Moving Beyond Traditional Incident Response: Combating APTs with Warfare-Enabled Continuous Response

Abid Hussain Shah
CIS Department, University of Melbourne, Melbourne, Australia

***Abstract*—Critically examining the cybersecurity management practices, it can be concluded that security management used by the organizations is mostly control-centered against a wide range of threats to information systems. This control-centered approach has matured to act as a shield to prevent against a large variety of attacks. Since threats against the information systems are becoming sophisticated, persistent and evolving, therefore, the current approach has not been very effective against the advanced strategies and techniques used by the emerging threats like APTs (Advanced Persistent Threats). The core argument of this paper suggests that to match up the capabilities of APTs, organizations need a major shift in their strategies. This shift needs to focus more on the response oriented techniques relegating erstwhile prevention-centered approach. Traditionally the warfare strategies are more response oriented. Some of the non-kinetic strategies (not involving physical fighting) can be useful in developing response capability of Information Systems. Therefore, drawing on the warfare paradigm, and making use of DCT (Dynamic Capability Theory), this research examines the applicability of warfare strategies in the entrepreneur domain. This article will also contribute by means of a research framework arguing that the integration of prevailing information security capabilities; such as incident response capabilities and security capabilities from the warfare practices is possible resulting in dynamic capabilities (warfare-enabled). Such capabilities can improve security performance.**

Keywords*—*Information operations; information warfare; cyber security; dynamic capabilities; incident response capabilities; warfare enabled capabilities

I. Introduction

Within organizations, the most valuable assets are information systems and the infrastructures which require protection. Organizations are vulnerable against a variety of attacks which threaten to breach security mechanisms of the organizations to reach to the critical assets. Against this vast spectrum of attacks, information security approaches are traditional. Now a days, protecting the data against cyber-attacks has become a mounting challenge. Mostly the purpose of cyber-attacks remains financial gains [1]. Cyber-attacks can have many purposes may be military or political. Research conducted by Atif Ahmad and Richard Baskerville suggests that Organizations try to counter threats following strategies which are preventive in nature and are mostly control-centered [2], [3]. Such strategies have proved to be reasonably strong/successful against predicted or known attacks; nevertheless, the current traditional approach is being challenged by the increasingly complex and evolving threat environment. The emergence of highly sophisticated and potent cyber threat known as APT (Advanced Persis-tent Threats), challenges conventional information security paradigms in organizations. Baskerville [3] has strongly recommended new paradigms to follow; relegating the compromised prevention-oriented techniques for ensuring information systems' security. In this pursuit, learning from the Warfare Strategies mostly the non-kinetic strategies as well as incorporating theory of Dynamic Capabilities (DC), this article is looking at prospects of enhancing the corporate security performance, through the dynamic capabilities achieved as a result of integrating Warfare capabilities and conventional Incident Response capabilities.

The use of internet is on a constant and rapid increase and currently over 3 billion users world over use internet on daily basis (Tan et al., 2021). Many of the researches conducted in the domain of information security conclude that safeguarding the critical databases and ensuring the protection of information resources in the organizations has become complex, costly and time-consuming [4]–[6]. Scholars define information security threat as, an adverse event which sometimes may be in shape of a violation of policy or an unauthorized access [7]. Security threats are further categorized as Incidental threats, encompassing human errors, technical failures or forces of nature affecting security [7]. The second category of threats is critical and known as Purposive threats. The purposive threats look for deliberate and intentional breaches to a system's security, essentially driven by human efforts and intelligence [2], [7]. These are the 2nd category of threats the purposive threats; which are becoming increasingly challenging since mostly they are new, changing, exploring new vulnerabilities and are persistent in nature, well disciplined and are focused to achieve strategic goals/ objectives. Due to their peculiar characteristics of the purposive threats the security environment has become more vulnerable and increasingly uncertain [7] [8]. To address the growing challenges this article focuses to counter the real threats to information systems; the purposive threats.

