*Online Journal of Applied Knowledge Management*

A Publication of the International Institute for Applied Knowledge Management

*Volume 12, Issue 1, 2024*

# Knowledge management and technology for enhanced cybersecurity effectiveness

**James Burrell,** Boston College, USA, james.burrell@bc.edu

**Nory Jones,** University of Maine, USA, njones@maine.edu

## Abstract

*Cybersecurity continues to be a major concern and presents significant challenges for businesses, governments, nonprofits, and individuals. Organizations are working diligently to mitigate threats to these entities while the rate of cybercrime continues to increase in sophistication and reach. Current models in cybersecurity are becoming increasingly ineffective against the velocity, agility, and persistence of cyber adversaries. This challenge presents an opportunity to consider concepts and methods in knowledge management to strategically evaluate and prioritize adversarial cyber threat activities. This research aims to explore a conceptual framework designed to provide cybersecurity professionals with new models for knowledge management to increase the effectiveness of the detection, mitigation, and attribution of these threats. This conceptual approach draws from the literature on knowledge management and cybersecurity to integrate key concepts into a new theoretical framework. This paper presents a new hybrid model for cybersecurity that integrates core concepts of the classic Nonaka and Takeuchi Knowledge Spiral and the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0 augmented with emerging artificial intelligence and machine learning technologies. The development of a hybrid cybersecurity model combined with proven knowledge management strategies for continual knowledge creation and innovation represents an integrative model designed to address emerging cybersecurity challenges.*

**Keywords**: Knowledge management, knowledge management models, cybersecurity framework, knowledge spiral, information sharing, cybersecurity, leadership, and culture.

## Introduction

The constantly changing cybersecurity environment represents an increasingly complex challenge to protect systems and data from exploitation and compromise by global adversaries. In terms of future predictions, "the global cost of cybercrime is expected to surge in the next four years, rising from $9.22 trillion in 2024 to $13.82 trillion" in comparison to the projected 2024 Gross Domestic Product (GDP) of the United States ($28.8 trillion), China ($18.5 trillion), and Germany ($4.5 trillion) (Fleck, 2024, para. 1; Statistics Times, 2024). The immensity of the problem is staggering and characterized by 880,418 complaints and $12.5 billion in potential losses in 2023 representing an approximate increase of 10% in complaints and 22% in losses compared to 2022 (Federal Bureau of Investigation, 2023, p. 3).

*DOI: https://doi.org/10.36965/OJAKM.2024.12(1)54-72*

*Accepting Editor: Meir Russ*

The 2024 United States (U.S.) Intelligence Community Threat Assessment identified China as the primary cyber threat to the U.S. based on the ability to initiate "aggressive cyber operations against U.S. critical infrastructure and military assets" and "China's cyber espionage operations have included compromising telecommunications firms, providers of managed services and broadly used software, and other targets potentially rich in follow-on opportunities for intelligence collection, attack, or influence operations" (U.S. Office of the Director of National Intelligence, 2024, p. 11). The report also suggests Russia, Iran, and North Korea pose significant cyber threats including attacks on critical infrastructure and election influence utilizing emerging technologies including Generative AI (GenAI).

In this paper, we examine human models of knowledge management and translate these models into a human and technology-based innovation model. The existing literature focuses on data and information gathering, analysis, and sharing. However, this paper focuses on the ability to capture rare, inimitable tacit knowledge, and share it effectively among Subject Matter Experts (SMEs) as well as potential training data for GenAI systems to continually create new knowledge. The goal is to create a competitive advantage in the cybersecurity realm to effectively harness the immense amount of knowledge distributed across many sectors and create a technology-enhanced knowledge management model that provides continuous learning and transfer of new knowledge to experts, creating a cyber-knowledge spiral.

## Literature Review

A classic definition of knowledge management is the process of capturing, distributing, and effectively using knowledge (Davenport, 1994; Koenig, 2018). Knowledge resources represent unique, rare, and non-imitable tacit knowledge with the ability to provide a competitive advantage when integrated into a knowledge management strategy. In rapidly changing complex business environments, the ability to harness and leverage tacit knowledge for continual knowledge creation and innovation, distribution, and use can increase organizational responsiveness, absorptive capacities, and competencies for competitive advantage, increased market value and profitability (Coad & Rao, 2007; Moustaghfir & Schiuma, 2013).

What is the relationship between knowledge creation and innovation? Noruzy et al. (2013) found a direct association between knowledge management as a requirement for innovation and resulting performance improvement in manufacturing firms. Their research demonstrated that organizational learning through knowledge management was critical for continual innovation and increased performance. Similarly, a study in the procurement field assessed the impact of innovation on performance and found that "61% of procurement leaders delivered better year-over-year savings performance than in 2017" (Deloitte, 2018, p. 4). The literature supports the association between knowledge creation and innovation in many different contexts with the suggestion that knowledge creation is the required precursor to innovation. In addition, current theories support the Open Innovation (OI) model involving cooperation between stakeholders inside and outside an organization for optimal knowledge creation and subsequent continual innovation (Alqahtani et al., 2023; Papa et al., 2020).

*DOI: https://doi.org/10.36965/OJAKM.2024.12(1)54-72*

*Accepting Editor: Meir Russ*

Applying knowledge management to cybersecurity practices can result in continual learning and innovation for competitive advantage relative to cyber adversaries. In addition, knowledge management continues to evolve by integrating technologies like artificial intelligence into knowledge creation, storage, transfer, and utilization. By integrating proven knowledge management models with emerging technologies, hybrid models could further contribute to potential competitive advantages. David et al. (2020) suggest knowledge sharing and an increase in absorptive capacity improve efficiency and effectiveness in mitigating cyber vulnerabilities. The authors also reiterate continual learning, which increases absorptive capacity and leads to continual innovation, which is necessary to protect against cyber-attacks.

The knowledge spiral, created by Nonaka and Takeuchi (1995) represents a foundational concept in knowledge sharing and creation and is accepted and practiced globally. According to Henderson and Callahan (2023), "The SECI model is recognized as one of the most relevant and comprehensive theoretical proposals in knowledge management" (para. 2). Given its credibility, the knowledge creation and sharing concept is used as one of the foundations for our hybrid model discussed in a later section.

