mode strategies need to become more commonplace if these future challenges are to be mastered. Yet many cybersecurity practitioners do not have the skills, time, or resources to effectively implement the strategies. These are more likely to be implemented in larger organizations and IT intensive organizations that can afford to attract and retain cybersecurity professionals with the requisite levels of skills. The smaller and mid-size organizations probably need to rely on third-party cybersecurity operations vendors (e.g., FireEye) for more advanced cybersecurity weapons employing AI and ML (Samtani et al., 2022).

Organizational sector

The heuristic and proactive mode strategies may also be implemented and be successful in utility companies and government institutions with critical infrastructures and large-scale, highly interdependent systems. In these organizations, there is a great need to deter APT and other attacks on ICS, CPS, and NCS targets, especially those instigated by well-funded governments and nation-states. The TRACI framework (Plachkinova and Vo, 2023) to analyze risk of cyberattacks on critical infrastructures is an example of a reactive mode strategy. ISS research mathematical modeling to uncover black-hat hackers' strategic choices regarding organizational vulnerabilities is an example of a heuristic mode strategy that promises great potential (Li and Chen, 2022), while using ethical hacking to predict and remove threats is a proactive mode strategy (Aiyanyo et al., 2020).

While QC can help the "good guys" in their cyber defense efforts, it also can help the "bad guys" in their cyberattacks. For example, key public infrastructures in current use, as well as the Internet of Things, will become insecure because of the availability of large-scale QC to cyberattackers (Cheng et al., 2017; ENISA, 2021). Cybersecurity practitioners are not the only type of cybersecurity professionals who are "good guys." IS researchers can be cybersecurity professionals in the war against cyberattackers. Amid this rapid development, IS researchers have the interdisciplinary perspective, capabilities, and training to be "good guys." That is, IS researchers can understand and implement available technologies, such as AI, to detect and respond to intensified cyber incidents. They have the expertise in IS design, development and maintenance to build computational IT artifacts that can support CTI activities. Their future research can focus on developing and perfecting AI technologies, which, when added to the current cyber defense arsenal, afford more proactive technical security control. IS researchers are also in a good position to deal with what Wolff (2016) refers to as perverse effects. AI regularly exceeds human abilities, in terms of both speed and accuracy. Nevertheless, AI still struggles when solving problems where additional context is needed to reach an answer, whereas that context would be common sense for a human.

Once the three strategic cyber defense modes have been balanced, CISOs and TMTs will need to know how to implement the cyber defense strategies. Considerations will include how to put various defensive and offensive models, practices, and methods into a production environment; how to sell the TMT (and maybe CISO) and insiders in the business units on complying and supporting the cyber defense strategies; and how to deal with needed changes in culture.

Implementing Cyber Defense Strategies

Once a cyber defense model or method has been developed by cybersecurity professionals or IS researchers, it needs to be put into a

Table 2
Strategic Modes of the Whole of Cyber Defense.

	Reactive	Heuristic	Proactive
Cyber Defense Focus	Identifying, detecting and protecting against cyberattacks; includes digital perimeter; does not include an offensive component	Information processing related to cyber defense; learning how hackers', insiders', and cyber professionals' perceptions impact building and implementing cyber defenses and responding to cyberattacks	Using advanced technology such as Artificial Intelligence and machine learning to offer better defenses against cyberattacks; may include an offensive component
Associated Avenue	First	Second	Third
Primary Theoretical Basis	Ashby's Minimal Self-Organizing System	Newell and Simon simulating the human mind; models for information processing and decision-making	Artificial Intelligence and machine learning
Key Concepts of Avenues	Homeostasis, adaptation to novelty, body self-regulation	Processing languages; human information processing; computational and associative models of the mind; game theory; scales and experiments to measure how people think and perceive	Duplicate the cognitive and reasoning abilities of humans

production environment. That means that operational and tactical cybersecurity professionals need to consider various organizational constraints and contexts before they can scale up the new models or methods. Furthermore, the cost of implementing the strategy needs to be justified. This justification is particularly challenging for models and methods in the proactive mode because of the difficulty in assessing the monetary value of damage that was averted. Kotsias et al. (2023) describe some ways of justifying the cost of offensive actions. Finally, moving from a traditional reactive mindset to a military mindset needed for the proactive mode requires a change in organizational culture. SETA training can be a start, but a transformation strategy is needed which involves the CISO and TMT. Below in Table 3 are some future research directions designed to enhance the success of implementing cybersecurity challenges.

Challenges and Limitations

Due to its interdisciplinary nature, coding articles was, in a word, challenging. For example, making sense of the articles' contributions required some knowledge of reference fields, such as organization and military sciences (Wolff, 2016), mathematics and computer sciences (Temizkan et al., 2017), and ISS. The leap among the definitions, constructs, and measures academics from various backgrounds have proposed in their articles is consequential, but interestingly the articles share similar premises. Relatedly, the main coder dyad (i.e., one academic and one practitioner) is needed to understand and reconcile the different assumptions and paradigms underlying the articles' coding of this complex topic. Appendices B and D are the result of their reconciliation efforts. Though challenging, future research could benefit from using academic-practitioner teams.

A limitation of our review is our failure to code for all relevant aspects of cybersecurity. For example, cyber resilience is a topic that recently has emerged as extremely important. Coden et al. (2023, p. 3) recommend that, to become cyber-resilient, management's thinking should "shift from the current approach of 80 % protection and 20 % resilience to one focusing more on resilience." By cyber resilience, we mean "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on cyber resources" (Bodeau et al., 2018, p. iii in Smith, 2023). We did not realize the value of coding for resilience until we started theorizing, and even if we had coded for resilience, we likely would not have found very many representative instances in our sample. Although we now recognize the importance of resilience and many other related topics, we focused on topics that were of the greatest interest to cyber practitioners when we initiated our study.

That said, resilience should be explored in future research on cyber defense. Perhaps resilience is another mode, as suggested by Dewar (2017), or perhaps it is a characteristic of the modes we are proposing. We found some possible theoretical links between our cyber defense modes and resilience. For example, the reactive mode relates closely to restorative resilience. *Restorative resilience* reflects the ability of an entity "to respond, and recover, by returning it to a normal state of functioning" (Prior and Herzog, 2013, p. 10). In the reactive mode, the attacked system aims to return to a pre-incident status quo, or "bounce back." Proactive mode strategies could be linked to adaptive resilience. *Adaptive resilience* "aims to ensure that the victim system can change its status quo to reflect the new situation following an intrusion. The system alters its parameters to take account of the effects of an attack and continues to function" (Dewar, 2017, p. 11). Thus, our theorization about modes may prove helpful to future researchers studying resilience.

Contributions

The cyber warfare landscape is changing drastically, quite literally every minute, as the weapons that the cybercriminals use become more sophisticated and dangerous, and as nation-states enter the fray as attackers. Traditional approaches to combating attacks are no longer adequate; more aggressive, deadly offensive actions need to be taken by defending organizations and governments. Perhaps the greatest contribution of our research is that we emphasize the need for a new mindset to battle in these ever-evolving cyber warfare landscapes, and that we then demonstrate how military science cyber defense concepts could address this need. Consistent with the stated research problem, our review demonstrates that cyber defense concepts derived from the cybersecurity and military science fields can be used within the IS field for developing strategies to help CISOs and other cybersecurity professionals in the war against cyberattackers. We identify nine potentially fruitful topic areas and related possible research questions for future research that we derived from the application of the Cyber Defense Grid to our coding of 125 IS cyber defense articles (See Table 1).

Furthermore, based on Kline's (2011) Cybernetic Avenues, we introduce three strategic cyber defense modes that can be used to support CISOs and cybersecurity professionals when defending organizations against cyberattacks. These modes can be used to help

Table 3
Future Research Directions related to Strategic Cyber Defense Modes.

Strategic Mode	Future Research Directions
Reactive	- Conducting more research on the following: DDoS attacks; ICS, CPS, and NCS attacks; vulnerabilities; informal controls (see Table 1 above) - Determining appropriate combinations to create a balance of this mode with other two modes in different contexts (i.e., ICS vs. CPS vs. NCS attacks; various sectors)
Heuristic	- More research using mathematical modeling and simulation on predicting and combating APT attacks - Determining the best approaches for managing changes to organizations when implementing models of information processing related to cyber defense
Proactive	- Evaluating the effectiveness of various proactive mode strategies - Designing new management and governance mechanisms that consider the unique maintenance requirements of AI-enabled cybersecurity controls

envision and devise strategies for cyber defense. We discuss considerations for their use in different contexts and suggest future research directions to further explore these and other considerations. We also offer the three strategic modes of the whole of the cyber defense domain as theoretical lenses to better or differently understand the problems faced by cyber professionals (Rai, 2016) and to start theorizing about an extremely important (and under-researched) strategic topic: cyber defense in the IS field.

Conclusion

Our systematic literature review has demonstrated that the field of military science has been barely touched upon in IS literature. However, the potential contribution of military science research to theorizing about cyber defense by IS researchers is considerable. Overall, we argue for a multi-disciplinary approach and greater collaboration with researchers in the field of military science to develop native IS theories related to cyber defense. Remaining ahead of the cyberattack is, in practice, a rat race. In the Chinese military treatise "The Art of War," Sun Tzu (5th century BCE) stated: "Engage people with what they expect; it is what they are able to discern and confirms their projections. It settles them into predictable patterns of response, occupying their minds while you wait for the extraordinary moment — that which they cannot anticipate" (United States Joint Force Command, 2008, p. 10). The "good guys" may lose the race because they may engage the "bad guys" in ways that they expect. The attackers expect cybersecurity professionals to engage in commercial partnership ventures to leverage AI. For example, Darktrace is collaborating with Microsoft to create new sophisticated technical controls to shield companies from threats (Kean, 2021). Still, there is hope: the "bad guys" may not expect the private and public sectors to combine their goals.

Finally, most cyber professionals recognize that the threats posed by cyberattacks are growing exponentially, in conjunction with the advanced technologies (i.e., AI, QC) developed to alleviate them. While using these technologies will be crucial to fend against cyberattacks, authors such as Lindsay (2020) argue that "Intelligence advantage in political competition depends on the interaction of technological infrastructure with organizational institutions (…). Scientific innovation in quantum technology only affects one of the dimensions" (p. 335).

CRediT authorship contribution statement

Kristel M. de Nobrega: Writing – review & editing, Writing – dissertation, original draft, Conceptualization. **Anne-F. Rutkowski:** Writing – review & editing, Writing – original draft, Conceptualization. **Carol Saunders:** Writing – review & editing, Writing – original draft, Conceptualization.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

We appreciate the help of Shan Pan, the Senior Editor, and the review team whose comments and insights helped to improve this paper. The paper is drawn in part from and extends the dissertation of the lead author: de Nobrega, K. (2023). *Cyber defensive capacity and capability: A perspective from the financial sector of a small state*. [Doctoral Thesis, Tilburg University]. CentER, Center for Economic Research.

Appendix A. Description of main Cybersecurity Frameworks

Frameworks used by practitioners, while developed or influenced by military practices, have been adapted and applied across various sectors, including government, critical infrastructure, and private industry, due to the universal nature of cybersecurity threats.