As the technological advancements in the field of IT are super rapid, therefore, the security paradigm of information security is also changing quickly. The threats to information systems are becoming more silent and therefore, difficult to detect. Threats are also becoming complex and evolving so, we are facing more incidents and more frequently. The scenario suggests that enhancing the information security capabilities of the organizations is essentially required [3], [6], [7], [9]. Why

the APTs are succeeding? It can be safely concluded that the current response capabilities of the organizations are inadequate to match the superior capabilities of APTs (Shah et al. 2019). Contrary to Information Security strategies, the Warfare response strategies are inherently quicker in generating response therefore; they are more suited to ever changing threat landscape [3], [7], [10] [11][12]. In this article it is being proposed that for enhancing enterprise security (information systems security), a major shift of the security focus is needed. The suggestion is to focus and adopt the best practices of response domain of the warfare paradigm, which is largely response-oriented paradigm. Analyzing extant literature, it is revealed that there is hardly any literature available to answer the question of adopting warfare practices by the organizations to enhance their information security landscape.

Therefore, to enhance the security of the organizations especially in the response domain, this article is proposing a response framework which incorporates warfare response capabilities. Almost all organizations face the challenges of external and internal security threat to their Information systems; this article is better suited for those organizations which possess their exclusive Incident response Teams/setups. There are four sections in this paper. The theoretical framing has been explained in the next section. In the literature review section, the extant literature on security incident response has been explored extensively. Possibility of integration of the capabilities of Information Warfare and Incident Response capabilities has also been explored resulting in dynamic capabilities. Based on this discussion a conceptual frame-work of warfare-based security response has been introduced before concluding the paper. In the next section we will be discussing Dynamic Capabilities theory to understand its usage in developing dynamic cyber security capabilities in the ever-changing threat landscape.

II. Dynamic Capabilities (DC) Theory and Security Response

Considering the rapidly changing technological advancements, there has been substantial focus to make the organizational capabilities dynamic instead of static, therefore, the importance of Dynamic Capabilities (DC) cannot be ignored. The DC have been explained by many authors especially Teece. He proposes the DC approach as "an extension of the resource-based view (RBV)", which was an erstwhile concept [13]. Since the security threat environment is continuously changing while the RBV is static in its nature, hence it is unable to match up the ever changing threat spectrum, faced by information systems' security. [7] [14]. This mismatch was adequately addressed by Teece et al. [13] through introduction of concept of DC. Teece has explained the dynamic capability as the one which can combat the challenging environments and possesses the ability to develop, built also integrate and subsequently reconfigure the competencies whether internal or external [15]. Explaining the concept further, it has been recognized that through the DC, organizations can develop advanced resources and configuration following specific strategic routines [16] [17]. DC also contribute in achieving competitive advantage, by exploiting available opportunities, sometimes create opportunities and thus keep the firm well prepared to meet future and current challenges. This phenomenon is essentially sensing, seizing the available opportunities and keeping the firm competitive [15]. The DC approach also contributes in learning from incidents [7], [18]. It is also argued that the Incident Response can be managed by the organizations efficiently by developing DC [7], [19]. Therefore, it is essential that organizations adapt to the rapidly changing threat environments. It is also well recognized that better adaptation occurs by following an interdisciplinary approach [20]. Drawing from the Henry's conclusions; an inter-disciplinary approach, an integrative and dynamic capability development can be ensured which possesses more abilities and robustness for adapting to frequently changing environments. This approach can also avoid pensive and closed-minded views [7], [21] [22]. Since the warfare capabilities are response oriented and conventional Incident Response (IR) capabilities are prevention oriented, integration of both results in Dynamic Capabilities (DC) ensuring much better security against the looming threats. Thus, the overall enterprise security performance enhances many folds [7]. It has been argued in the paper that DC theory is appropriate and relevant for the research as in the information security domain organizations face threats which are complex and evolving swiftly. This phenomenon creates high levels of uncertainty which can be addressed though building dynamic capabilities. The section covers the detailed literature review with an objective to understand available and being practiced conventional Incident Response Capabilities. Subsequently, warfare relevant capabilities like operational security and deception have also been explored. Both these warfare capabilities are non-kinetic in nature and can be integrated with the traditional Incident Response capabilities, resulting in dynamic capabilities which have been named as Warfare Enabled Dynamic Response Capabilities (WEDRC).