## Moderating Variables in Knowledge Management

### Leadership and Culture

Leaders have organizational authority to allocate resources, establish the culture, and determine priorities, thus, demonstrating the inextricable link between leadership and culture (Groysberg et al., 2018). In knowledge sharing, they can embed norms and values, but assumptions can facilitate or impede it. Associations between effective leaders and innovation and new knowledge creation in organizations result from several major factors. Effective leaders can communicate and empower colleagues and stakeholders to take ownership and create a shared mission and vision as co-creators. Effective leaders are also responsible for creating the necessary culture and infrastructure to allow different knowledge and perspectives and the development of trust and shared meaning for knowledge creation and innovation to arise. In addition, leaders can bridge these differences and act as catalysts to create smoothly functioning ecosystems (Aghina et al., 2018; Hill, 2024). The inference is that leaders can create a culture to nurture knowledge sharing, resulting in continual new knowledge creation which is a prerequisite for an effective cybersecurity system. A McKinsey & Company survey also addressed the capabilities required to support and succeed in executing rapid transformational organizational change which emphasized that effective knowledge sharing and business intelligence are crucial for competitive advantage (Krishnan et al., 2023). Holste and Fields (2010) suggest two major types of trust are necessary for effective knowledge sharing: (1) affect-based trust, which means people have good relationships, and (2) cognition-based trust, which means people believe the expertise and knowledge of others can be trusted. In addition, the researchers maintain that affect and cognition-based trust are necessary for valid and effective knowledge creation, innovation, and transfer.

### Innovation and Collaboration

Aghina (2018) proposed a system of networks comprised of small "performance cells" for autonomy and accountability with a diversity of perspectives and expertise. The cells were

*DOI: https://doi.org/10.36965/OJAKM.2024.12(1)54-72*

*Accepting Editor: Meir Russ*

considered analogous to building blocks with the ability to be configured and interconnected in different ways. The networks infer knowledge creation and involve the integration of different knowledge and perspectives. Another classic theory known as "The Strength of Weak Ties" forms a foundation for effective knowledge transfer and new knowledge creation (Granovetter, 1973). The essence of the Strength of Weak Ties theory is one where homophilous groups have common backgrounds and strong relationships which promotes mutual understanding and effective transfer of tacit knowledge. However, homophilous groups tend to share the same foundation of knowledge which inhibits new knowledge creation. Thus, there is a need for "boundary-spanning" in the formation of heterophilous networks for credibility and commonalities with several different groups which can act as liaisons or translators to link different groups together to form more diverse networks. Diversity increases innovation through "creative abrasion" where people with different knowledge and perspectives unite to continually create new knowledge or innovation (Leonard-Barton, 1995).

Collaboration among heterophilous groups, integrated into knowledge management, represents a potential method to mitigate adversarial activities. Collaboration is evolving at different levels to include the U.S. Cybersecurity and Infrastructure Security Agency (CISA). According to Goldstein (2023), "In 2021, CISA and our partners across government and the private sector created a new kind of partnership organization — the Joint Cyber Defense Collaborative (JCDC)" (para. 1).

## The Role of Technology

The reliance on human analysis and decision processes is increasingly being outpaced by technological development, especially Artificial Intelligence (AI) and Machine Learning (ML) technologies. Rapid advancements in GenAI are reshaping the ability to monitor and respond to real-time cyber threats. Experts agree AI and ML advancements present opportunities and threats to defenders as attackers also discover new AI-enabled procedures and methods. Cyber analysts need to respond at the same speed as the threat to remain effective which emphasizes the need for new and creative ways to address cybersecurity. The severity of the problem is highlighted in a recent study by Palo Alto Networks, which "found that security teams take 145 hours – or around six days – on average to resolve a security alert, with 60% of organizations taking longer than four days. Previous Palo Alto research revealed threat actors often begin exploiting a newly disclosed vulnerability within hours, leaving a potentially lengthy window of exposure for many firms" (Muncaster, 2023, para. 4).

To mitigate these threats, some organizations are starting to use ML to detect and respond to cyber threats in a timely manner (Zorz, 2023). Moreover, organizations recognize the value of proactively detecting and mitigating vulnerabilities before being exploited by attackers. A current example is the Defense Advanced Research Projects Agency (DARPA) program Intelligent Generation of Tools for Security (INGOTS), which involves new techniques using AI and program analysis to measure vulnerabilities. In addition, the DARPA INGOTS program proactively enables human intervention integrated with information systems to detect and fix these high-risk vulnerabilities before an attack can occur (U.S. Defense Advanced Research Project Agency, 2023). DARPA has also established the Guaranteeing AI Robustness against Deception (GARD)

program, which identifies system foundations and vulnerabilities to enhance resilience and defensive measures (Velasquez, 2024).

A McKinsey & Company study suggests organizations should integrate technologies into every "nook and cranny" to enable seamless communication to support enterprise-wise detection and response. Integration includes a transformation to digital, automated processes and proactive approaches to learning and leveraging emerging technologies like "containers, micro-service architectures, and cloud-based storage and services" as well as artificial intelligence, machine learning, and the Internet of Things (IoT) (Aghina et al., 2018, Chapter 5). The integration and implementation of emerging technologies, including AI and ML, may also present adverse potential risks to security and privacy for information technology systems and data.

Sayan et al. (2019) referenced a report where some organizations receive over a million daily security alerts. Microsoft Corporation similarly reported its organization has identified over 20 billion security events per day (Krenz, 2023). In addition, the authors recognized an infrastructure for knowledge management provides a method for managing complex analysis and mitigation options to potentially prevent cyber incidents. There have been other advancements in improving cyber knowledge management, such as combining cyber threat intelligence with results from forensic examinations to improve cybersecurity risk management.

Developing effective prevention, detection, and response capabilities against increasingly complex attack patterns requires more than process improvement and automation. The volume of available network flow data, threat indicators, and intelligence information from internal and external sources rapidly develops into a big data challenge even for organizations with existing knowledge management models. Armenia and Loia (2021) researched the domain of knowledge and information management with a combination of external and internal knowledge to align information and create "harmonic relations" and collective knowledge systems. The application of technology to address the challenges associated with big data provides incredible potential for the improvement of knowledge management.