Framework and components	Description
Intelligence-driven cybersecurity framework	**Cyber kill chain**: Security Operation Centers and Incident Response Teams (SOC/CIRT) rely on the cyber kill chain as a mental process to develop preventive measures (Wen et al., 2017). The cyber kill chain has been adapted from the military concept which identifies the structure of an attack (Hutchins et al., 2011; Zhang and Thing, 2021). The seven different stages of a cyber kill chain follow a sequential, incremental and progressive process of reconnaissance (i.e., phishing email), weaponization (i.e., delivery payload; virus, worm and malware), delivery (i.e., insider threat, SQL, bot attack), exploitation (i.e., CVE; software vulnerability; network vulnerability), installation (i.e., actual payload setting up locally), command and control (i.e., trojan), and actions on objective (i.e. ransomware). Preventive measures can be taken at different steps of the kill chain to dam the cyber avalanche. The cyber kill chain has been criticized (Haga et al. 2020). For example, Greene (2016) underscores that multiple kill chains are necessary to mitigate complex waves of attacks (i.e., sequential vs. parallel

(*continued on next page*)

(*continued*)

Framework and components	Description
	information processing). **MITRE's ATT&CK**[1] is a framework (Hassan et al., 2020), while not directly military-derived, the MITRE ATT&CK Framework, provides a comprehensive matrix of techniques used by adversaries during cyberattacks. It is widely used in both military and civilian sectors for threat intelligence and defensive purposes.The ATT&CK framework contains the largest and most widely used collections of Tactics, Techniques and Procedures (TTP) (Shoorbajee 2018; Glick 2019). Currently, all ten of the top endpoint detection and response tools surveyed by Gartner (Gartner 2022) leverage the Mitre ATT&CK knowledge base for detection. It provides a standardized language for discussing and sharing information about adversary behaviors, enabling organizations to better defend against cyberattacks and improve their overall security posture. Additionally, MITRE maintains an ATT&CK Navigator, an interactive tool that allows users to visualize and explore the framework, facilitating threat modeling, gap analysis, and security assessment activities.
Cyber security framework components	**Tactics, Techniques and Procedures** (TTP) are integral components of the cybersecurity frameworks presented above. TTP provides a comprehensive understanding of the behavior and methods of cyber adversaries. TTP describes the behavior of a threat actor and the structured framework for executing a cyberattack (i.e., a signature). Understanding and documenting TTP is essential for cybersecurity professionals in identifying, analyzing, and mitigating cyber threats effectively. It allows defenders to detect and prevent future cyberattacks in evaluating the capabilities, doctrine, objectives, and limitations of the attacker (Bahrami et al. 2019). For example, in the context of the MITRE ATT&CK Framework a detailed matrix of TTPs used by adversaries across various stages of an attack life cycle is provided. **Cyber Threat Intelligence** (CTI) refers to the collection and analysis of information about threats and threat actors that provides actionable insights to improve an organization's security posture. CTI follows cycle of *Prevent-Detect-Respond* securing the environment by understanding threats before they materialize. Cyber Threat Intelligence (CTI) can be integrated into each phase of the *Plan-Do-Check-Act* cycle helping to improve the security posture of an organization.

[1]MITRE ATT&CK®.

Appendix B. Coding table for Cyber Defense Grid

(Anatomy of an attack)

Note: This appendix was modified from the initial coding table for the Cyber Defense Grid as a result of discussions ensuing from the coders trying to gain an understanding and agreement about coding differences.

Categories and definition	Sub-categories and definition	Main keywords and combinations
Attack class is an attack vector that classifies a large category of cyberattacks according to the attack method (Kim et al. 2020) An attack method may be composed of multiple, sequential, or parallel classes of attacks Four main attack classes have been identified in the information security literature (see Raiyn 2014; Alharbi et al. 2018)	*Denial of Service (DoS)* attacks entail overloading a computing or memory resource and consequently enabling it to handle legitimate requests such as user access to a machine. Typical DoS attacks include the smurf attack, ping of death, and the SYN flood attack. A particular form of DoS attack—the *distributed denial-of-service (DDoS)*—occurs when multiple machines are operating together to attack a target or public-facing service. The DDoS attack cripples the organization's ability to provide its service online. (Raiyn 2014)	Overload, service interruption, network congestion, resource depletion, flood attack, unavailability of services, distributed, amplification, targeted, brute force
	Remote to Local (R2L) is a class of attack, during which packets are sent to the machine of a local host (user's machine) over internet (or a network), and then it exploits the machine's vulnerability to illegally gain access (Paliwal and Gupta 2012). *User to Root (U2R)* access a normal user account on the system to gain root access. When a software vulnerability is exploited, it allows an unauthenticated attacker to execute arbitrary code execution (Raiyn, 2014)	Remote access, remote exploitation, unauthorized access, privilege escalation, local host/resources, password cracking, man-in-the-middle, session hijacking, SQL injection, cross-site scripting, phishing attacks, whaling attack, spear phishing Root access, kernel, lateral movement, shell escape
	Probing attacks is a form of "recon" activity in military jargon. A network is scanned to gather information or find known vulnerabilities of a target system (Alharbi et al. 2018)	Information gathering, reconnaissance, target identification, network scanning, port scanning, enumeration, OS fingerprinting,
Advanced Persistent Threats (APTs) campaign (Ahmad et al. 2019)		Back doors, Stuxnet, advanced tactics, persistent, targeted attacks, covert operations, nation-state actors, stealthy techniques, custom malware, zero-day exploits, long-term campaigns, supply chain of attacks, solar winds, sophisticated evasion method, cyber espionage, high-value targets, Command and Control (C2) infrastructure, cyber

(*continued on next page*)

(*continued*)

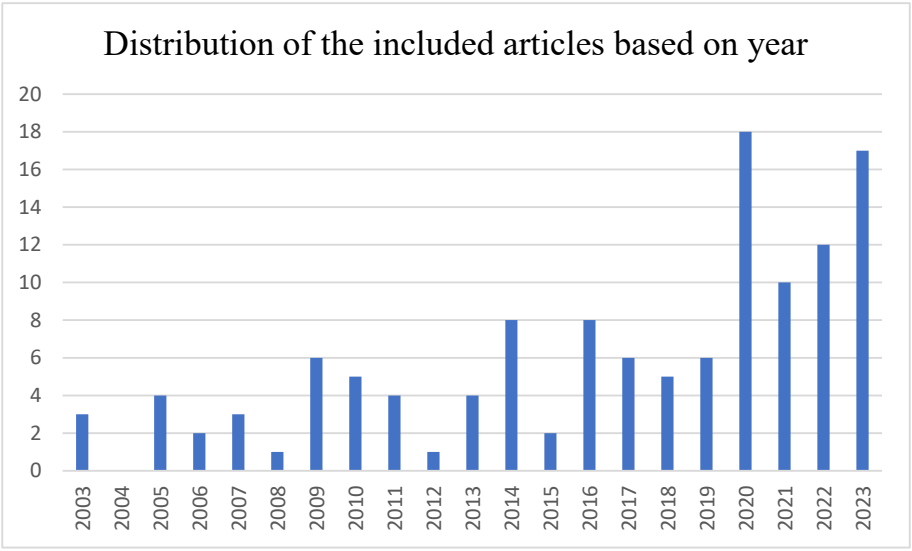
Categories and definition	Sub-categories and definition	Main keywords and combinations
		weaponization, APT signature, advanced social engineering
Target A physical entity, all core information systems and control systems supporting the private and the public sector	*Computer*	Computer, Personal devices, mobile devices, smart devices
	Network Control System (NCS) is connecting the cyber space and the physical space allowing remote tasks execution (Kim et al. 2020)	Control loops, network protocols, feedback mechanisms, packet loss, remote monitoring and control, wireless communication, security protocols (e.g., SSL/TLS, IPSec), authentication mechanisms, network segmentation, redundancy and failover, traffic analysis, network access control
	Cyber-Physical System (CPS) is composed of feedback loops where physical processes affect computations and vice versa (Lee 2008)	Embedded devices, real-time data processing, sensor networks, smart grids
	Industrial Control System (ICS) is a broad term used to describe several types of systems used in industries systems critical to the operation of critical infrastructures that are often highly interconnected and mutually dependent systems (Drias et al., 2015)	Distributed Control Systems (DCS), Supervisory Control and Data Acquisition (SCADA), Industrial Automation system (IAS), Industrial Automation and Control Systems (IACS), Programmable Logic Controller (PLC), Operational technology (OT), Process control, Industrial espionage, Stuxnet, Physical sabotage, flexibility
	Specified sectors	Sector private and public, critical infrastructure, technology users
Payload The component of the malicious attack which causes harm to the target (Hansman 2003)	Malware, exploits, payload delivery, trojan horses, ransomware, deleting or modifying files, viruses, remote access tools (RATs), persistence mechanisms, metasploit payloads, logic bombs, drive-by-download (droppers), data breach, data theft	
Vulnerability A system susceptibility or flaw in the design of the hardware or software and can be exploited to gain unauthorized access (Duffany 2018)	Vulnerability assessment, disclosure, scanning, management, remediation, exploitable weakness, security flaws, CVE (Common Vulnerabilities and Exposures), Zero-day, attack surface, security updates, security advisories Citrix	
Attackers	Insiders, crackers, cybercriminals, black hats, script kiddies, hacktivists, penetration testers, malicious actors, intruders, nation-state, organized crime, cyberterrorist	
Defenders	Cyber-professional, Information security expert, CISO, Security professionals, ethical hackers (White hats), red teaming, Cybersecurity analysts, incident responders, Security engineers, administrators, hunter, Security Operations Center (SOC), Blue teams, Digital forensics experts, Malware analysts, Network defenders, Security architects, Security trainers, Security managers, Security auditors	
Taxonomy/ framework "the systematic classification of things or concepts in which the components are grouped into a certain concept, and the classification categories have the purpose itself" (Kim et al. 2020, p. 996)	Intelligence-driven, TTP, Cyber Kill Chain, offender, Fleury's, AVOIDIT, Diamond model of analysis, MITRE ATT&CK, parallel Kill Chain attack method, path of attack, sequential single, cognitive cybersecurity model	
Countermeasures "the set of all countermeasures implemented by an organization can be viewed as an ISS countermeasure (ISSC) portfolio, with each component of the portfolio interacting with other components" (p. 242). ISMs focus mainly on protecting the organization from security threats through application of formal, informal, and technological controls (Ahmad et al. 2014)	*Technical* (Dhillon 2007, Ahmad et al. 2014)	Firewall, VPN's, SIEM, MISP, Intrusion Detection System (IDS), Distributed IDS, basic security standard of confidentiality, integrity and availability, Intrusion Prevention System (IPS), antivirus software, encryption, Secure Sockets Layer/Transport Layer Security (SSL/TLS), virtual Private Network (VPN), two-factor authentication (2FA), network segmentation, security Information and Event Management (SIEM), endpoint security, access control, secure coding practices, data loss prevention (DLP), security Operations Center (SOC), sandboxes, honeypot
	Formal controls are defined as techniques, processes, and tools for continuous risk management, identification, analysis, governance of risk, and compliance strategies. These security policies and procedures provide advice and outline punitive measures for noncompliance Formal controls mostly are built on international standards and frameworks and have legal grounding (Ahmad et al. 2019; Dhillon 2007)	Two-factor authentication (2FA) policy, endpoint security onboarding, access control, secure coding practices, data loss prevention (DLP) policy, disaster recovery, patch management, incident response policy / process, Common Vulnerabilities and Exposures (CVE), Common Weakness Enumeration (CWE), ISO/IEC 27001, Open Web Application Security Project (OWASP), cyber hygiene, ISACA, 1996; NIST, ISO2700, Sarbanes-Oxley, HIPAA, CLOUD act, IEC 62443 formally called ISA99 Industrial standards, IEC 62351, regulations, compliance, governance, risk management, change management, business continuity planning, disaster recovery plan, least