III. Literature Review

To conduct a systematic literature review creating a firm foundation for advancing knowledge and to establish the need for answering the identified research question, literature review was conducted following the parameters explained by [23]. Latest as well as relevant publications (articles) published in renowned conferences and journals in the domains of Cyber Security, Information Operations (IO), Information Warfare (IW), Information Systems (IS), Information System Security, cyber and Information Management were consulted. For focused results and get the relevant hits research was done based on the phrases and key words like; 'Cyber security management', 'information security issues', 'information security superior strategy', information systems' security management', 'strategies dealing advanced persistent threats', 'information systems controls', 'warfare superior strategies', 'dynamic capabilities development', 'incident response for organizations' and 'information security risk management'. Initially 157 articles were selected besides 12 books and 10 field manuals from US military literature. The research focus was narrowed based on the contents of the articles and relegating not relevant to our research domain. Further relevancy was established keeping in view the intent and the focus of research question such as: How the enterprise security performance can be enhanced? How we can improve the

security response capability of information systems? And what all can be adopted from the warfare strategies for information systems' security enhancement? Thus the strength of articles was reduced to 66. Subsequently the for-ward and backward chaining process was carried out using the references of selected 66 articles; which resulted in an addition of 15, increasing the total to 81 articles, two books and 4 United States military field manuals on Information Warfare. With maturing the research process 13 articles initially included were deferred, bringing the total of articles to 68. Progressive and objective analysis gave birth to the proposed framework (Fig. 1). The results of the literature review suggest that the incident response capabilities are more focused on prevention of the incidents [7], [24], [25]. Therefore, they can address predicted or known threats only. Secondly the warfare capabilities have inbuilt response due to the nature of the warfare [5], [6]. Thirdly, DC theory provides sufficient helping tools in shape of sensing, seizing and transformation for efficient and dynamic incident response handling [19].

A. Conventional Incident Response (IR) Capabilities

Amongst the security threats to the information systems (IS), the purposive threats are more serious and damaging challenge to the security of organizations since they are very well organized, having mostly a well-orchestrated strategic objective, persistent in nature, and are ever evolving [7], [8]. The purposive threats always look for vulnerabilities in organizational de-fences. In the domain of information security, threats are combatted by application of controls, such as: (1) Formal (e.g. security policies, management of risk) (2) Informal (training), and (3) Technological controls (e.g. Fire walls, intrusion detection and protection systems, anti-viruses) [6], [7], [26]. Since the information systems; threats are usually handled by applying appropriate controls, this process of security management represents a control-centered approach [3], [7]. Since the Incident Response capabilities can be defined in many different ways, for this article DC theory perspective has been used. According to the well-known author Teece, the term 'capabilities' actually defines the role of firm's strategic management to adapt, integrating, and reconfigure organizational skillsets, resources, and acquired competences to deal with the changing environment and requirements" [13]. This has given lead to de-fine the Incident Response Capabilities: IR capabilities constitute all available controls (for-mal, informal and technical), practices and processes; to address security threats to IS while performing IR functions [7]. Literature also mentions about another perspective related to capabilities; people, processes and technologies for handling the security incidents [27].

Today's modern organizations are facing challenges to protect their information resources, and IT infrastructure. Literature also reveals that the current IS security response is essentially based on prevention strategy [7], [28]. The prevention-oriented approach has been quite successful for known threats. However, despite following the prevention oriented controls, in-formation security incidents are still happening reflecting failure of our defensive security mechanisms [7]. Large sized organizations, financial firms, banks and government organizations maintain exclusive incident response teams, however, maintaining exclusive IR teams becomes very expensive and does not remains cost-effective for smaller businesses and organizations [7]. Therefore to remain cost effective, most of the medium and small sized organizations maintain temporary IR teams. Also, the incident responders generally perform as 'fire-fighters' [5], [7].

B. Warfare Capabilities – Information Operations

While conceiving the leading plans in the warfare domain, multiple contingencies are hypothesized for that leading operational plan. This approach harnesses and harbors possibility of generating a robust response at the spur of the moment when and where required, harnessing and articulating the available resources in the given environment (e.g. an adversary's offensive movement). There are many warfare strategies which govern specific areas of the warfare. Amongst these multiple military strategies, few are non-kinetic like the Information Warfare (IW) which does not involve physical fighting and aims at protecting information and information systems, while disrupting those of the adversary [7], [12],[9]. The warfare paradigm is predominantly response oriented. Following the war fare principles pf employment like defense-in-depth, early warning Systems, maintain reserves at all tiers and extensive contingency planning; the defensive response and maneuvers can be well orchestrated against unknown offensive in unknown and fluent environments of the battlefield [7].