## Challenges

Several major challenges prevent collaboration, knowledge sharing, and new knowledge creation (innovation) to achieve the desired results which include the requirement for secrecy, leadership perception, institutional logic, resources, and limited cost value (Chang & Huang, 2023). Most cybersecurity practices involve information sharing rather than the sharing of knowledge. The ability to transmit valuable nuanced expert knowledge learned over time can potentially create valuable strategies and tactics against adversarial cyber-attack methods. Technological advances, adoption, and reliance on AI and ML systems for organizational functions and operations introduce increased institutional risk and requirements to secure these systems. AI and ML technologies have also evolved to provide the ability to detect patterns and indicators embedded within massive amounts of cyber threat intelligence at levels exceeding the capabilities of human analysts. However, even though governments and businesses are working to incorporate these technologies into cybersecurity practices and defenses, cyber adversaries have also adopted the use of AI and ML technologies to advance their capabilities.

*DOI: https://doi.org/10.36965/OJAKM.2024.12(1)54-72*

*Accepting Editor: Meir Russ*

### *Explicit vs. tacit knowledge*

Explicit knowledge has been codified and can be stored, searched, and shared in a database and network which forms the basis of most cybersecurity-sharing systems. In contrast, tacit knowledge represents the accumulated experiences and learning developed over time. Therefore, the value of a new knowledge management-based cybersecurity model provides the ability to include expert tacit knowledge for new knowledge creation using automated systems with the recognition that the ability to share tacit knowledge represents a more complex challenge.

### *Trust and privacy*

Cybersecurity threat information often contains extremely sensitive data to include organizational vulnerabilities and security strategies. Challenges exist with the ability to maintain the desired value and context of the information while protecting sensitive corporate information and business practices for the information sharing process. An association exists between trust and privacy where the level of trust can be determined based on personal or organizational reputation as well as policies and processes to define conditions of access to specific data. There have been efforts to incorporate privacy-enhancing functions into information-sharing mechanisms. According to Gartner (2024), sixty-three percent of organizations worldwide have adopted zero-trust and secure data sharing principles. The implementation may be more problematic in terms of identifying the appropriate scope, integration, communication, training, and other costs. However, leaders recognize the benefit of adopting industry best practices, and the concepts of privacy and trust are inextricably linked which demonstrates the importance of preventing data disclosure and protecting all stakeholders' privacy (Tuteja, 2022).

## Cybersecurity

Cyber adversaries continue to evolve and adapt with increased complexity. These adversaries possess multi-functional expertise with sophisticated approaches to outsource cybercrime as a service (CaaS) in specialized areas such as ransomware and malware as a service (MaaS). The interconnected nature of cybercrime enables an optimal collaboration environment, especially with the use of AI and ML to automate malware campaigns and avoid detection (Townsend, 2023).

The transition to a zero-trust security model has gained increasing support as a foundation for modern complex networking environments and requires every request for device, application, and data access to be authenticated, authorized, and encrypted. The concept of explicit validity and least privileged access combined with other information security methodologies, such as micro-segmentation, can increase the overall security level, minimize unauthorized lateral movement within networks, and provide the ability to detect potential security issues with advanced analytics (Microsoft Corporation, 2021).

Emerging technologies including quantum computing represent new potential threats to cybersecurity defense and the enablement of adversarial capabilities. According to Townsend (2023), the term “crypto apocalypse” is “the point at which quantum computing becomes powerful enough to use Shor's algorithm to crack PKI encryption” (para. 3). Shor suggests certain encrypted data will become vulnerable with the accessibility to practical large-scale quantum computational resources. The realization that the financial, industrial, defense, and intelligence sectors would be at increased risk, and although these technological capabilities are not operational today,

*DOI: https://doi.org/10.36965/OJAKM.2024.12(1)54-72*

*Accepting Editor: Meir Russ*

adversaries are acquiring and storing encrypted data and other information now to "harvest" it when the technology becomes available.

## Artificial Intelligence (AI) and Machine Learning (ML)

With the emergence of GenAI-enabled applications, there is a growing recognition of the capabilities of AI and ML and the potential impact on cybersecurity. Machine learning is a subset of artificial intelligence: "artificial intelligence refers to the general ability of computers to emulate human thought and perform tasks in real-world environments, while machine learning refers to the technologies and algorithms for the enablement of systems to identify patterns, make decisions, and improve themselves through experience and data" (Columbia University, 2023, paras. 5-9).

As discussed in an earlier section, cyber adversaries are becoming more sophisticated in their organization, structure, and use of AI and ML to increase the speed and complexity of their attacks. Therefore, the adoption and use of appropriate technologies are imperative to effectively counter emerging cyber threats. A crucial consideration for the adoption of AI and ML relates to trust associated with data and models "coupled with automation, it can improve our defense posture significantly—automatically taking action across the entire incident detection, investigation, and response lifecycle, without relying on human intervention" (Muppidi, 2023, para. 7). The speed associated with processes like threat detection could increase exponentially and represent a valuable tool in the fight against cybercrime.

# Other Considerations

## Information Sharing Organizations

Several national and international information sharing organizations and public-private partnerships have been established to improve awareness of cybersecurity threats. In the United States, the Executive Order for Promoting Private Sector Cybersecurity Information Sharing, enacted in 2015 encouraged the sharing of cybersecurity threat information within the private sector and between the private sector and government (U.S. Executive Office of the President, 2015). The establishment of the Information Sharing and Analysis Organization (ISAO) and Information Sharing and Analysis Center (ISAC) concepts provide centralized structures and resources to enable sharing between and within the private and public sectors (U.S. Cybersecurity and Information Systems Information Sharing Analysis Center, 2024). A representative example of this type of organization is the Information Technology ISAC (IT-ISAC), a nonprofit private sector organization, with a mission to provide a forum for managing risks in corporate IT infrastructures through cyber information sharing, analysis, and coordination. The sharing of information represents a useful resource for member organizations, but it does not explicitly indicate support for knowledge sharing and management.