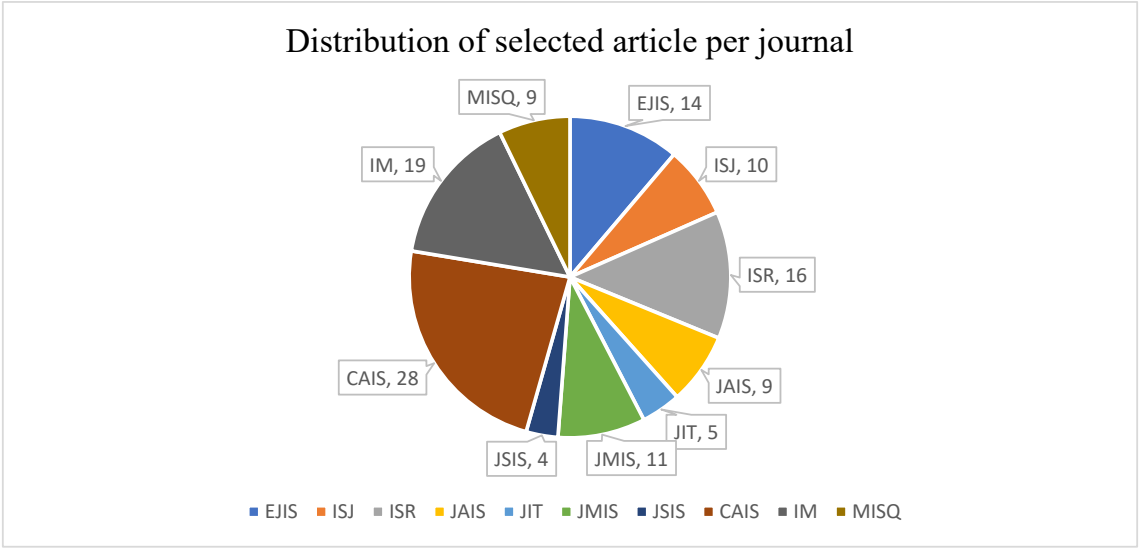
(*continued on next page*)

(*continued*)

Categories and definition	Sub-categories and definition	Main keywords and combinations
		privilege, audit trails, check list, IT governance
	Informal controls are subsequently promoted in organizations, such as behavioral control (Dhillon 2007)	Policies, procedures, Security awareness training, security culture, continuous monitoring, social engineering awareness, employee awareness, peer accountability, knowledge sharing, continuous learning, security mindset, proactive security measures, incident reporting culture, protection motivation, fear appeals, sanction/rewards, neutralization technics

Appendix C. Distribution of the included articles based on year and journal





Appendix D. Coding scheme for Kline's Cybernetic Avenues

Note: This appendix was modified from the initial coding table for Kline's Cybernetic Avenues as a result of discussions ensuing from the coders trying to gain an understanding and agreement about coding differences.

First avenue: Minimal self-organizing system

Imported theories from organizational and/or behavioral sciences, including Behavioral Information System Security (BISS) or/ and law. Key elements: maintaining balance (Homeostasis, equilibrium), self-regulating mechanisms, adaptation, self-organization, organizational layers, interdependence, collaboration, multiple stakeholders.

Second avenue: Simulating human thoughts

Imported theories from mathematics, econometrics, cognitive psychology. Key elements: Information processing (thought process), associative model, decision-making, optimization, heuristic, reduction of complexity, rule-based expert systems, simulation, causation, correlation, gaming.

Third avenue: Artificial intelligence

Imported theories from computer sciences. Key elements: duplicate reasoning, powerful computer, robots, neural network, Machine learning, algorithms, reinforcement learning, supervised learning process, learning and/or identification and/or recognition of patterns, Deep learning, no/little human supervision, data unstructured and unlabeled, Neural networks, Natural Language Processing (NLP), Robotic process automation, robots; Important to have advanced machine learning and AI.

Appendix E. Coding of the IS literature per Cyber Defense Grid

Defense Framework		
Attack class (unique n=36)	DoS/DDoS (n=12)	Bose and Leung (2007); Yayla and Hu (2011); Salisbury et al., (2011); Zhao et al., (2013); Hui et al., (2017); Samtani et al., (2017); Ebrahimi et al., (2020); Helm (2021); D'Arcy and Basoglu (2022); Samtani et al., (2022); Sen et al., (2022); Ebrahimi et al., (2023)
	R2L (n=24)	Bose and Leung (2007); Liang and Xue (2010); Yayla and Hu (2011); Hovav and Gray (2014); Goel (2015); Crossler and Posey (2017); Wang et al., (2017); Boyson et al., (2019); Green et al., (2020); Ivaturi et al., (2020); Naidoo (2020); Pienta et al., (2020); Roumani and Nwankpa (2020); Sen et al., (2020); Helm (2021); Nguyen et al., (2021); D'Arcy and Basoglu (2022); Li and Chen (2022); Samtani et al., (2022); Sen et al., (2022); Tripathi and Mukhopadhyay (2022); Ayaburi and Andoh-Baidoo (2023); Ebrahimi et al., (2023); Frauenstein et al., (2023)
	U2R (n=10)	Katos and Adams (2005); Bose and Leung (2007); Mookerjee et al., (2011); Wang et al., (2016); Jeager and Eckhardt (2020); Naidoo (2020); Wu et al., (2021); Samtani et al., (2022); Sen et al., (2022); Ebrahimi et al (2023)
	Probing (n=9)	Ransbotham and Mitra (2009); Salisbury et al., (2011); Mookerjee et al., (2011); Goel (2015); Shin et al., (2018); Dincelli and Chengalur-Smith (2020); Green et al., (2020); Kotsias et al., (2023); Plachkinova and Vo (2023)
Advanced Persistent Threats (APTs) (n=3)		Shin et al., (2018); Kotsias et al., (2023); Plachkinova and Vo (2023)
Target	Computer (n=17)	Bagchi and Udo (2003); Bose and Leung (2007); Lee and Larsen (2009); Liang and Xue (2009); Anderson et al., (2010); Liang and Xue (2010); Mookerjee et al., (2011); Yayla and Hu (2011); Zhao et al., (2013); Goel and Shawky (2014); Hovav and Gray (2014); Boyson et al., (2019); Roumani and Nwankpa (2020); Helm (2021); Chen et al (2021a); Sen et al., (2022); Samtani et al., (2022)
	NCS (n=2)	Salisbury et al., (2011); Sen et al., (2022)
	CPS(n=3)	Goel (2015); Green et al., (2020); Sen et al., (2022)
	ICS/ Critical Infrastructure (n=4)	Sen et al., (2022); Samtani et al., (2022); Plachkinova and Vo (2023); Kotsias et al., (2023)
Payload (unique n=38)	Data breach and theft (n=31)	Bagchi and Udo (2003); Boyson et al., (2019); Chen et al., (2021a); Cheng et al., (2022); Dinev and Hu (2007); Gal-Or and Ghose (2005); Goel and Shawky (2009); Yayla and Hu (2011); Wang et al., (2013); Goel and Shawky (2014); Hovav and Gray (2014); Liu et al., (2014); Nicho and Kamoun (2014); Goel (2015); Samtani et al. (2017); Shin et al., (2018); Jeong et al., (2019); Kim and Kwon (2019); D'Arcy et al. (2020); Ebrahimi et al.(2020); Ivaturi et al., (2020); Jeager and Eckhardt (2020); Haislip et al., (2021); D'Arcy and Basoglu (2022); Donalds and Barclay (2022); Li and Chen (2022); Sen et al., (2022); Tripathi and Mukhopadhyay (2022); Wang and Ngai (2022); Wang et al., (2023); Zhao et al., (2023)

(*continued on next page*)

(*continued*)

	Ransomware (n=12)	Hui et al., (2017); Samtani et al., (2017); Shin et al., (2018) Benjamin et al., (2019); Ebrahimi et al., (2020); Sharma et al. (2020); Ghahramani et al., (2022); Kam et al., (2022); Li and Chen (2022); Sen et al., (2022); Pigola and da Costa (2023); Plachkinova and Vo (2023)
Vulnerability (n=13)		Gal-Or and Ghose (2005); Arora et al., (2010); Beebe et al., (2014); Appan and Bačić (2016); Green et al., (2020); Roumani and Nwankpa (2020); Syed (2020); Wallace et al., (2020); Zhuang et al., (2020); Helm (2021); Li and Chen (2022); Samtani et al., (2022); Wang and Ngai (2022)
Attackers (unique n=35)	Insiders (n=13)	Alder et al., (2006); Herath and Rao (2009); Nicho and Kamoun (2014); Lowry et al., (2015); Johnston et al., (2016); Willison et al., (2018); Orazi et al., (2019); Shuetz et al., (2020); D'Arcy and Basoglu (2022); Tripathi and Mukhopadhyay (2022); Li and Chen (2022); Wang and Ngai, (2022); Burns et al., (2023)
	Black hat hackers (n=20)	Mookerjee et al., (2011); Yayla and Hu (2011); Zhao et al., (2013); Hovav and Gray (2014); Benjamin et al., (2016); Hui et al., (2017); Samtani et al., (2017); Benjamin et al., (2019); Ebrahimi et al., (2020); Naidoo, (2020); Roumani and Nwankpa (2020); Sen et al., (2022); Samtani et al., (2022); D'Arcy and Basoglu (2022); Tripathi and Mukhopadhyay (2022); Li and Chen (2022); Wang and Ngai (2022); Burns et al., (2023); Ebrahimi et al., (2023); Wang et al., (2023)
	Nation-state (n=8)	Salisbury et al., (2011); Hua and Bapna (2013); Goel (2015); Hua et al., (2018); Shin et al., (2018); Sen et al., (2022); Samtani et al., (2022); Kotsias et al., (2023)
Defenders (unique n=20)	Cyber professionals (n=17)	Ma and Pearson (2005); Lee and Larsen (2009); Ramachandran et al., (2013); Beebe et al., (2014); Nicho and Kamoun (2014); Lowry et al., (2015); Jalali et al., (2019); Green et al., (2020); Pienta et al., (2020); Shuetz et al., (2020); Wallace et al., (2020); Haislip et al., (2021); Li and Chen (2022); Samtani et al (2022); Sen et al., (2022); Hassandoust and Johnston (2023); Plachkinova and Vo (2023)
	White hat hacker (n=4)	Whitworth and Zaic (2003); Samtani et al. (2017); Li and Chen (2022), Wang et al., (2023)
Taxonomy/ framework Intelligence-driven and mechanism (unique n=24)	Cyber kill chain, MITRE Att&ck, TTP, CTI, PDCA, PDR (Appendix A) (n=16)	Salisbury et al., (2011); Li et al., (2016); Benjamin et al., (2016); Samtani et al., (2017); Benjamin et al., (2019); Jalali et al., (2019); Ebrahimi et al., (2020); Dincelli and Chengalur-Smith (2020); Syed (2020); Donalds and Barclay (2022); Samtani et al., (2022); Sen et al., (2022); Hassandoust and Johnston (2023); Kotsias et al., (2023); Pigola and Da Costa (2023); Plachkinova and Vo (2023)
	Offender (n=6)	Ransbotham and Mitra (2009); Beebe and Rao (2010); Mookerjee et al., (2011); Hui et al., (2017); Orazi et al., (2019); Ebrahimi et al., (2023)
	Defender (n=3)	Helm (2021); Plachkinova and Vo (2023); Zhao et al., (2023)
Countermeasures	Technical (n=36)	Bagchi and Udo (2003); Knapp et al., (2003); Whitworth and Zaic (2003); Cavusoglu et al., (2005); Katos and Adams (2005); Adler et al., (2006); Dinev and Hu (2007); Lee and Larsen (2009); Arora et al., (2010); Liang and Xue (2010); Mookerjee et al., (2011); Wang et al., (2013); Baskerville et al., (2014); Herath et al., (2014); Hovav and Gray (2014); Anderson et al., (2016); Wolff (2016); Belanger et al., (2017); Crossler and Posey (2017); Temizkan et al., (2017); Benaroch (2018); Hui et al., (2019); Ebrahimi et al., (2020); Roumani and Nwankpa (2020); Sharma et al., (2020); Syed (2020); Vedadi and Warkentin (2020); Helm (2021); Wu et al., (2021); Li and Chen (2022); Samtani et al., (2022); Sen et al., (2022); Wang and Ngai (2022); Bahreini et al., (2023); Kotsias et al., (2023); Pigola and Da Costa (2023)
	Formal (n=52)	Ma and Pearson (2005);Dhillon and Torkzadeh (2006); Dinev and Hu (2007); Goodman and Ramer (2007); Lim, (2008); Boss et al., (2009); Herath and Rao (2009); Liang and Xue (2009); Ransbotham and Mitra (2009); Liang and Xue (2010); Smith et al., (2010); Zhao et al., (2013); Baskerville et al. (2014); Beebe et al., (2014); Goel and Shawky (2014); Herath et al (2014); Nicho and Kamoun (2014); Posey et al., (2014); Yadav and Dong (2014); Goel (2015); Lowry et al., (2015); Appan and Bačić (2016); Johnston et al., (2016); Belanger et al., (2017); Wang et al., (2017); Benaroch (2018); Willison et al., (2018); Boyson et al. (2019); Carpenter et al., (2019); Hui et al. (2019); Jeager and Eckhardt (2020); Jensen et al., (2020); Pienta et al., (2020); Syed (2020); Yoo et al., (2020); Chen et al., (2021b); Goel et al., (2021); Haislip et al., (2021); Wu et al., (2021); Chen et al., (2022); Cheng, et al., (2022); Donalds and Barclay (2022); Ghahramani et al., (2022); Andersson et al., (2022); Sen et al., (2022); Tripathi and Mukhopadhyay (2022); Wang and Ngai (2022); Asatiani et al., (2023); Ayaburi and Andoh-Baidoo (2023); Burns et al., (2023); Kotsias et al., (2023); Zhao et al., (2023)
	Informal (n=32)	Adler et al., (2006); Dhillon and Torkzadeh (2006); Karjalainen and Siponen (2011); Ramachandran et al., (2013); Posey et al., (2014); Lowry et al., (2015); Anderson et al., (2016); Wang et al., (2016); Wang et al., (2017);Orazi et al., (2019); Shuetz et al., (2020); Smith, 2020 (2020); Vedadi and Warkentin (2020); Chen et al., (2021a); Chen et al., (2021b); Goel et al., (2021); Haislip et al., (2021); Kam et al., (2021); Chen et al., (2022); Ng et al., (2021); Nguyen et al., (2021); Nguyen et al., (2023); Dincelli and Chengalur- Donalds and Barclay (2022); Sen et al., (2022); Tripathi and Mukhopadhyay (2022); Wang and Ngai (2022); Ayaburi and Andoh-Baidoo (2023); Frauenstein et al,. (2023); Hassandoust and Johnston (2023); Raddatz et al., (2023); Tejay and Mohammed (2023); Xu et al. (2023)