Literature concerning military sciences reveals that the IW is a non-kinetic war strategy; which has proved to be quite successful in protecting, exploiting, corrupting, denying or destroying information as well as information systems and infrastructure. Thus, it helps achieve competitive advantage over adversary [29],[9]. Since the IW deals with information and information systems (IS), therefore, its utility has been fairly established by many authors much beyond the warfare domain. As per the US military doctrine, success of IW comes through the integrated employment of Core, Supporting and Related capabilities (total 13 in number) which successfully affects the adversaries' decision makers, information and information systems. It also protects own information and information systems against adversary's such efforts resulting in influencing the decision making process [11], [12] [7]. An in-depth analysis of all the 13 capabilities of IW for their applicability for non-military organizations reveal that many of the capabilities are applicable in the corporate world however, for this article only two of the warfare capabilities namely; Operational Security (Opsec), and Deception are being considered [7].

- Operational Security (Opsec). It is Information Warfare strategy which is designed to meet operational needs. Successful application of Opsec assists in mitigating the risks related to the specific defensive vulnerabilities. This process is designed to shield critical information and observable indicators to the adversaries [7], [11]. Operational security can also be used for identification of the existing vulnerabilities in defensive/information systems of the adversaries, conducting risk assessment and planning/ application of appropriate protective measures [7]. To identify the looming threats like APTs,

the scope of Opsec can be extended in Information Security (IS) domain to carryout monitoring and attaining knowledge about the strategic objectives of threats. Another application of Opsec can be discerning about the phases of APTs thus denial of objectives of the intruders in each phase can also be planned [7].

- Deception. Deception is an old age warfare concept which has been frequently used in information security domain as well. It mostly consists of those activities, actions which deliberately mislead the adversary's decision making process and operations. In fact successful deception forces the adversaries to take specific actions or inactions which are well planned for own benefit. Thus, deception hides the facts from adversary and presents the false [11]. If the warfare capability of deception is employed in the in security mechanism, the response capability against the critical threats like APTs gets enhanced [30]. Concept of deception is already in use though, not with its deepest fruits and in depth understanding as a capability. Some of the examples of the concept being used in IS domain are honey pots, breadcrumbs, and personas etc. The purpose of deception as a capability (dynamic) is to incorporate response, developing understanding of the strategies, methods, practices and objectives of the APTs through taking the threats into safe and imitated environments [7] (Shah et al. 2019).

C. Warfare Enabled Dynamic Response Capabilities (WEDRC)

Dynamic Capabilities (DC) ensure that the firm remains competitive by continuously improving the methods, process and technologies as well as reviving the role components of the organization. The capabilities which are responsible for routine functionalities of the organizations are called ordinary capabilities while the higher level capabilities which keep the organizations competitive are known as dynamic capabilities which can at times change the ordinary capabilities as well [7], [31]. Many authors have discussed different aspects of dynamic capabilities, like the Teece [13] calls ordinary capabilities as; micro-foundations and dynamic capabilities as higher-order capabilities. His arguments suggest that by the phenomenon of sensing, seizing and transforming the micro foundation capabilities develop into higher order dynamic capabilities [7].

Similarly, in this article it has been argued that higher order dynamic capabilities can be developed through the integration of warfare capabilities (response oriented) with IR capabilities (prevention-oriented). Therefore, by adopting warfare strategies such as Opsec, we can identify different phases of APTs and can determine style, the strategic objectives of APTs in different phases. In corporate world this process is recognized as shaping and sensing process. Later on by applying deception eg breadcrumbs, tags and tripwires etc; the critical assets can be protected and strategies employed by intruders can be well known. When phases of APTs and objectives in each phase have been identified, combined application of deception and Opsec (e.g. kill chain) can deter APT disrupting the entire effort of the adversary. This is in fact a seizing process, through this process, the transformation of the capabilities to DC (Dynamic Capabilities; able to withstand the continuously changing threat environments) occurs [7]. In this paper the warfare enabled dynamic response capabilities (WEDRC) are the DC which were transformed by integrating warfare capabilities (deception, Opsec) and conventional Incident Response (IR) capabilities.

D. Enhanced Enterprise Security Performance

The enterprise security performance can be evaluated using many methods and factors; however, most of the scholars keep it in grey and invariably challenge the criterions for measuring security performance. One way to ascertain security performance of any organization may be related to the robustness or the effectiveness of the organization to counter internal and external frictions. In other words, it ensures the, confidentiality, integrity and availability of critical information [7], [19]. For this research article it has been argued that the enterprise security performance is the organizational acquiring which organizations can combat and respond to unknown threats including APTs.