Similarly, the U.S. Department of Homeland Security's CISA developed an Automated Indicator Sharing (AIS) service to broadly share threat intelligence across the public and private sectors. INTERPOL created the Cybercrime Knowledge Exchange (CKE) to support the ability of law enforcement, governments, international organizations, and cybersecurity industry experts to share non-investigative information where the "unique workspace represents a dynamic communication channel to enable users around the world to discuss the latest cybercrime trends, prevention

*DOI: https://doi.org/10.36965/OJAKM.2024.12(1)54-72*

*Accepting Editor: Meir Russ*

strategies, detection technologies, and investigation techniques with authorized colleagues globally" (Interpol, 2020, p. 2). INTERPOL also created the Cybercrime Collaborative Platform – Operation (CCP – Operation) to serve as a "centralized information hub for the coordination of global law enforcement operations against cybercrime. Hosting multiple, independent workspaces, this restricted-access platform enables operational stakeholders to share intelligence in an interactive and secure environment" (Interpol, 2020, p. 2).

Recognition of the critical importance of knowledge sharing in cybersecurity can be seen in the recent U.S. 2024 National Cybersecurity Strategy Implementation Plan focused on collaboration with virtually all stakeholders, including "private sector; civil society; state, local, tribal, and territorial governments, and international partners" (The White House, 2024, p. 4).

## Knowledge Structures for Cybersecurity

The U.S. National Initiative for Cybersecurity Education (NICE) Workforce Framework established a common taxonomy for cybersecurity and identified seven components: Analyze Collect and Operate, Investigate, Operate and Maintain, Oversee and Govern, Protect and Defend, and Secure Provision (Newhouse et al., 2017; Petersen et al., 2020). The NICE framework identifies knowledge management functions to identify, manage, and enable processes and resources to access intellectual and information content. The CSIAC, a U.S. Department of Defense-sponsored Center of Excellence, maintains technical focus areas in the fields of Cybersecurity, Knowledge Management, Information Sharing Modeling and Simulation, as well as Software Data and Analysis (U.S. CSIAC, 2024). The CSIAC distinguishes information sharing as data exchange, communication protocols and technological infrastructures, and knowledge management. Similarly, the globally accepted National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0 (2024) provides industry, government agencies, and other organizations guidelines for assessing and mitigating cybersecurity risks. The trust, acceptance, and use of the NIST Cybersecurity Framework 2.0 (2024) were the basis for the development of a proposed hybrid cybersecurity-knowledge management model.

Information systems security represents a domain predominantly reliant on the knowledge and experience of experts (Belsis et al., 2005). The objective of knowledge management systems in cybersecurity is to improve the ability to detect and respond to threats and reduce operational and business impacts. Sayan et al. (2019) studied the construction of ontologies for cybersecurity and determined the primary focus was general cyber and attack-specific knowledge and recognized the requirement to establish an ontology for cyber threat intelligence to incorporate relationships and key concepts such as vulnerability, product, and recommendations. A more recent study suggested the "development of an ontology for extortion attacks can provide a terminology for software, system components, and other elements in the chain of such cyber threats" (Keshavarzi & Ghaffary, 2023, p. 2). Given the enormity and complexity of creating an ontology, the application of AI and ML could be useful in its creation.

## Proposed Cybersecurity Knowledge Management Models

A hybrid model is presented for cybersecurity knowledge management based on the complexity of moderating variables in the knowledge management and cybersecurity domains identified in

*DOI: https://doi.org/10.36965/OJAKM.2024.12(1)54-72*

*Accepting Editor: Meir Russ*

the literature. The competitive advantage of a hybrid approach exists in the ability to harness the tacit knowledge of SMEs in different areas of cybersecurity. The continuous input of rare non-imitable knowledge with the technology-augmented integration of new knowledge created by cyber experts could lead to a sustainable competitive advantage against current and emerging cyber-attack methods.

## Conceptual Hybrid Cyber-Technology-Knowledge Management Models and Hypotheses

The first model draws upon the classic "knowledge spiral" creation model which represents a never-ending cycle of knowledge transfer for continual knowledge creation and innovation (Nonaka & Takeuchi,1995). The proposed hybrid model integrates several other related theories:

1. The theory of weak ties where SMEs with different, but crucial knowledge are integrated for new knowledge creation, otherwise referred to as "creative abrasion."
2. The McKinsey & Company study proposed a system of networks composed of small "performance cells" with autonomy and accountability, and a diversity of perspectives and expertise (Aghina et al., 2018). The researchers described these cells as building blocks with the ability to be configured in different ways. These cells could also represent unique Communities of Collaboration (CoCs) to integrate experts from different knowledge domains as mentioned in the previous paragraph based on the strength of weak ties theory which suggests innovation and new knowledge creation rely on the fusion of different levels of expertise, knowledge and perspectives (Granovetter, 1973).
3. The impact of emerging technologies on the effectiveness of current cybersecurity methods is creating new capabilities and limitations. The integration of emerging technologies and applications is intended to be represented in each element of the proposed Cyber Knowledge Spiral to facilitate the creation, transfer, and sharing of new knowledge.
4. Taxonomies and ontologies to create a shared understanding among the SMEs.
5. AI, ML, and cloud-based technologies are used to process, analyze, and share massive amounts of threat information and knowledge provided by SMEs. Advanced technologies augment the knowledge base enabling experts to learn, collaborate, and develop new knowledge integrated into the knowledge base.

The proposed Cyber Knowledge Spiral model could provide a national or global pool of cyber-SMEs with access to a network of CoCs. The network would be analogous to a decentralized model of inter-connected points (performance cells, containers) connected to a data warehouse or data lake-type system where new knowledge is introduced into the learning process (See Figure 1). To integrate the approach into the knowledge spiral model, we propose:

1. Socialization (Tacit to Tacit Knowledge Exchange).: The SME's can identify collaborate and communicate directly with other SMEs to share their knowledge. These tacit-to-tacit knowledge exchanges can occur in performance cells (CoCs) with new knowledge (innovation) accessible using a data warehouse. In addition, SMEs with different expertise (theory of weak ties) within these cells/CoCs could use the "creative abrasion" approach to develop new knowledge.