Appendix F. Detailed description and synthesis of coding of IS Literature per Cyber Defense Grid

In this Appendix, we report the detailed results related to Cyber Defense Grid (See Appendix E).

Attack class, Target and Vulnerability

The attack class is not easily identifiable. Only a quarter of the articles specify the attack class. The most common type of attack reported was *R2L* (n=24), followed by *DoS/DDoS* (n=12), *U2R* (n=10) and *probing* (n=9). The most common target is computer systems (n= 17). Interestingly, four studies about ICS/critical infrastructures were published in 2022 and 2023, followed by three studies about R2L attacks on CPS (Goel, 2015; Green et al., 2020; Sen, 2022), and two about an attack on a NCS critical infrastructure (Salisbury et al., 2011; Sen et al., 2022). In their study of DDoS attacks, Salisbury et al. (2011) indicate that "given vulnerabilities of these systems, the movement toward a smart electrical grid which would be even more dependent on information systems and networks, presents yet another concern" (p. 301). Sen et al. (2022) is a particularly rich article that not only gives specific examples of all types of attack classes and targets, but also addresses most of the practices in the rest of Appendix E.

Articles on R2L attacks are growing in popularity with more than half (n=17) being published during or after 2019. For example, Boyson et al. (2019) research the extent to which the perceptions of threat and other factors influence students to avoid using wearable activity tracking devices and an associated health fitness data account. The authors acknowledge that the vector of attacks between the wearable device, the user's smartphone (via Bluetooth), and the private data stored on the device poses both a data threat and a personal security threat. Articles on DoS/DDoS attacks are also common and frequently describe attacks are on stock values and hacker communities (e.g., Yayla and Hu, 2011; Samtani et al., 2017; Ebrahimi et al., 2020, Li and Chen, 2022; Samtani et al. 2022).

While a number of sectors have been specifically studied, the most popular object of study is the financial sector with twelve articles. Retail organizations are represented in five articles. Other industries that are explored are health, government, software, and law enforcement. Please see Appendix G for more details.

Thirteen articles have been published which specifically focus on vulnerabilities. An excellent example is one by Samtani et al. (2022) which uses design science to build a system to prioritize vulnerabilities that are most likely to be attacked by black-hat hackers. Another example is the model assessing software vulnerabilities and the timing of patch releases (Arora, 2010).

Payloads

A main focus of the IS literature is on data breaches (n=31), which is the topic of most concern to practitioners. IS research is primarily based on public sources, such as public financial market data. It examines a variety of topics, including live breach cases (Ivaturi et al., 2020), breach disclosures (Wang et al., 2013; Wang and Ngai, 2022), financial consequences associated with data breaches (Jeong et al., 2019), and perceived "greenwashing" efforts associated with security exploitation (D'Arcy et al., 2020). Attackers may use the same form of public reporting as researchers. Relatedly, Liu et al. (2014) propose a model of collaboration that encourages information sharing among its members while also offering insurance coverage should their collaboration result in a loss because of a cyberattack. Two emerging payload types (mostly in 2022) are ransomware (e.g., Li and Chen, 2022; Pigola and da Costa, 2023) and Advanced Persistent Threats (APTs) (Shin et al., 2018; Kotsias et al., 2023, Plachkinova and Vo, 2023). Particularly relevant is the work by Kotsias et al. (2023), who emphasize that APTs are increasingly sophisticated because they recruit IT experts into purpose-built teams and deploy military-grade cyber weaponry in high-precision attacks. Earlier, Shin et al. (2018) illustrate the importance of developing frameworks to prevent state-led cyberattacks and private-led cyberattacks using an approach utilizing multiple case studies. They highlight the state level the Stuxnet attack on Iran's nuclear facility in 2010, as well as the 3/20 Advanced Persistent Threat (APT) attack that caused major economic damage (US$867.2 million) to South Korea in 2013. They complement their work investigating the hacking and advanced persistent threat attack against SK Communications in Korea in 2011, in which information of about 35 million customers was stolen. These studies illustrate the dangerous consequences of cyberattacks on nations and companies. Plachkinova and Vo (2023) use mix methods to demonstrate that the TRACI taxonomies can successfully capture the characteristic of various cyberattacks against critical infrastructure.

Attackers and defenders

Thirteen studies are about attacks from insiders. For example, researchers explore ways to identify cues that herald an insider attack (Willison et al., 2018), use a unique mix of personality traits to assess insider intentions (Johnston et al., 2016), and benefit from firm diversity as a way of coordinating security strategies and enhancing information security liaisons (Wang and Ngai, 2022). Most attacker studies are about black-hat hackers (n=20). Hui et al. (2017) emphasize the difficulty of obtaining field data about the motivations and behaviors of "black-hat" hackers. The twenty studies of defenders focus on challenges related to social dynamics (Green et al., 2020), security culture across business professions (Ramachandran et al., 2013), C-level managers (Pienta et al., 2020; Haislip et al., 2021), and employee network behavior (Adler et al., 2006). Jalali et al. (2019) is a good example of research about defenders. Specifically, they examine the proactiveness of experienced and less experienced managers in building cybersecurity capabilities. Ebrahimi et al. (2022) do a particularly good job describing how their research could assist cybersecurity professionals at multiple levels: At the operational level it may assist security management, information security officers (ISOs) and practitioners in cybersecurity analytics organizations; At the strategic level it may assist ISS managers (ISSMs) and CISOs. Four more studies relate to "white-hat" hackers. Wang et al.'s (2023) study of the Chinese Computer Misuse Act found that the law had a chilling effect not only on

black-hat hackers, but also, unfortunately, on the helpful contributions of white-hat hackers and cybersecurity professionals. Eight articles deal with state-sponsored attacks.

Taxonomies and Frameworks

Twenty-four articles offer a theoretical model or framework specifically focused on cyber defense. Although only eleven were published before 2020, some cyber professionals are using these older taxonomies and frameworks as they fight against cyberattackers (e.g., Simmons et al., 2014; Hutchins et al., 2011; Zhang and Thing, 2021). Beebe and Rao (2010) present an interesting offender taxonomy (e.g., offender motivation, skill, the offender-victim relationship, and offender involvement). More recently, Pigola and Da Costa (2023) propose a Dynamic Capability and Cybersecurity Intelligence (DCCI) framework that is related to the Plan-Do-Check-Act cycle used in practice as part of the ISO standards. Plachkinova and Vo (2023) develop a theory-backed taxonomy for risk assessment of cyberattacks on critical infrastructures (TRACI). Kotsias et al. (2023) encourage adopting and integrating CTI usage to tackle advanced adversaries (APT) as a key enabler for cyber defense, e.g., tracking and breaking the attacker's kill chain. Dincelli and Chengalur-Smith (2020) also draw from the military-related work on the cyber kill chain, namely the first phase of reconnaissance, to address design of SETA.

Countermeasures

Fifty-two articles out of 125 focus on *formal controls* such as training in SETA campaigns (Jensen et al., 2020) For example, Jensen et al. (2020) apply social judgment theory and reported that training in SETA campaigns should build on collective experiences and understanding of attacks. Some deal with security policies. Herath and Rao (2009) address formal control with their Protection Motivation and Deterrence Model (PMDT) that links perceptions of the severity of the breach, response efficacy, and self-efficacy with attitudes toward security policies. Lowry et al. (2015) report how to deter reactive computer abuse following enhanced organizational information security policies. IS researchers have published 36 articles about *technical controls*, such as technologically-enforced passwords or trusted identity (Belanger et al., 2017; Crossler and Posey, 2017) antimalware software (e.g., Lee and Larsen, 2009; Sharma et al., 2020), or Intrusion Detection System (Cavusoglu et al., 2005), to name a few. Thirty-two articles relate to *informal control*. For example, Posey et al. (2014) suggest that employees feel a sense of personal responsibility or obligation to protect their organizations' information resources. Smith et al. (2010) interpret power, resistance, norms, and cultural relationships in the compliance process. Schuetz et al. (2020) draw conclusions about the effectiveness of concrete fear appeals on information security.