IV. Proposed Research Framework

In the below framework (Fig. 1) it has been proposed that conventional Incident Response (IR) capabilities which are largely prevention oriented can be integrated with the relevant capabilities, practices from the warfare strategies, which are essentially response oriented.

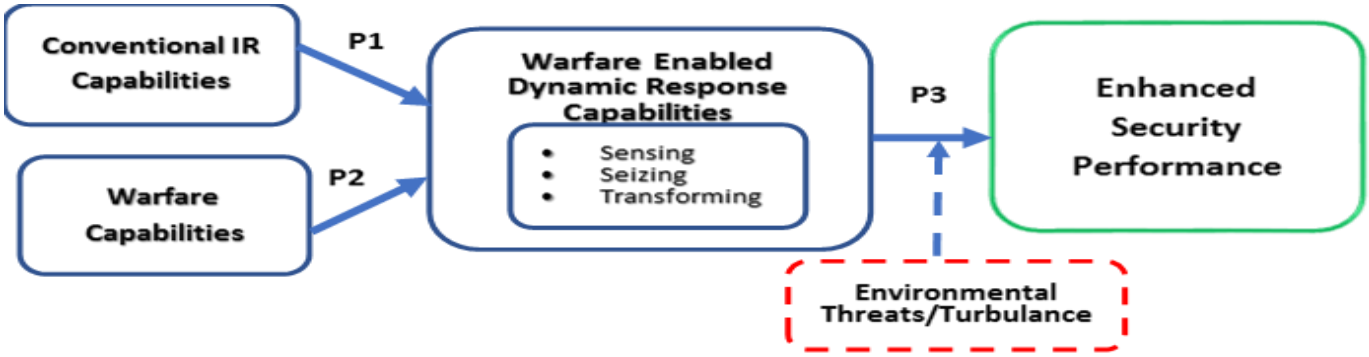

Fig. 1. Enterprise security performance enhancement framework (Developed for this article).

This integration results in warfare enabled dynamic response capabilities (WEDRC), which are higher level dynamic capabilities. This integration and consequently the development of DC can ensure enhancement of the overall security performance.

A. Contribution of IR Capabilities (Prevention Oriented)

Due to sufficient maturity of Information Systems' (IS) security practices, there has been a focus on developing standards, control and frameworks to identify the best practices, such as the ISO 27000 [7] (Shah et al., 2019). These standards assist in identification of threats to Information Systems (IS). Within IS security practices; the Incident Response activities, practices sense and eliminate IS security threats and incidents to information systems [32]. Most of the system attacks can be addressed through IR processes [33]. However, most of the organizations fail to focus on the learning process of IR, which is generally the last phase of IR, this aspect remains as a deficiency in the IR process. [7], [34]. Therefore, the controls are only able to respond to /appropriate for routine security tasks, ensuring prevention and the continuation of known or predicted threats. The conclusion therefore, is that IR capabilities are contributing positively in prevention of predicted (known) threats. Therefore:

P 1: Explains the extent of contribution of conventional IR capabilities to WEDRC in prevention domain.

B. Contribution of Warfare Capabilities (Response Oriented)

Since the current attacks faced by the IS are strategic in nature, persistent, sophisticated and evolving; therefore, the prevention-oriented approach seems failing against the APTs in the ever changing threat environments [3], [7]. Although a lot of work has already been done for development of more robust and improved controls, still the innovative, APTs succeed. The warfare security practices being more response oriented house dynamism [35]. Therefore, the relevant warfare capabilities, suitably developed into warfare enabled dynamic response capabilities (WEDRC) can amicably deal with unpredicted or unknown APTs. Therefore, it is proposed that:

P 2: Focuses on the contribution of Warfare relevant capabilities for WEDRC, in response domain.

C. Warfare Enabled Dynamic Response Capabilities (WEDRC)

Since the DC theory explains phenomenon of integration of dynamic capabilities through the process of the sensing, seizing, and transforming; therefore the birth of proposed Warfare enabled Dynamic capabilities is presumed to combat APTs much better than erstwhile traditional IR capabilities [7], [13]. Framework explains that the traditional IR capabilities can contribute positively to WEDRC (largely in the prevention domain), while the warfare relevant capabilities can assist in the response domain. It can also be concluded that the WEDRC can ensure better knowledge management as well as can obtain competitive advantage even under ever changing threat environment (Environmental Turbulence). Resultantly, the enterprise security performance is enhanced. Therefore, it is proposed:

P 3: Warfare enabled Dynamic Response Capabilities enhance enterprise security performance.