*DOI: https://doi.org/10.36965/OJAKM.2024.12(1)54-72*

*Accepting Editor: Meir Russ*

2. Externalization (Tacit to Explicit): SMEs would learn from the information contained in the data warehouse during the socialization phase and then codify new knowledge, providing context with examples. The creation of new knowledge represents potential training data for the AI and ML algorithms and SMEs.
3. Combination (Explicit to Explicit): A machine-learning model continually improves with new codified knowledge and patterns and creates new potential knowledge related to cyber threats, vulnerabilities, risks, and effective mitigation strategies.
4. Internalization (Explicit to Tacit): SMEs could query and learn from the continually evolving knowledge sources related to different aspects of cybersecurity.

The Cyber Spiral Model infers the integration of moderating variables of trust, collaboration, and effective leadership.

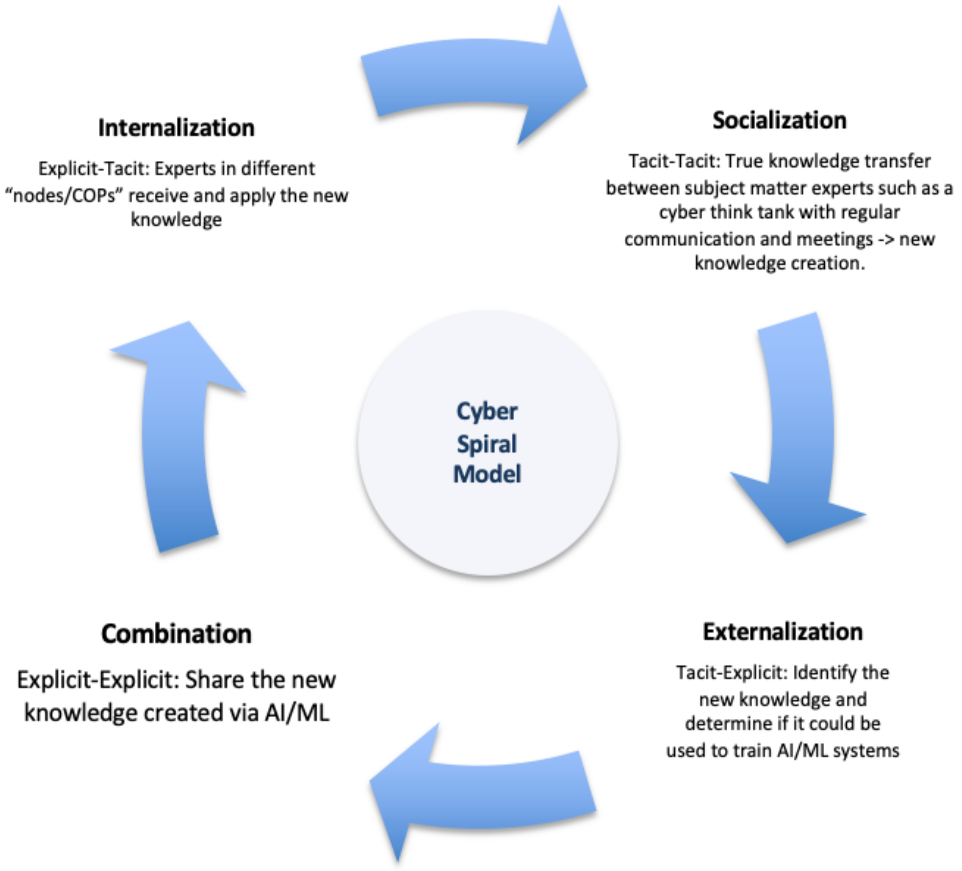


**Figure 1.** Cyber Spiral Model

The NIST Cybersecurity Framework 2.0 (2024) has been adopted internationally by public and private sector organizations to develop procedures to assess and mitigate cybersecurity risks (threats, vulnerabilities, and impacts). The current version of the NIST Cybersecurity Framework 2.0 was updated from Version 1.1 to 2.0 in 2024 which added Govern to the list of existing foundational Identify, Protect, Detect, Respond, and Recover functions to support the concept of

*DOI: https://doi.org/10.36965/OJAKM.2024.12(1)54-72*

*Accepting Editor: Meir Russ*

executive level strategy and management functions associated with the risks identified in the framework. The NIST Cybersecurity Framework 2.0 (2024)was selected for integration with the proposed Cyber Spiral Model based on its international acceptance and could also be applied to another cybersecurity framework. The integration of the NIST Cybersecurity Framework 2.0 (2024)and Cyber Spiral Model includes the following functions (See Figure 2):

1. Identify: Organizations identify the areas of greatest potential risk and vulnerability to cyber-attacks. In the Cyber Spiral Model socialization phase (tacit to tacit), SMEs can share their unique knowledge to identify new, emerging vulnerabilities. In the externalization phase (tacit to explicit), they can potentially automate processes for data mining or best practices related to their specific business, industry, and other critical factors. Similarly, in the "internalization" phase (explicit to tacit), SMEs can access continually evolving new knowledge related to cyber threats and continually adapt identification methods for increased agility. In addition, in the "combination" phase (explicit to explicit), automated AI and ML systems are continually learning and can alert organizations to new and emerging threats. The knowledge integration for the proposed Cyber Spiral Model is similar to the next four phases of the NIST Cybersecurity Framework 2.0 (2024).
2. Protect: An organization identifies methods to protect critical assets and potentially automate the process with a secure link to the Cyber Spiral Model and AI and ML systems.
3. Detect: The ability for experts to continually collaborate, develop, and share new knowledge to improve detection capabilities and provide AI and ML systems with the knowledge to learn should considerably improve these processes with new and evolving detection applications and methodologies. Again, agility increases as SMEs learn and adapt their detection systems relating to the "internalization" phase of the proposed Cyber Spiral Model.
4. Respond: The ability of organizations and governments to collaborate and develop contracts and treaties would enable more efficient and effective responses to cyber-attacks. Developing shared AI and ML, information sharing, and automated communication protocols would provide more efficient response capabilities. SMEs could use the "socialization" phase (tacit to tacit) for proactive knowledge sharing to improve response systems.
5. Recover: Integrating systems into the proposed Cyber Spiral Model would enable organizations to detect and respond to cyber-attacks more quickly to reduce and mitigate the severity of the attacks. Emerging AI and ML technologies, including GenAI, could also provide increased access to critical recovery data for SMEs and security systems.