Appendix G. Sectors in the IS literature

Specific/context sector (n=25)	Articles
Banking/Financial (n=11)	Bagchi and Udo, (2003); Dhillon and Torkzadeh, (2006); Yayla and Hu, (2011); Liu et al., (2014); Li et al., (2016); Benaroch, (2018); Hua et al., (2018); Naidoo, (2020); Haislip et al., (2021); Kotsias et al. (2023); Raddatz et al., (2023)
Retail (n=5)	Goodman and Ramer, (2007); Lee and Larsen, (2009); Baskerville et al., (2014); Hovav and Gray, (2014); Li and Chen, (2022)
Government (n=4)	Smith et al. (2010); Shin et al. (2018); Green et al., (2020); Helm (2022)
Hospital (n=3)	Herath and Rao, (2009); Kim and Kwon, (2019); Samtani et al. (2022)
Software (n=1)	Sen et al. (2020)
Law enforcement (n=1)	Yoo et al. (2020)

Appendix H. Coding of the articles per Kline's cybernetic avenues and imported theories

Avenues descriptions and associated imported theories	Source
First avenue (n=91): Minimal self-organizing system Imported theories: organizational and behavioral sciences, law	Knapp et al. (2003); Whitworth and Zaic (2003); Ma and Pearson (2005); Adler et al. (2006); Dhillon and Torkzadeh (2006); Dinev and Hu (2007); Goodman and Ramer (2007); Lim (2008); Lee and Larsen (2009); Boss et al. (2009); Herath and Rao (2009); Liang and Xue (2009); Anderson et al. (2010); Beebe and Rao (2010); Liang and Xue (2010); Smith et al. (2010); Karjarlainen and Siponen (2011); Salisbury et al. (2011); Yayla and Hu (2011); Ramachandran et al. (2013); Baskerville et al. (2014); Beebe et al. (2014); Goel and Shawky (2014); Herath et al. (2014); Hovav and Gray (2014); Nicho and Kamoun (2014); Posey et al. (2014); Yadav and Dong (2014); Goel (2015); Lowry et al. (2015); Anderson et al. (2016); Appan and Bačić (2016); Johnston et al. (2016); Wang et al. (2016); Wolff (2016); Belanger et al. (2017); Crossler and Posey (2017); Hui et al. (2017); Wang et al. (2017); Hua et al. (2018); Jeong et al. (2018); Shin et al. (2018); Willison et al. (2018); Benjamin et al. (2019); Boyson et al. (2019); Carpenter et al. (2019); Orazi et al. (2019); Dincelli and Chengalur-Smith (2020); Green et al. (2020); Ivaturi et al. (2020); Jeagert and Eckhardt, (2020); Jensen et al. (2020); Naidoo (2020); Pienta et al. (2020); Schuetz et al. (2020); Vedadi and Warkentin (2020); Wallace et al. (2020); Yoo et al. (2020); Zhuang et al. (2020); Chen et al. (2021a); Chen et al. (2021b); Goel et al. (2021); Haislip et al. (2021); Helm (2021), Kam et al.

(*continued on next page*)

(*continued*)

Avenues descriptions and associated imported theories	Source
	(2021); Ogbanufe et al. (2021); Ng et al. (2021); Nguyen et al. (2021); Nguyen et al. (2023); Vedadi et al. (2021); Wu et al. (2021); Andersson et al. (2022); D'Arcy and Basoglu (2022); Donalds and Barclay (2022); Chen et al. (2022); Ghahramani et al. (2022); Wang and Ngai (2022); Plachkinova and Vo (2023); Ayaburi and Andoh-Baidoo (2023); Burns et al. (2023); Bahreini et al. (2023); Cheng et al. (2023); Frauenstein et al. (2023); Hassandoust and Johnston (2023); Kotsias et al. (2023); Liang et al. (2023); Pigola and Da Costa (2023); Raddatz et al. (2023); Tejay and Mohammed (2023); Zhao et al. (2023); Xu et al. (2023)
Second avenue (n=24): Simulating human thoughts Information processing, decision-making, optimization, heuristic, simulation and gaming	Bagchi and Udo (2003); Cavusoglu et al. (2005); Katos and Adams (2005); Gal-Or and Ghose (2005); Bose and Leung (2007); Goel and Shawky (2009); Ransbotham and Mitra (2009); Arora et al. (2010); Mookerjee et al. (2011); Hua and Bapna (2013); Wang et al. (2013); Zhao et al. (2013); D'Arcy et al. (2014); Liu et al. (2014); Benjamin et al. (2016); Temizkan et al. (2017); Benaroch (2018); Hui et al. (2019); Jalali et al. (2019); Kim and Kwon (2019); Roumani and Nwankpa (2020); Sen et al. (2020); Tripathi and Mukhopadhyay (2022); Wang et al. (2023)
Artificial intelligence (n=10): computer sciences, machine learning	Li et al. (2016); Samtani et al. (2017); Ebrahimi et al. (2020); Sharma et al. (2020); Syed (2020); Ebrahimi et al. (2022); Li and Chen (2022); Samtani et al. (2022); Sen et al. (2022); Asatiani et al. (2023)

References

Ahmad, A., Maynard, S.B., Park, S., 2014. Information security strategies: towards an organizational multi-strategy perspective. J. Intell. Manuf. 25 (2), 357–370.

Ahmad, A., Webb, J., Desouza, K.C., Boorman, J., 2019. Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack. Comput. Secur. 402–418.

Aiyanyo, I.D., Samuel, H., Lim, H., 2020. A systematic review of defensive and offensive cybersecurity with machine learning. Appl. Sci. 10 (17), 5811.

Alder, G.S., Noel, T.W., Ambrose, M.L., 2006. Clarifying the effects of Internet monitoring on job attitudes: The mediating role of employee trust. Inf. Manag. 43 (7), 894–903.

Alharbi, A., Alhaidari, S., Zohdy, M., 2018. Denial-of-Service, Probing, User to Root (U2R) & Remote to User (R2L) Attack Detection using Hidden Markov Models. International Journal of Computer and Information Technology 204–210.

Ampel, B.M., Samtani, S., Zhu, H., Chen, H., 2024. Creating proactive Cyber Threat Intelligence with hacker exploit lables: A deep transfer learning approach. MIS Q. 48 (1), 137–166.

Anderson, C.L., Agarwal, R., 2010. Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. MIS Q. 613–643.

Anderson, B.B., Vance, A., Kirwan, C.B., Jenkins, J.L., Eargle, D., 2016. From warning to wallpaper: Why the brain habituates to security warnings and what can be done about it. J. Manag. Inf. Syst. 33 (3), 713–743.

Andersson, A., Hedström, K., Karlsson, F., 2022. Standardizing information security–a structurational analysis. Inf. Manag. 59 (3), 103623.

Appan, R., Bačić, D., 2016. Impact of information technology (IT) security information sharing among competing IT firms on firm's financial performance: An empirical investigation. Commun. Assoc. Inf. Syst. 39 (1), 12.

Arora, A., Krishnan, R., Telang, R., Yang, Y., 2010. An empirical analysis of software vendors' patch release behavior: impact of vulnerability disclosure. Inf. Syst. Res. 21 (1), 115–132.

Asatiani, A., Hakkarainen, T., Paaso, K., Penttinen, E., 2023. Security by envelopment–a novel approach to data-security-oriented configuration of lightweight-automation systems. Eur. J. Inf. Syst. 1–23.

Ashby, W.R., 1957. An Introduction to Cybernetics. Chapman & Hall, London.

Ayaburi, E.W., Andoh-Baidoo, F.K., 2023. How do technology use patterns influence phishing susceptibility? A two-wave study of the role of reformulated locus of control. Eur. J. Inf. Syst. 1–21.

Bagchi, K., Udo, G., 2003. An analysis of the growth of computer and Internet security breaches. Commun. Assoc. Inf. Syst. 12 (1), 46.

Bahrami, P., Dehghantanha, A., Dargahi, T., Parizi, R., Choo, K., Javadi, H., 2019. Cyber kill chain-based taxonomy of advanced persistent threat actors: Analogy of tactics, techniques, and procedures. J. Inf. Process. Syst. 15 (4), 865–889.

Bahreini, A.F., Cavusoglu, H., Cenfetelli, R.T., 2023. How "What you think you know about cybersecurity" can help users make more secure decisions. Inf. Manag. 60 (7), 103860.

Banks, K.W., 2009. Global Diffusion of the Internet XIV: The Internet in Iraq and Its Societal Impact. Commun. Assoc. Inf. Syst. 24 (1), 10.

Baskerville, R., 1993. ISS design methods: implications for information systems development. *ACM Comput. Surv.* (CSUR) 25 (4), 375–414.

Baskerville, R., Spagnoletti, P., Kim, J., 2014. Incident-centered information security: Managing a strategic balance between prevention and response. Inf. Manag. 51 (1), 138–151.

Beebe, N.L., Rao, V.S., 2010. Improving organizational information security strategy via meso-level application of situational crime prevention to the risk management process. Commun. Assoc. Inf. Syst. 26 (1), 17.

Beebe, N.L., Young, D.K., Chang, F.R., 2014. Framing information security budget requests to influence investment decisions. Commun. Assoc. Inf. Syst. 35 (1), 7.

Bélanger, F., Collignon, S., Enget, K., Negangard, E., 2017. Determinants of early conformance with information security policies. Inf. Manag. 54 (7), 887–901.

Benaroch, M., 2018. Real Options Models for Proactive Uncertainty-Reducing Mitigations and Applications in Cybersecurity Investment Decision Making. Inf. Syst. Res. https://doi.org/10.1287/isre.2017.0714.

Benjamin, V., Zhang, B., Nunamaker Jr, J.F., Chen, H., 2016. Examining hacker participation length in cybercriminal internet-relay-chat communities. J. Manag. Inf. Syst. 33 (2), 482–510.

Benjamin, V., Valacich, J.S., Chen, H., 2019. DICE-E: A Framework for Conducting Darknet Identification, Collection. Evaluation with Ethics. *MIS Quarterly* 43 (1), 1–22. https://doi.org/10.25300/misq/2019/13808.

Biamonte, J., Wittek, P., Pancotti, N., Rebentrost, P., Wiebe, N., Lloyd, S., 2017. Quantum machine learning. Nature 549 (7671), 195–202.

Bodeau, D.J., Graubart, R.D., McQuaid, R.M., Woodill, J., 2018. Cyber Resiliency Metrics Catalog. The MITRE Corporation, Bedford, MA.

Bose, I., Leung, A.C.M., 2007. Unveiling the mask of phishing: Threats, preventive measures, and responsibilities. Commun. Assoc. Inf. Syst. 19 (1), 24.

Boss, S.R., Kirsch, L.J., Angermeier, I., Shingler, R.A., Boss, R.W., 2009. If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. Eur. J. Inf. Syst. 18 (2), 151–164.

Boysen, S., Hewitt, B., Gibbs, D., McLeod, A., 2019. Refining the threat calculus of technology threat avoidance theory. Commun. Assoc. Inf. Syst. 45 (1), 5.

Burns, A.J., Roberts, T.L., Posey, C., Lowry, P.B., Fuller, B., 2023. Going beyond deterrence: A middle-range theory of motives and controls for insider computer abuse. Inf. Syst. Res. 34 (1), 342–362.

Carpenter, D., Young, D. K., Barrett, P., McLeod, A. J. 2019. Refining technology threat avoidance theory. *Communications of the Association for Information Systems*, 44.