D. Key Findings

- Under the current environments the Incident Responders struggle to distinguish amongst the false positives considering the huge number of logs they need to face on daily basis. This phenomenon is impacting badly on the incident response process.
- One solution to go around huge false positives is automated decision making regarding which incident must be escalated and which should be ignored or treated differently. This could be done at SOC (Security Operation Center)
- Since Incident Responders are mostly those individuals who are performing other tasks and are collected on ad-hoc basis, therefore, use of IBM playbooks to follow the incident response steps remains useful.
- Since APTs have evolved to become more complex, persistent therefore, the better way to combat them is follow standards like IBM play books. However, since the APTs employ a military style approach, so, therefore, even by following the frameworks and established standards, there are likely chances that APTs will succeed. Adoption of military strategies like deception, and operational security assist in combating APTs in much better way
- Whenever the threats received escalate to the next level, the utility of teamwork becomes essential to go through the incident response phases in an organized manner.
- The deception strategy assists in developing mutated network, capable of not only preventing rather ensuring CIA (confidentiality, Integrity and Availability) of essential data. It also assists in tracking down the perpetrators.
- Through Warfare Enabled Dynamic Response Capabilities, Continuous response is possible.
- Through continuous response the process of early detection and identification of the likely threats is possible, and it assists many folds in the response process.

V. Conclusion

As the information security is largely prevention focused, so, mostly the APTs succeed revealing that the current prevention oriented security mechanism lacks behind APTs. Thus the call of the situation is to enhance response capabilities of the information systems security. Since the warfare domains employ hierarchical response practices to defeat the adversary at different tiers, adoption of warfare response-oriented techniques can enhance the response capabilities of organizations ensuring better cyber security.

As a future work we would like to carry out research of two more case study sites which use deception and operational security as one of their practices to develop deep insight about the continuous response phenomenon.

REFERENCES

[1] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," Energy Reports, vol. 7, pp. 8176–8186, 2021.

[2] J. Webb, A. Ahmad, S. B. Maynard, and G. Shanks, "A situation awareness model for information security risk management," Comput. Secur., vol. 44, pp. 1–15, 2014.

[3] R. Baskerville, P. Spagnoletti, and J. Kim, "Incident-centered information security: Managing a strategic balance between prevention and response," Inf. Manag., vol. 51, no. 1, pp. 138–151, Jan. 2014.

[4] R. E. Crossler, A. C. Johnston, P. B. Lowry, Q. Hu, M. Warkentin, and R. Baskerville, "Future directions for behavioral information security research," Comput. Secur., vol. 32, pp. 90–101, 2013.

[5] A. Ahmad, J. Hadgkiss, and A. B. Ruighaver, "Incident response teams - Challenges in supporting the organisational security function," Comput. Secur., vol. 31, no. 5, pp. 643–652, 2012.

[6] S. A. Slaughter David A, L. Levine, B. Ramesh, J. Pries-Heje, and R. Baskerville, "ALIGNING SOFTWARE PROCESSES WITH STRATEGY 1," 2006.

[7] A. H. Shah, A. Ahmad, S. B. Maynard and H. Naseer, "Enhancing Strategic Information Security Management in Organizatin_Own Paper ACIS_2019," ACIS 2019 Proc., no. 2019, pp. 448–455, Dec. 2019.

[8] A. Lemay, J. Calvet, F. Menet, and J. M. Fernandez, "Survey of publicly available reports on advanced persistent threat actors," Comput. Secur., vol. 72, pp. 26–59, 2018.

[9] D. E. Denning, "Quarter, 2011). The views expressed in this paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.," vol. 63, no. May, pp. 1–3, 2013.

[10] H. Naseer, G. Shanks, A. Ahmad, and S. Maynard, "Australasian Conference on Information Systems Enhancing Information Security Risk Management with Security Analytics: A Dynamic Capabilities Perspective."

[11] U. S. A. Doctrine, "FM 33-1," no. June, 1968.

[12] "Information Operations : Doctrine , Tactics , Techniques , and," vol. 13, no. November, 2003.