*DOI: https://doi.org/10.36965/OJAKM.2024.12(1)54-72*

*Accepting Editor: Meir Russ*


**Figure 2.** NIST Cybersecurity Framework 2.0 (2024) Functions

The integration of the proposed Cyber Spiral Model with the NIST Cybersecurity Framework 2.0 (2024) serves as an example of the incorporation of specific phases of the knowledge spiral into the NIST Cybersecurity Framework 2.0 (2024), in theory, all phases of the spiral can be applied to the integrated model (See Figure 3). SMEs with different expertise can communicate using the newly created knowledge from the spiral to adapt to all phases of the NIST Cybersecurity Framework 2.0 (2024). Their new tacit knowledge can be entered into the system (externalization) to adapt identification, protection, detection, response, and recovery systems, which are shared in the combination phase and then easily made available in the internalization phase.

Emerging technologies discussed in the prior sections including AI and ML could be integrated into the proposed Cyber Spiral Model. The concept of a hybrid intelligent platform using these technologies integrated with expertise from cybersecurity experts would create the hybrid NIST Cyber Spiral Model. It would also be necessary to identify challenges to developing the conceptual hybrid model, including different platforms, protocols, trust, credibility/reputation, communication, ontologies, risks, and difficulties in codifying tacit knowledge.

*DOI: https://doi.org/10.36965/OJAKM.2024.12(1)54-72*

*Accepting Editor: Meir Russ*

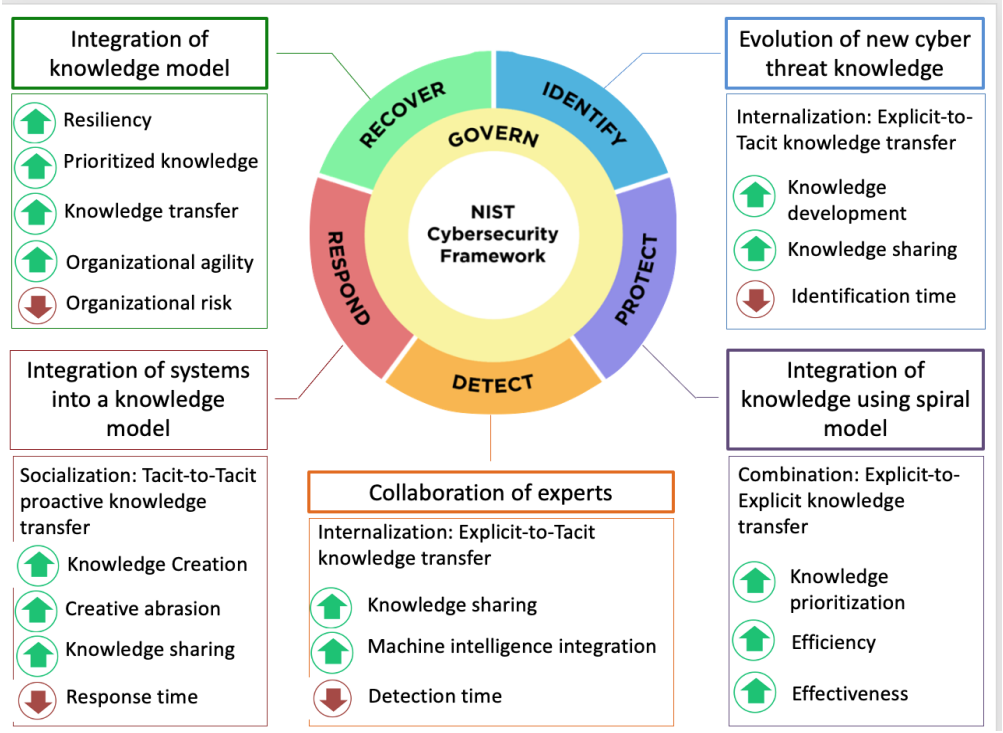


**Figure 3.** Proposed Model: Applying the Knowledge Spiral to the NIST Cybersecurity Framework 2.0 (2024)

## Discussion and Conclusions

The human knowledge creation (innovation) model for sustainable continual learning and competitive advantage demonstrates the ability to use knowledge for innovation (Jones & Mahon, 2018). However, transferring to an automated cyber-security model involves many more layers of complexity. The foundation for the new model lies in the concept of machine learning and other technology advances capable of analyzing data to identify patterns and make inferences to emulate human expertise, and decision-making, which can lead to the creation of new knowledge. However, the limitations identified to date involve the focus on analyzing data and information rather than knowledge. Knowledge gained from SMEs is nuanced and context-based and requires expertise to truly conceptualize the growing foundation of knowledge and contribute effectively to the knowledge base. Furthermore, if trusted SMEs collaborate in CoCs (communities of collaboration), they can create significant new knowledge or innovation via the synergies created by their diverse knowledge bases.

If AI and ML systems are developed proactively to search for unique knowledge about cyber-attack prevention, continually learning from these diverse sources of knowledge, and making them readily available to SMEs would result in a sustainable innovation in cybersecurity incident prevention. Combining the expertise of different cybersecurity professionals using CoCs (Communities of Collaboration) via "creative abrasion" for continual integration of new knowledge into the proposed hybrid model provides unique content for the ML and AI to increase

*DOI: https://doi.org/10.36965/OJAKM.2024.12(1)54-72*

*Accepting Editor: Meir Russ*

the sophistication and complexity of the cybersecurity protection systems and methods. In theory, with an increased level of cybersecurity sophistication, cyber adversaries would encounter an increased level of difficulty with reduced effectiveness. If we were to look at science fiction for inspiration, the "Borg" adversaries in Star Trek Next Generation were all linked into a giant hive where knowledge was seamless, and the collective was a giant never-ending accumulation of knowledge from the universe with different species added to the collective, aka "you will be assimilated, resistance is futile" (Bole, 1990). While this approach may be extreme, it represents a conceptualization of our theory.

The issues of structures and processes in the human model could potentially be analogous to developing ontologies, protocols, and compatible languages so technology-enabled systems can better communicate, collaborate, and learn from each other. The human model of performance cells and heterophilous building blocks of knowledge can be combined in many ways like Lego blocks and may be thought of as mini cybersecurity cells. Similarly, the "The Strength of Weak Ties" (Granovetter, 1973) and "Creative Abrasion" (Leonard-Barton, 1995) models suggest diverse knowledge, expertise, and perspectives are necessary conditions for a hybrid model to be effective. AI and ML systems can incorporate neural networks to combine these unique knowledge blocks in novel ways to create new knowledge and innovation for the development of advanced cybersecurity systems.