Cavusoglu, H., Mishra, B., Raghunathan, S., 2005. The value of intrusion detection systems in information technology security architecture. Inf. Syst. Res. 16 (1), 28–46.
Chen, Y., Galletta, D.F., Lowry, P.B., Luo, X., Moody, G.D., Willison, R., 2021a. Understanding inconsistent employee compliance with information security policies through the lens of the extended parallel process model. Inf. Syst. Res. 32 (3), 1043–1065.
Chen, R., Kim, D.J., Rao, H.R., 2021b. A study of social networking site use from a three-pronged security and privacy threat assessment perspective. Inf. Manag. 58 (5), 103486.
Chen, Y., Luo, X.R., Li, H., 2022. Beyond adaptive security coping behaviors: Theory and empirical evidence. Inf. Manag. 59 (2), 103575.
Cheng, X., Hsu, C., Wang, T.D., 2022. Talk too much? The impact of cybersecurity disclosures on investment decisions. Commun. Assoc. Inf. Syst. 50 (1), 26.
Cheng, C., Lu, R., Petzoldt, A., Takagi, T., 2017. Securing the Internet of Things in a quantum world. IEEE Commun. Mag. 55 (2), 116–120.
Chng, S., Lu, H.Y., Kumar, A., Yau, D., 2022. Hacker types, motivations and strategies: A comprehensive framework. Computers in Human Behavior Reports 5, 1006167. https://doi.org/10.1016/j.chbr.2022.100167.
Clarke, M., & Oxman, A. D. 2001. Cochrane Reviewers' Handbook 4.1. *Review Manager* (RevMan). The Cochrane Collaboration, Updated June, 2000Version, 4.
Coden, M. Reeves, M, Pearlson, K. Madnick, S, & Berriman, C. 2023. An action plan for cyber resilience. *Sloan Management Review*, https://cams.mit.edu/wp-content/uploads/2023-01-04_SMR.pdf (accessed 19 February 2023).
Crossler, R., Posey, C., 2017. Robbing Peter to pay Paul: Surrendering privacy for security's sake in an identity ecosystem. J. Assoc. Inf. Syst. 18 (7), 2.
D'Arcy, J., Hovav, A., Galletta, D., 2009. User awareness of security counter-measures and its impact on information systems misuse: A deterrence approach. Information System Research 20, 79–98. https://doi.org/10.1287/ISRE.1070.0160.
D'Arcy, J., Adjerid, I., Angst, C.M., Glavas, A., 2020. Too good to be true: Firm social performance and the risk of data breach. Inf. Syst. Res. 31 (4), 1200–1223.
D'Arcy, J., Basoglu, A., 2022. The influences of public and institutional pressure on firms' cybersecurity disclosures. J. Assoc. Inf. Syst. 23 (3), 779–805.
Dbir, 2024. Verizons Data Breach investigations Report (DBIR) 2024. accessed 3 May 2024. https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf.
Dewar, R. S. 2017. Active cyber defense. CSS Cyberdefense Trend Analyses, 1. Center for Security Studies (CSS), ETH Zürich. https://doi.org/10.3929/ethz-b-000169631.
Dhillon, G., 2007. Principles of ISS: Texts and Cases. John Wiley & Sons Incorporated.
Dhillon, G., Backhouse, J., 2001. Current directions in ISS research: towards socio-organizational perspectives. Inf. Syst. J. 11 (2), 127–153.
Dhillon, G., Smith, K., Dissanayaka, I., 2021. ISS research agenda: Exploring the gap between research and practice. J. Strateg. Inf. Syst. 30 (4), 101693.
Dhillon, G., Torkzadeh, G., 2006. Value-focused assessment of information system security in organizations. Information System Journal 16, 293–314. https://doi.org/10.1111/j.1365-2575.2006.00219.x.
Diesch, R., Pfaff, M., Krcmar, K., 2020. A comprehensive model of information security factors for decision-makers. Comput. Secur. 92, 101747.
Dincelli, E., Chengalur-Smith, I., 2020. Choose your own training adventure: designing a gamified SETA artefact for improving information security and privacy through interactive storytelling. Eur. J. Inf. Syst. 29 (6), 669–687.
Dinev, T., Hu, Q., 2007. The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information, Technologies. Journal of the Association of Information System 8, 386–408. https://doi.org/10.17705/1jais.00133.
Donalds, C., Barclay, C., 2022. Beyond technical measures: a value-focused thinking appraisal of strategic drivers in improving information security policy compliance. Eur. J. Inf. Syst. 31 (1), 58–73.
Dorn, A.W., 2009. Intelligence-led peacekeeping: The United Nations stabilization mission in Haiti (MINUSTAH), 2006–07. Intelligence and National Security 24 (6), 805–835.
Drias, Z., Serhrouchni, A., & Vogel, O. 2015. Analysis of cyber security for industrial control systems. In 2015 international conference on cyber security of smart cities, industrial control system and communications (ssic), 1-8.
Duffany, J., 2018. Computer Security. *Computer and Network Security Essentials*. Springer, Cham, pp. 3–20.
Dunjko, V., Briegel, H.J., 2018. Machine learning & artificial intelligence in the quantum domain: a review of recent progress. Rep. Prog. Phys. 81 (7), 074001.
Ebrahimi, M., Nunamaker Jr, J.F., Chen, H., 2020. Semi-supervised cyber threat identification in dark net markets: a transductive and deep learning approach. J. Manag. Inf. Syst. 37 (3), 694–722.
Ebrahimi, M., Chai, Y., Samtani, S., Chen, H., 2022. Cross-lingual cybersecurity analytics in the international dark web with adversarial deep representation learning. MIS Q. 46 (2).
ECB, 2021. ECB Annual Report on supervisory activities 2021. https://www.bankingsupervision. europa.eu/press/publications/annual-report/html/ssm.ar2021~52a7d32451.en.html (accessed 30 October 2022).
ENISA, 2021. Post Quantum Cryptography, current state of quantum mitigation. https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation DOI: 10.2824/92307 (accessed 23 January 2023).
Fingas, J., 2022. Cyberattack takes down Israeli government websites. retrieved on 3 January, 2023 Engadget. https://www.engadget.com/israel-faces-cyberattack.html.
Fleury, T., Khurana, H., Welch, V., 2008. Towards a taxonomy of attacks against energy control systems. International Conference on Critical Infrastructure Protection. Springer, Boston, MA.
Frauenstein, E.D., Flowerday, S., Mishi, S., Warkentin, M., 2023. Unraveling the behavioral influence of social media on phishing susceptibility: A Personality-Habit-Information Processing model. Inf. Manag. 60 (7), 103858.
Gal-Or, E., Ghose, A., 2005. The economic incentives for sharing security information. Inf. Syst. Res. 16 (2), 186–208.
Ghahramani, F., Yazdanmehr, A., Chen, D., Wang, J., 2023. Continuous improvement of information security management: an organisational learning perspective. Eur. J. Inf. Syst. 32 (6), 1011–1032.
Glick, A., 2019. Why attack Mitre matters. retrieved on January 3, 2023. https://symantec-enterprise-blogs.security.com/blogs/expert-perspectives/why-mitre-attck-matters.
Goel, S., 2015. Anonymity vs. security: The right balance for the smart grid. Commun. Assoc. Inf. Syst. 36 (1), 2.
Goel, S., Shawky, H.A., 2009. Estimating the market impact of security breach announcements on firm values. Inf. Manag. 46 (7), 404–410.
Goel, S., Shawky, H.A., 2014. The impact of federal and state notification laws on security breach announcements. Commun. Assoc. Inf. Syst. 34 (1), 3.
Goel, S., Williams, K.J., Huang, J., Warkentin, M., 2021. Can financial incentives help with the struggle for security policy compliance? Inf. Manag. 58 (4), 103447.
Goodman, S.E., Ramer, R., 2007. Global sourcing of IT services and information security: Prudence before playing. Commun. Assoc. Inf. Syst. 20 (1), 50.
Green, A.W., Woszczynski, A.B., Dodson, K., Easton, P., 2020. Responding to Cybersecurity Challenges: Securing Vulnerable US Emergency Alert Systems. Commun. Assoc. Inf. Syst. 46 (1), 8.
Greene, T. 2016. Why the 'cyber kill chain' needs an upgrade. Network World From IDG, https://www. Networkworld.com/article/3104542/security/why-the-cyber-kill-chain-needs-an-upgradesecurity-pros-need-to-focus-more-on-catching-attackers-aft.html, (accessed 19 February 2022).
Gupta, S., Mohanta, S., Chakraborty, M., Ghosh, S., 2017. Quantum machine learning-using quantum computation in artificial intelligence and deep neural networks: Quantum computation and machine learning in artificial intelligence. *8th Ind.* Autom. Electromechanical Eng. Conf. IEMECON 268–274. https://doi.org/10.1109/IEMECON.2017.8079602.
Haga, K., Meland, P.H., Sindre, G., 2020. Breaking the cyber kill chain by modelling resource costs. In: International Workshop on Graphical Models for Security. Springer International Publishing, Cham, pp. 111–126.
Haislip, J., Lim, J.H., Pinsker, R., 2021. The impact of executives' IT expertise on reported data security breaches. Inf. Syst. Res. 32 (2), 318–334.
Hansman, S. (2003). *A taxonomy of network and computer attack methodologies*. Department of Computer Science and Software Engineering. University of Canterbury, Christchurch, New Zealand.
Harknett, R.J., Stever, J.A., 2011. The new policy world of cybersecurity. Public Adm. Rev. 71 (3), 455–460.