[13] D. J. Teece, G. Pisano, and A. Shuen, "Dynamic capabilities and strategic management," Knowl. Strateg., vol. 18, no. March, pp. 77–116, 2009.

[14] R. L. Priem, "A consumer perspective on value creation," Acad. Manag. Rev., vol. 32, no. 1, pp. 219–235, 2007.

[15] D. J. Teece and M. Augier, "Dynamic capabilities and multinational enterprise: Penrosean insights and omissions," Technol. Know-How, Organ. Capab. Strateg. Manag. Bus. Strateg. Enterp. Dev. Compet. Environ., vol. 47, no. June 2005, pp. 69–86, 2008.

[16] A. Pettigrew, H. Thomas, and R. Whittington, "Handbook of Strategy and Management," Handb. Strateg. Manag., 2012.

[17] I. Barreto, "Dynamic Capabilities: A review of past research and an agenda for the future," J. Manage., vol. 36, no. 1, pp. 256–280, 2010.

[18] B. Levitt and J. G. March, "ORGANIZATIONAL LEARNING," 1988.

[19] H. Naseer, "A Framework of Dynamic Cybersecurity Incident Response To Improve Incident Response Agility," 2018.

[20] H. F. L. Chung, Z. Yang, and P. H. Huang, "How does organizational learning matter in strategic business performance? The contingency role of guanxi networking," J. Bus. Res., vol. 68, no. 6, pp. 1216–1224, Jun. 2015.

[21] G. C. Kane and M. Alavi, "Information technology and organizational learning: An investigation of exploration and exploitation processes," Organ. Sci., vol. 18, no. 5, pp. 796–812, Sep. 2007.

[22] M. Dodgson, "Organizational Learning : Literatures What is," Sci. Policy Res. Unit, Univ. Sussex, Bright. U.K., pp. 375–394, 2014.

[23] J. Webster and R. T. Watson, "Analyzing the Past to Prepare for the Future: Writing a Literature Review.," MIS Q., vol. 26, no. 2, pp. xiii–xxiii, 2002.

[24] S. Ainslie, D. Thompson, S. Maynard, and A. Ahmad, "Cyber-threat intelligence for security decision-making: A review and research agenda for practice," Comput. Secur., vol. 132, Sep. 2023.

[25] R. Baskerville and B. Jissec, "Information Warfare: A Comparative Framework for Business Information Security Journal of Information System Security."

[26] M. E. Whitman and H. J. Mattord, "Principles of Information Security Fourth Edition," Learning, pp. 269, 289, 2011.

[27] R. Werlinger, K. Muldner, K. Hawkey, and K. Beznosov, "Preparation, detection, and analysis: The diagnostic work of IT security incident response," Inf. Manag. Comput. Secur., vol. 18, no. 1, pp. 26–42, 2010.

[28] A. Ahmad, S. B. Maynard, and G. Shanks, "A case analysis of information systems and security incident responses," Int. J. Inf. Manage., vol. 35, no. 6, pp. 717–723, Dec. 2015.

[29] M. Robinson, K. Jones, and H. Janicke, "Cyber warfare: Issues and challenges," Comput. Secur., vol. 49, pp. 70–94, 2015.

[30] G. L. Kovacich, "Protecting 21 st Century Information-It's Time for a Change," 2001.

[31] M. Schulz, P. Winter, and S. K. T. Choi, "On the relevance of reports-Integrating an automated archiving component into a business intelligence system," Int. J. Inf. Manage., vol. 35, no. 6, pp. 662–671, Aug. 2015.

[32] J. Wiik and J. J. Gonzalez, "Limits to Effectiveness in Computer Security Incident Response Teams," Proc. 23rd Int. Conf. Syst. Dyn. Soc., no. March 2016, pp. 152–153, 2005.

[33] P. Stephenson, "Conducting incident post mortems," Comput. Fraud Secur., vol. 2003, no. 4, pp. 16–19, 2003.

[34] A. Ahmad, J. Webb, K. C. Desouza, and J. Boorman, "Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack," Computers and Security, vol. 86. Elsevier Ltd, pp. 402–418, 01-Sep-2019.

[35] R. Baskerville, J. Pries-Heje, and S. Madsen, "Post-agility: What follows a decade of agility?," in Information and Software Technology, 2011, vol. 53, no. 5, pp. 543–555.