Finally, and perhaps the most challenging issue relates to trust. Governments and businesses have valuable proprietary knowledge and intellectual capital that represent a competitive advantage for organizations. Other knowledge involves government and military security to protect national interests. Therefore, the ability to segment information and knowledge into different databases using a zero-trust model to verify the validity and credibility of SMEs in the CoCs may be feasible to overcome some of these issues. In addition, leadership and culture can potentially contribute to the development of trust and collaboration among different businesses, government, and nonprofit organizations. We have seen the beginning of these collaborations as mentioned with the CISA development of AIS service that shares threat intelligence broadly across the public and private sectors. The development of advanced secure cyber knowledge blocks, compatible protocols, and ontologies could be enhanced with collaborative leadership principles based on trust and collaboration.

Focusing on knowledge rather than information could help machine learning incorporate context from ontologies with integration into the secure knowledge blocks. In addition, the secure knowledge blocks could greatly enhance the effectiveness of machine learning and the sophistication of detection mechanisms.

The proposed hybrid model is a unique approach with the incorporation of relevant knowledge management and cybersecurity models which represent a continual knowledge creation, sharing, and use model based on the classic knowledge spiral. It integrates technology elements into knowledge systems based on learning from SMEs with augmented knowledge and vast processing capabilities. Again, the proposed model focuses on true knowledge rather than data or information, which is unique among existing models and systems. The resulting trends and patterns continually enter the spiral and are accessible to SMEs who learn from sophisticated analysis where new knowledge from the continuous innovation, absorptive capacity, and creative abrasion of many

SMEs contribute to the system. The foundation of knowledge developed in a continual cycle represents new knowledge creation, transfer, and use to potentially increase the level of protection against cyber adversaries. The potential for the incorporation of the globally recognized and implemented NIST framework with the proposed Cyber Spiral Model introduces a hybrid knowledge model that may enhance the effectiveness of existing cybersecurity methods.

## Limitations

This paper is conceptual in nature, building upon models and theories from different literature streams, which are based on new, emerging information unavailable at the time of publication.

## Future Research

This paper represents a conceptual approach to emulating the human knowledge management model with technologies to reduce the threat of cybercrime. However, in reality, the complexity is greater than represented by the initial model. Therefore, future research should seek to confirm, refute, or modify the model to reflect additional and changing moderating variables and explore more specific applications and details of the models.

## References

Aghina, W., Ahlback, K., De Smet, A., Lackey, G., Lurie, M., Murarka, M., & Handscome, C. (2018). The five trademarks of agile organizations. McKinsey. https://www.mckinsey.com/capabilities/people-and-organizational-performance/our-insights/the-five-trademarks-of-agile-organizations

Alqahtani, A., Hawryszkiewycz, I., & Erfani, E. (2023). Relationship between knowledge creation and open innovation applied through public open innovation platforms. *Electronic Journal of Knowledge Management, 21*(1), 73-86.

Armenia, S., & Loia, F. (2022). Integrating big data analytics, systems thinking and viable systems approach towards a shift from individual to collective intelligence and collective knowledge systems. *puntOorg International Journal, 7*(1), 62-83.

Belsis, P., Kokolakis, S., & Kiountouzis, E. (2005). Information systems security from a knowledge management perspective. *Information Management & Computer Security, 13*(3), 189-202.

Bole, C. (Director). (1990, June 18). *Best of both worlds, part 1.* (Season 3, Episode 26) [TV series episode]. In M. Piller (Executive Producer), Star Trek: The Next Generation, Paramount Domestic Television.

Chang, K., & Huang, H. (2023). Exploring the management of multi-sectoral cybersecurity information-sharing networks. *Government Information Quarterly, 40*(4), 101870.

Coad, A., & Rao, R. (2008). Innovation and firm growth in high-tech sectors: A quantile regression approach. *Research Policy, 37*(4), 633-648.

Columbia University School of Engineering and Applied Science (2023). *Artificial intelligence (AI) vs. machine learning*. https://ai.engineering.columbia.edu/ai-vs-machine-learning/

David, D. P., Keupp, M. M., & Mermoud, A. (2020). Knowledge absorption for cyber-security: The role of human beliefs. *Computers in Human Behavior, 106*, 106255.

Davenport, T. (1994). Saving IT's soul: Human-centered information management. *Harvard Business Review, 72*(2), 119-131.

Federal Bureau of Investigation. (2023). *Internet crime report 2023.* https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

Fleck, A. (2024, February 22). Cybercrime expected to skyrocket in coming years. *Statista.* https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/

Gartner. (2024). Gartner survey reveals 63% of organizations worldwide have implemented a zero-trust strategy. https://www.gartner.com/en/newsroom/press-releases/2024-04-22-gartner-survey-reveals-63-percent-of-organizations-worldwide-have-implemented-a-zero-trust-strategy

Goldstein, E. (2023). JCDC focused on persistent collaboration and staying ahead of cyber risk in 2023. CISA. https://www.cisa.gov/news-events/news/jcdc-focused-persistent-collaboration-and-staying-ahead-cyber-risk-2023

Granovetter, M. S. (1973). The strength of weak ties. *American Journal of Sociology, 78*(6), 1360-1380.

Groysberg, B., Lee, J., Price, J., & Cheng, J. (2018). The leader's guide to corporate culture. *Harvard Business Review, 96*(1), 44-52.

Henderson, C., & Callahan, K. (2023). *Creating new knowledge about change by combining research-based knowledge with the wisdom of practice.* Accelerating Systemic Change Network (ASCN). https://ascnhighered.org/ASCN/posts/262536.html

Hill, L. (2024). How the best leaders drive innovation. https://hbr.org/podcast/2024/02/how-the-best-leaders-drive-innovation

Holste, J. S., & Fields, D. (2010). Trust and tacit knowledge sharing and use. *Journal of Knowledge Management, 14*(1), 128-140.