Hassan, W. U., Bates, A., & Marino, D., 2020 (May). Tactical provenance analysis for endpoint detection and response systems. *2020 IEEE Symposium on Security and Privacy (SP)* 1172-1189.
Hassandoust, F., Johnston, A.C., 2023. Peering through the lens of high-reliability theory: A competencies driven security culture model of high-reliability organisations. Inf. Syst. J. 33 (5), 1212–1238.
Hayes, A.F., Krippendorff, K., 2007. Answering the call for a standard reliability measure for coding data. Commun. Methods Meas. 1 (1), 77–89.
Helm, J.E., 2021. Distributed Internet voting architecture: A thin client approach to Internet voting. J. Inf. Technol. 36 (2), 128–153.
Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., Rao, H.R., 2014. Security services as coping mechanisms: An investigation into user intention to adopt an email authentication service. Inf. Syst. J. 24 (1), 61–84.
Herath, T., Rao, H.R., 2009. Protection motivation and deterrence: a framework for security policy compliance in organisations. Eur. J. Inf. Syst. 18 (2), 106–125.
Hovav, A., Gray, P., 2014. The ripple effect of an information security breach event: A stakeholder analysis. Commun. Assoc. Inf. Syst. 34 (1), 50.
Hua, J., Bapna, S., 2013. The economic impact of cyber terrorism. The Journal of Strategic Information Systems 22, 175–186. https://doi.org/10.1016/j.jsis.2012.10.004.
Hua, J., Chen, Y., Luo, X.R., 2018. Are we ready for cyberterrorist attacks?—Examining the role of individual resilience. Inf. Manag. 55 (7), 928–938.
Hui, K.L., Kim, S.H., Wang, Q.H., 2017. Cybercrime deterrence and international legislation: Evidence from distributed denial of service attacks. MIS Q. 41 (2), 497.
Hui, K.L., Ke, P.F., Yao, Y., Yue, W.T., 2019. Bilateral liability-based contracts in information security outsourcing. Inf. Syst. Res. 30 (2), 411–429.
Hutchins, E., Cloppert, M., Amin, R., 2011. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Leading Issues in Information Warfare & Security Research 1 (1), 80.
Hyatt, D., Cropanzano, R., Finfer, L. A., Levy, P., Ruddy, T. M., Vandaveer, V., & Walker S. 1997. Bridging the gap between academics and practice: *Suggestions from the field. Ind Psychol*, 35(1), 29-32L ;35(1):29–32. https://doi.org/10.1108/09604521211218936.
Imf, 2021. Global Cyber Threat to financial systems. accessed 22 October 2022. https://www.imf.org/external/pubs/ft/fandd/2021/03/pdf/global-cyber-threat-to-financial-systems-maurer.pdf.
Ivaturi, K., Bhagwatwar, A., 2020. Mapping sentiments to themes of customer reactions on social media during a security hack: a justice theory perspective. Inf. Manag. 57 (4), 103218.
Jaeger, L., Eckhardt, A., 2020. Eyes wide open: The role of situational information security awareness for security-related behaviour. Inf. Syst. J. 31 (3), 429–472.
Jahan, N., Naveed, S., Zeshan, M., Tahir, M.A., 2016. How to conduct a systematic review: a narrative literature review. Cureus 8 (11).
Jakub, P. 2022. Russia's war on Ukraine: Timeline of cyber-attacks. https://policycommons.net /artifacts/2476 881/russias-war-on-ukraine/3498934/ (accessed 12 February 2023).
Jalali, M.S., Siegel, M., Madnick, S., 2019. Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment. J. Strateg. Inf. Syst. 28 (1), 66–82.
Jensen, M.L., Durcikova, A., Wright, R.T., 2020. Using susceptibility claims to motivate behaviour change in IT security. Eur. J. Inf. Syst. 1–19.
Jeong, C.Y., Lee, S.Y.T., Lim, J.H., 2019. Information security breaches and IT security investments: Impacts on competitors. Inf. Manag. 56 (5), 681–695.
Johnson, J., 2019. Artificial intelligence & future warfare: implications for international security. Def. Secur. Anal. 35 (2), 147–169.
Johnston, A.C., Warkentin, M., McBride, M., Carter, L., 2016. Dispositional and situational factors: influences on information security policy violations. Eur. J. Inf. Syst. 25 (3), 231–251.
Kam, H.J., Ormond, D.K., Menard, P., Crossler, R.E., 2022. That's interesting: An examination of interest theory and self-determination in organisational cybersecurity training. Inf. Syst. J. 32 (4), 888–926.
Karjalainen, M., Siponen, M., 2011. Toward a new meta-theory for designing information systems (IS) security training approaches. J. Assoc. Inf. Syst. 12 (8), 3.
Katos, V., Adams, C., 2005. Modelling corporate wireless security and privacy. J. Strateg. Inf. Syst. 14 (3), 307–321.
Kean, 2021. Darktrace and Microsoft team up on AI cybersecurity https://www.siliconrepubli c.com/enterprise/darktrace-microsoft-ai-cybersecurity (accessed 19 February 2022).
Khan, S., Parkinson, S., 2018. Review into state of the art of vulnerability assessment using artificial intelligence. Guide to Vulnerability Analysis for Computer Networks and Systems. Springer, Cham, pp. 3–32.
Khooshabeh, P., Gale, L., 2018. Virtual human role players for studying social factors in organizational decision making. Front. Psychol. 9, 194.
Kim, S., Heo, G., Zio, E., Shin, J., Song, J.G., 2020. Cyberattack taxonomy for digital environment in nuclear power plants. Nucl. Eng. Technol. 52 (5), 995–1001.
Kim, S.H., Kwon, J., 2019. How do EHRs and a meaningful use initiative affect breaches of patient information? Inf. Syst. Res. 30 (4), 1184–1202.
Kline, R., 2011. Cybernetics, automata studies, and the Dartmouth conference on artificial intelligence. IEEE Ann. Hist. Comput. 33 (4), 5–16.
Knapp, E.D. & Langill, J.T., 2015. Industrial Network Security Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems, 2nd edition., Syngress (Elsevier), Massachusetts, USA.
Knapp, K., Morris, F., Rainer Jr, R.K., Byrd, T.A., 2003. Defense mechanisms of biological cells: A framework for network security thinking. Commun. Assoc. Inf. Syst. 12 (1), 47.
Kotsias, J., Ahmad, A., Scheepers, R., 2023. Adopting and integrating cyber-threat intelligence in a commercial organisation. Eur. J. Inf. Syst. 32 (1), 35–51.
Lee, Y., Larsen, K.R., 2009. Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. Eur. J. Inf. Syst. 18 (2), 177–187.
Lee, E. A., 2008 (May). Cyber physical systems: Design challenges. *11th IEEE international symposium on object and component-oriented real-time distributed computing (ISORC)* (pp. 363-369). IEEE. Lexicon, 2011.
Lexicon, The Cyber warfare Lexicon, v1.7.6. https://info.publicintelligence.net /USSTRATCOM-CyberWarfareLexicon.pdf (accessed May 2024).
Li, W., Chen, H., Nunamaker Jr, J.F., 2016. Identifying and profiling key sellers in cyber carding community: AZSecure text mining system. J. Manag. Inf. Syst. 33 (4), 1059–1086.
Li, W., Chen, H., 2022. Discovering Emerging Threats in the Hacker Community: A Nonparametric Emerging Topic Detection Framework. MIS Q. 46 (4), 2337–2350.
Liang, N., Hirschheim, R., Luo, X., Hollingsworth, H., 2023. Identifying the idiosyncrasies of behavioral information security discourse and proposing future research directions: A Foucauldian perspective. J. Inf. Technol. 38 (4), 382–415.
Liang, H., Xue, Y., 2009. Avoidance of information technology threats: A theoretical perspective. MIS Q. 71–90.
Liang, H., Xue, Y.L., 2010. Understanding security behaviors in personal computer usage: A threat avoidance perspective. J. Assoc. Inf. Syst. 11 (7), 1.
Lim, N., 2008. Escaping the computer-forensics certification maze: A survey of professional certifications. Commun. Assoc. Inf. Syst. 23 (1), 30.
Lindsay, J., 2020. Demystifying the Quantum Threat: Infrastructure, Institutions, and Intelligence Advantage. Secur. Stud. 29 (2), 335–361.
Linnhoff-Popien, C., 2020. PlanQK — Quantum Computing Meets Artificial Intelligence. Digit Welt 4, 28–35.
Liu, C.Z., Zafar, H., Au, Y.A., 2014. Rethinking fs-isac: An it security information sharing network model for the financial services sector. Commun. Assoc. Inf. Syst. 34 (1), 2.
Lowry, P.B., Posey, C., Bennett, R.B.J., Roberts, T.L., 2015. Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust. Inf. Syst. J. 25 (3), 193–273.
Ma, Q., Pearson, J.M., 2005. ISO 17799:" Best Practices" in Information Security Management? Commun. Assoc. Inf. Syst. 15 (1), 32.
Madnick, S. 2017. Preparing for the cyberattack that will knock out US power grids. Harvard Business Review 10 Study report by the University of Maryland retrieved from, https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds (accessed 6 June 2021).
Maurushat, A., 2019. Ethical Hacking. University of Ottawa Press, Ottawa.
McCarthy, J.J., Minsky, M.L., Rochester, N., 1959. Artificial intelligence. Research Laboratory of Electronics at the Massachusetts Institute of Technology (MIT).
Mookerjee, V., Mookerjee, R., Bensoussan, A., Yue, W.T., 2011. When hackers talk: Managing information security under variable attack rates and knowledge dissemination. Inf. Syst. Res. 22 (3), 606–623.
Naidoo, R., 2020. A multi-level influence model of COVID-19 themed cybercrime. Eur. J. Inf. Syst. 29 (3), 306–321.
Newell, A., Shaw, J.C., Simon, H.A., 1957. Empirical explorations of the logic theory machine: a case study in heuristic. Techniques for reliability, Western joint computer conference, pp. 218–230.

Newell, A., Simon, H.A., 1972. Human Problem Solving, Vol. 104, No. 9. Prentice-hall, Englewood Cliffs, NJ.
Ng, K.C., Zhang, X., Thong, J.Y., Tam, K.Y., 2021. Protecting against threats to information security: An attitudinal ambivalence perspective. J. Manag. Inf. Syst. 38 (3), 732–764.
Nguyen, C., Jensen, M.L., Durcikova, A., Wright, R.T., 2021. A comparison of features in a crowdsourced phishing warning system. Inf. Syst. J. 31 (3), 473–513.
Nguyen, C., Jensen, M., Day, E., 2023. Learning not to take the bait: a longitudinal examination of digital training methods and overlearning on phishing susceptibility. Eur. J. Inf. Syst. 32 (2), 238–262.
Nicho, M., Kamoun, F., 2014. Multiple case study approach to identify aggravating variables of insider threats in information systems. Commun. Assoc. Inf. Syst. 35 (1), 18.
Nist, 2014. Framework for Improving Critical Infrastructure Cybersecurity. Gaithersburg, MD, USA, In Cybersecurity Framework; National Institute of Standards and Technology, p. 41.
Ogbanufe, O., Kim, D.J., Jones, M.C., 2021. Informing cybersecurity strategic commitment through top management perceptions: The role of institutional pressures. Inf. Manag. 58 (7), 103507.
Okeke, F., 2022. 12 most in-demand cybersecurity jobs in 2022, TechRepublic. accessed 2 July 2022. https://www.techrepublic.com/article/hottest-cybersecurity-jobs/.
Oliver, D.J., Randolph, A.B., 2022. Hacker Definitions in Information Systems Research. J. Comput. Inf. Syst. 62, 397–409. https://doi.org/10.1080/08874417.2020.183 3379.
Orazi, D.C., Warkentin, M., Johnston, A.C., 2019. Integrating Construal-level Theory in Designing Fear Appeals in ISS Research. Commun. Assoc. Inf. Syst. 45. https://doi.org/10.17705/1CAIS.04522.
Paganini, P. 2022. Anonymous announced that the affiliate group Black Rabbit World has leaked 28 GB of data stolen from the Central Bank of Russia. https://securityaffairs.co/ wordpress/129490/hacking/central-bank-of-russia-data-leak-anonymous.html (accessed 3 January 2023).
Paliwal, S., Gupta, R., 2012. Denial-of-service, probing & remote to user (R2L) attack detection using genetic algorithm. International Journal of Computer Applications 60 (19), 57–62.
Paré, G., Trudel, M.C., Jaana, M., Kitsiou, S., 2015. Synthesizing information systems knowledge: A typology of literature reviews. Inf. Manag. 52 (2), 183–199.
Pfleeger, C.P., Pfleeger, S.L., 2012. Analyzing Computer Security: A Threat/vulnerability/ counter-measure Approach. Prentice Hall Professional.
Pham, H.C., Brennan, L., Furnell, S., 2019. Information security burnout: Identification of sources and mitigating factors from security demands and resources. Journal of Information Security and Applications 46, 96–107.
Pienta, D., Thatcher, J.B., Johnston, A., 2020. Protecting a whale in a sea of phish. J. Inf. Technol. 35 (3), 214–231.
Pigola, A., da Costa, P.R., 2023. Dynamic Capabilities in Cybersecurity Intelligence: A Meta-Synthesis to Enhance Protection Against Cyber Threats. Commun. Assoc. Inf. Syst. 53 (1), 46.
Plachkinova, M., Vo, A., 2023. A Taxonomy for Risk Assessment of Cyberattacks on Critical Infrastructure (TRACI). Commun. Assoc. Inf. Syst. 52 (1), 1.
Posey, C., Roberts, T.L., Lowry, P.B., Hightower, R.T., 2014. Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. Inf. Manag. 51 (5), 551–567.
Prior, T., Herzog, M., 2013. Risk Factsheet 9. Resilience Manifestation and Expression. ETH Zurich, The Practical Application of Resilience.
Protection Group International, Breaking down the cost of a cyberattack, Sept 5, 2023 https://www.pgitl.com/insights/breaking-down-the-cost-of-a-cyber-attack (Accessed May 17, 2024).
Raddatz, N., Coyne, J., Menard, P., Crossler, R.E., 2023. Becoming a blockchain user: understanding consumers' benefits realisation to use blockchain-based applications. Eur. J. Inf. Syst. 32 (2), 287–314.
Rai, A., 2016. Celebrating 40 years of MIS quarterly: MISQ's history and future through the lenses of its editors-in-chief. MIS Q. 40 (4), iii–xvi.
Raiyn, J., 2014. A survey of cyber attack detection strategies. International Journal of Security and Its Applications 8 (1), 247–256.
Ramachandran, S., Rao, C., Goles, T., Dhillon, G., 2013. Variations in information security cultures across professions: A qualitative study. Commun. Assoc. Inf. Syst. 33 (1), 11.
Ransbotham, S., Mitra, S., 2009. Choice and chance: A conceptual model of paths to information security compromise. Inf. Syst. Res. 20 (1), 121–139.
Roumani, Y., Nwankpa, J., 2020. Examining exploitability risk of vulnerabilities: a hazard model. Commun. Assoc. Inf. Syst. 46 (1), 18.
Rowe, F., 2014. What literature review is not: diversity, boundaries and recommendations. Eur. J. Inf. Syst. 23 (3), 241–255.
Rutkowski, A.F., Saunders, C., 2018. Emotional and Cognitive Overload. The Dark Side of Information Technology. Routledge.
Salisbury, W., Miller, D.W., Turner, L.C.J.M., 2011. On contending with unruly neighbors in the global village: Viewing information systems as both weapon and target. Commun. Assoc. Inf. Syst. 28 (1), 295–312.
Samtani, S., Chinn, R., Chen, H., Nunamaker Jr, J.F., 2017. Exploring emerging hacker assets and key hackers for proactive cyber threat intelligence. J. Manag. Inf. Syst. 34 (4), 1023–1053.
Samtani, S., Chai, Y., Chen, H., 2022. Linking Exploits from the Dark Web to Known Vulnerabilities for Proactive Cyber Threat Intelligence: An Attention-Based Deep Structured Semantic Model. MIS Q. 46 (2), 911–946.
Schatz, D., Bashroush, R., Wall, J., 2017. Towards a more representative definition of cyber security. J. Digit. Forensic Secur. Law 12 (2), 8.
Schuetz, S.W., Benjamin Lowry, P., Pienta, D.A., Bennett Thatcher, J., 2020. The effectiveness of abstract versus concrete fear appeals in information security. J. Manag. Inf. Syst. 37 (3), 723–757.
Schuld, M., Petruccione, F., 2018. *Supervised Learning with Quantum Computers*, 17. Springer, Berlin.
Schuld, M., Sinayskiy, I., Petruccione, F., 2015. An introduction to quantum machine learning. Contemp. Phys. 56 (2), 172–185.
Schulze, M. 2020. Cyber in war: Assessing the strategic, tactical, and operational utility of military cyber operations. *12th International Conference on Cyber Conflict (CyCon)*, 1300, 183-197.
Sen, R., Verma, A., Heim, G.R., 2020. Impact of cyberattacks by malicious hackers on the competition in software markets. J. Manag. Inf. Syst. 37 (1), 191–216.
Sen, R., Heim, G., Zhu, Q., 2022. Artificial Intelligence and Machine Learning in Cybersecurity: Applications, Challenges, and Opportunities for MIS Academics. Commun. Assoc. Inf. Syst. 51. https://doi.org/10.17705/1CAIS.05109.
Sharma, S., Kumar, N., Kumar, R., Krishna, C.R., 2020. The Paradox of Choice: Investigating Selection Strategies for Android Malware Datasets Using a Machine-learning Approach. Commun. Assoc. Inf. Syst. 46 (1), 26.
Shin, Y.Y., Lee, J.K., Kim, M., 2018. Preventing state-led cyberattacks using the bright internet and internet peace principles. J. Assoc. Inf. Syst. 19 (3), 3.
Shoorbajee, Z., 2018. New EAC chairman will continue to focus on election security. retrieved on January 3, 2023 Cyberscoop. https://www.cyberscoop.com/thomas-hickseac-chair/.
Siddiqi, M.A., Ghani, N., 2016. Critical analysis on advanced persistent threats. Int. J. Comput. Appl 141 (13), 46–50.
Silic, M., Lowry, P.B., 2021. Breaking Bad in Cyberspace: Understanding why and how Black Hat Hackers Manage their Nerves to Commit their Virtual Crimes. Inf. Syst. Front. 23, 329–341. https://doi.org/10.1007/s10796-019-09949-3.
Simmons, C., Shiva, S., Dasgupta, D., & Wu, Q. 2014. AVOIDIT: A cyber attack taxonomy. University of Memphis. *Proceedings of the 9th Annual Symposium on Information Assurance* (ASIA'14), Albany, NY, USA.
Siponen, M.T., 2005. An analysis of the traditional ISS approaches: implications for research and practice. Eur. J. Inf. Syst. 14 (3), 303–315.
Smith, S., 2023. Towards a scientific definition of cyber resilience. International Conference on Cyber Warfare and Security 18 (1), 379–386.
Smith, S., Winchester, D., Bunker, D., Jamieson, R., 2010. Circuits of power: A study of mandated compliance to an ISS" De Jure" standard in a government organization. MIS Q. 463–486.
Stubley, D., 2013. What is Cyber Security? accessed 23 August 2023. https://www.7elements.co.uk/resources/blog/what-is-cyber-security/.
Syed, R., 2020. Cybersecurity vulnerability management: A conceptual ontology and cyber intelligence alert system. Inf. Manag. 57 (6), 103334.
Tejay, G.P., Mohammed, Z.A., 2023. Cultivating security culture for information security success: A mixed-methods study based on anthropological perspective. Inf. Manag. 60 (3), 103751.

Temizkan, O., Park, S., Saydam, C., 2017. Software diversity for improved network security: optimal distribution of software-based shared vulnerabilities. Inf. Syst. Res. 28 (4), 828–849.
Templier, M., Paré, G., 2015. A framework for guiding and evaluating literature reviews. Commun. Assoc. Inf. Syst. 37, 6.
Tertrais, B., 2016. Article 5 of the Washington Treaty: Its Origins. Meaning and Future, NATO Defense College.
Tripathi, M., Mukhopadhyay, A., 2022. Does privacy breach affect firm performance? An analysis incorporating event-induced changes and event clustering. Inf. Manag. 59 (8), 103707.
Tzu, S. 2005. The art of war. Boston: Shambala. (Original work published in 5th century BCE).
United State Joint Force command, 2008. *The Joint Operating Environment: Challenge and Implications for the Future of Joint force* (2008). https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joe_2008.pdf?ver=2017-12-30-132024-953(accessed 23 August 2023).
Vedadi, A., Warkentin, M., 2020. Can secure behaviors be contagious? A two-stage investigation of the influence of herd behavior on security decisions. J. Assoc. Inf. Syst. 21 (2), 3.
Vedadi, A., Warkentin, M., Dennis, A., 2021. Herd behavior in information security decision-making. Inf. Manag. 58 (8), 103526.
Wallace, S., Green, K.Y., Johnson, C., Cooper, J., Gilstrap, C., 2020. An Extended TOE Framework for Cybersecurity-adoption Decisions. Commun. Assoc. Inf. Syst. 47 (1), 20.
Walls, A., Perkins, E., & Weiss, J. 2013. Definition: Cybersecurity, 5. Retrieved from Gartner.com website: https://www.gartner.com/doc/2510116/definition-cybersecurity (accessed 23 August 2023).
Wang, Q.H., Geng, R., Kim, S.H., 2023. Chilling Effect of the Enforcement of Computer Misuse Act: Evidence from Publicly Accessible Hack Forums. Inf. Syst. Res. https://doi.org/10.1287/isre.2019.0346.
Wang, T., Kannan, K.N., Ulmer, J.R., 2013. The association between the disclosure and the realization of information security risk factors. Inf. Syst. Res. 24 (2), 201–218.
Wang, J., Li, Y., Rao, H.R., 2016. Overconfidence in phishing email detection. J. Assoc. Inf. Syst. 17 (11), 1.
Wang, J., Li, Y., Rao, H.R., 2017. Coping responses in phishing detection: an investigation of antecedents and consequences. Inf. Syst. Res. 28 (2), 378–396.
Wang, Q., Ngai, E.W., 2022. Firm diversity and data breach risk: a longitudinal study. J. Strateg. Inf. Syst. 31 (4), 101743.
Wang, Q., Yang, H., 2019. A survey on the recent development of securing the networked control systems. Systems Science & Control Engineering 7 (1), 54–64.
Wen, S., N. He, &H. Yan. 2017. Detecting and Predicting APT Based on the Study of Cyber Kill Chain with Hierarchical Knowledge Reasoning. *Proceedings of the 2017 VI International Conference on Network, Communication and Computing*,115-119.
Whitworth, B., Zaic, M., 2003. The WOSP model: Balanced information system design and evaluation. Commun. Assoc. Inf. Syst. 12 (1), 17.
Wiener, N., 1948. Cybernetics or Control and Communication in the Animal and the Machine. MIT Press, Cambridge, MA.
Willison, R., Warkentin, M., Johnston, A.C., 2018. Examining employee computer abuse intentions: Insights from justice, deterrence and neutralization perspectives. Inf. Syst. J. 28 (2), 266–293.
Wolff, J., 2016. Perverse effects in defense of computer systems: When more is less. J. Manag. Inf. Syst. 33 (2), 597–620.
Wolff, E.D., Growley, K.M., Lerner, M.O., Welling, M.B., Gruden, M.G., Canter, J., 2021. Navigating the SolarWinds Supply Chain Attack. The Procurement Lawyer 56 (2), 3–11.
Wu, Y., Tayi, G.K., Feng, G., Fung, R.Y., 2021. Managing information security outsourcing in a dynamic cooperation environment. J. Assoc. Inf. Syst. 22 (3), 2.
Xu, F., Hsu, C., Wang, T., Lowry, P.B., 2023. The antecedents of employees' proactive information security behaviour: The perspective of proactive motivation. Inf. Syst. J. https://doi.org/10.1111/isj.12488.
Yadav, S.B., Dong, T., 2014. A comprehensive method to assess work system security risk. Commun. Assoc. Inf. Syst. 34 (1), 8.
Yayla, A.A., Hu, Q., 2011. The impact of information security events on the stock value of firms: The effect of contingency factors. J. Inf. Technol. 26 (1), 60–77.
Yoo, C.W., Goo, J., Rao, H.R., 2020. Is cybersecurity a team sport? A multilevel examination of workgroup information security effectiveness. MIS Q. 44 (2).
Zhang, H., Shu, Y., Cheng, P., Chen, J., 2016. Privacy and performance trade-off in cyber-physical systems. IEEE Netw. 30 (2), 62–66.
Zhang, L., Thing, V.L., 2021. Three decades of deception techniques in active cyber defense-retrospect and outlook. Comput. Secur. 106, 102288.
Zhao, H., Jiang, N., Cai, Z., Lim, E.T., Tan, C.W., 2023. Toward a taxonomy of corporate data protection malpractices and their causal mechanisms: A regulatory view. J. Inf. Technol. 38 (3), 319–333.
Zhao, X., Xue, L., Whinston, A.B., 2013. Managing interdependent information security risks: Cyberinsurance, managed security services, and risk pooling arrangements. J. Manag. Inf. Syst. 30 (1), 123–152.
Zhuang, Y., Choi, Y., He, S., Leung, A.C.M., Lee, G.M., Whinston, A., 2020. Understanding security vulnerability awareness, Firm incentives, and ICT development in Pan-Asia. J. Manag. Inf. Syst. 37 (3), 668–693.