INTERPOL. (2020). Cybercrime collaboration services. https://www.interpol.int/en/content/download/15783/file/Cybercrime%20Collaboration%20Services-Factsheet.pdfhttps://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-Collaboration-Services

Jones, N. B., & Mahon, J. F. (2018). *Knowledge transfer and innovation.* Routledge.

Keshavarzi, M., & Ghaffary, H. R. (2023). An ontology-driven framework for knowledge representation of digital extortion attacks. *Computers in Human Behavior, 139*, 107520.

Koenig, M. (2018). *What is KM? Knowledge management explained.* https://www.kmworld.com/Articles/Editorial/What-Is/What-is-KM-Knowledge-Management-Explained-122649.aspx

Krenz, J. (2023). Boosting Microsoft's response to cybersecurity attacks with Microsoft Sentinel. https://www.microsoft.com/insidetrack/blog/boosting-microsofts-response-to-cybersecurity-attacks-with-microsoft-azure-sentinel/

Krishnan, R., Rainone, N., Silverman, Z., & Skerritt, D. (2023). *How to gain and sustain a competitive edge through transformation.* McKinsey Insights. https://www.mckinsey.com/capabilities/transformation/our-insights/how-to-gain-and-sustain-a-competitive-edge-through-transformation

Leonard-Barton, D. (1995). *Wellsprings of knowledge: Building and sustaining the sources of innovation.* Harvard Business School Press.

Microsoft Corporation. (2021). *Microsoft security zero-trust.* https://www.microsoft.com/en-us/security/business/zero-trust

Moustaghfir, K., & Schiuma, G. (2013). Knowledge, learning, and innovation: Research and perspectives. *Journal of Knowledge Management, 17*(4), 495-510.

Muncaster, P. (2023). *Cloud security alerts take six days to resolve.* Info Security Magazine. https://www.infosecurity-magazine.com/news/cloud-security-alerts-take-six/

Muppidi, S. (2023). *AI in cybersecurity: Yesterday's promise, today's reality.* https://www.technologyreview.com/2023/05/24/1073395/ai-in-cybersecurity-yesterdays-promise-todays-reality/

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. (National Institute of Standards and Technology, Gaithersburg, MD), Special Publication SP 800-181. https://doi.org/10.6028/NIST.SP.800-181

Nonaka, I. & Takeuchi, H. (1995). *The knowledge creating company*. Oxford University Press.

Nonaka, I., & Takeuchi, H. (2007). The knowledge-creating company. *Harvard Business Review, 85*(7/8), 162.

Noruzy, A., Dalfard, V. M., Azhdari, B., Nazari-Shirkouhi, S., & Rezazadeh, A. (2013). Relations between transformational leadership, organizational learning, knowledge management, organizational innovation, and organizational performance: an empirical investigation of manufacturing firms. *The International Journal of Advanced Manufacturing Technology, 64*, 1073-1085.

Papa, A., Dezi, L., Gregori, G. L., Mueller, J., & Miglietta, N. (2020). Improving innovation performance through knowledge acquisition: the moderating role of employee retention and human resource management practices. *Journal of Knowledge Management, 24*(3), 589-605.

Petersen, R. Santos, D., Wetzel, K., Smith, M., & Witte, G. (2020). National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. (National Institute of Standards and Technology, Gaithersburg, MD), Special Publication SP 800-181, Revision 1 November 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf

Sayan, C., Hariri, S., & Ball, G. L. (2019). Semantic knowledge architecture for cyber security. *Proceedings of the International Conference on Security and Management (SAM)* (pp. 69-76). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

Statistics Times. (2024). *Projected GDP ranking.* https://statisticstimes.com/economy/projected-world-gdp-ranking.php

The White House. (2024). *National cybersecurity strategy implementation plan.* https://www.whitehouse.gov/wp-content/uploads/2024/05/National-Cybersecurity-Strategy-Implementation-Plan-Version-2.pdf

Townsend, K. (2023). *Cyber insights 2023 quantum computing and the coming cryptopocalypse.* SecurityWeek. https://www.securityweek.com/cyber-insights-2023-quantum-computing-and-the-coming-cryptopocalypse/

Tuteja, A. (2022). *KPMG cyber trust insights 2022, Building trust through cybersecurity and privacy.* https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2022/10/kpmg-cyber-trust-insights-2022.pdf

U.S. Cybersecurity and Information Systems Information Sharing Analysis Center (2024). *Technical research and analysis services.* https://csiac.org/

U.S. Defense Advanced Research Project Agency (2023). *DARPA seeks a new gold standard in cybersecurity.* https://www.darpa.mil/news-events/2023-06-23

U.S. Executive Office of the President (2015, February 2, 2015). Executive Order 13691: FACT SHEET: Executive order promoting private sector cybersecurity information sharing. https://www.federalregister.gov/documents/2015/02/20/2015-03714/promoting-private-sector-cybersecurity-information-sharing

U.S. National Institute of Standards and Technology (2024, February 26). NIST Cybersecurity Framework Version 2.01.1. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

U.S. Office of the Director of National Intelligence (2024). 2024 Annual threat assessment of the U.S. Intelligence Community. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf

Velasquez, A. (2024). Guaranteeing AI robustness against deception (GARD). Defense Advanced Research Projects Agency (DARPA). https://www.darpa.mil/program/guaranteeing-ai-robustness-against-deception

Zorz, M. (2023). *Streamlining cybersecurity decision-making for analysts and CISOs.* Help Net Security. https://www.helpnetsecurity.com/2023/04/04/giorgos-georgopoulos-elemendar-cybersecurity-decision-making/

## Authors Biographies

**James Burrell, Ph.D.** is a Cyber and National Security Research Fellow at Boston College. He has served as a U.S. senior federal government executive, corporate c-level executive, and academic and research professional. He maintains academic appointments as a tenured professor and professorial lecturer at public and private universities and advisory affiliations with governmental, non-governmental, and private sector organizations.

**Nory Jones, Ph.D.** is a Professor of Business Information Systems at the University of Maine Business School. She earned her Ph.D. from the University of Missouri-Columbia with an emphasis on knowledge management. Her research and teaching focus on knowledge management, collaborative technologies, cybersecurity, innovation, e-business, and sustainable competitive advantage.

*DOI: https://doi.org/10.36965/OJAKM.2024.12(1)54-72*



*Accepting Editor: Meir Russ*