Building Cyber Warfare Capability: A Phased Approach to Integrating Cyber Operations into Military Structures

Mphahlela Thaba
Council for Scientific and Industrial Research (CSIR)

jthaba@csir.co.za

Jabu Mtsweni
Council for Scientific and Industrial Research (CSIR)/Stellenbosch University
mtswenij@gmail.com

Abstract

As the cyber domain increasingly becomes a critical battlefield, modern militaries must develop the capacity to conduct operations in and through the cyberspace. This paper presents a systematic approach to establishing cyber warfare capabilities within existing operational structures, offering a pathway for militaries to incrementally build and enhance their cyber capabilities. The approach emphasizes the integration of cyber warfare into traditional military operations, ensuring that new capabilities are developed in alignment with existing doctrines and structures. By proposing a phased methodology, the paper guides military organizations in creating appropriate command and control structures, training regimes, and technological frameworks to exploit cyberspace effectively. The focus is on developing a scalable and flexible cyber force that can adapt to evolving threats and leverage cyberspace for both defensive and offensive operations.

1 BACKGROUND

The cyber domain has emerged as a critical battleground in modern warfare. As nations become increasingly reliant on digital infrastructure, the potential for cyberattacks to disrupt critical systems, steal sensitive information, and undermine national security has grown exponentially. The Stuxnet worm, which targeted Iran's nuclear program in 2010, demonstrated the destructive capabilities of cyber weapons (Baezner and Robin, 2017; Horschig, 2020). Since then, cyber operations have been employed by both state and non-state actors, blurring the lines between traditional and cyber warfare. This evolution has necessitated the development of sophisticated cyber defense strategies and the integration of cyber capabilities into broader military doctrines (Ormrod and Turnbull, 2016).

The necessity for militaries to develop cyber warfare capabilities is increasingly urgent as cyberspace becomes a critical domain for both defense and offense. Cyber threats from state and non-state actors are growing in sophistication and frequency, targeting essential infrastructure, military networks, and national security assets (Sigholm, 2013; Małecka, 2024). Without robust cyber capabilities, militaries risk being outmaneuvered in this rapidly evolving domain, compromising national security and military effectiveness. Developing these capabilities ensures that militaries can protect their assets, deter adversaries, and maintain a strategic advantage in modern warfare.

Integrating cyber capabilities into existing military operational structures presents several challenges. Traditional military hierarchies and doctrines often struggle to accommodate the rapid pace of technological change inherent in cyber operations. Additionally, the integration of artificial intelligence (AI) into cyber warfare introduces complexities such as ensuring the reliability and ethical use of AI-driven systems in decision-making processes. These challenges necessitate a rethinking of command structures, training, and coordination across military and civilian agencies to maintain operational effectiveness.

This paper aims to provide a systematic approach for militaries to incrementally develop and integrate cyber warfare capabilities within their existing operational structures. By focusing on a phased methodology, the paper aims to guide military organizations in overcoming challenges related to traditional hierarchies and technological integration in cyber operations. The goal is to enable militaries to build scalable, flexible cyber forces that can effectively respond to and exploit the rapidly evolving cyber domain, ensuring they remain strategically prepared to address emerging cyber threats.

2 STATE OF THE ART

In this section, we provide related and existing research on cyber warfare and military functions integration. This

is then complemented by the analysis of current military strategies for cyber capability development. The gaps and challenges in existing approaches are also discussed.

2.1 Cyber warfare and military integration

The integration of cyber warfare capabilities into military strategies is an evolving field, with significant research focused on the strategic, operational, and doctrinal challenges it presents. Firdous (2020) offers a comprehensive analysis of how cyber commands and military cyber units are being established, emphasizing the critical implications for military doctrine and strategy. This research underscores the importance of cyber governance as a broader context for understanding the role of cyber warfare in military institutions.

Ormrod and Turnbull (2016) highlight the disparities in the conceptualization of cyber warfare across policy, military doctrine, and law. They propose a Cyber Conceptual Framework to foster a common understanding of cyberspace within a multinational military environment. This framework aims to bridge the gaps between different national doctrines and establish a coherent approach to cyber warfare, cyber conflict, and cyber-attacks.

Bellasio et al. (2018) acknowledge the dynamic and complex nature of the cyber environment, which complicates the development of clear and unambiguous concepts for cyber warfare. They emphasize the need for a coherent framework that links cyberspace with military operations, noting the challenges of integrating cyber capabilities with kinetic operations due to issues such as insufficient synchronization and coordination.

Pérez-Morón (2022) reflects growing concern among military strategists about the increasing role of cyber capabilities in modern warfare. This research highlights the lack of a coherently integrated doctrine that clearly defines and links the concepts of cyberspace, cyber warfare, and cyber-attacks. The transnational nature of the internet and its convergence with military operations necessitate a reevaluation of military doctrine to incorporate these cyber capabilities effectively.

Similarly, Caton (2019), Smeets (2018), and Hemanidhi and Chimmanee (2017) explore the global efforts to integrate cyber capabilities into military doctrine. They underscore the complexities of cyberspace, which make it challenging to develop clear concepts for cyber warfare. These studies call for a robust and coherent framework that connects cyberspace with traditional military operations, emphasizing the importance of secure communications and the integration of cyber systems into the operational environment.

Ormrod and Turnbull (2016) also point out the need for strategic research on the implications of cyber warfare for national security, international relations, and the balance of power. They discuss the operationalization of cyber capabilities in military campaigns, the coordination between cyber and kinetic forces, and the legal and ethical frameworks surrounding cyber warfare. This body of research underscores the necessity of a comprehensive approach to integrating cyber capabilities into military strategies and operations.

2.2 Military strategies for cyber war capability development

The existing literature on military strategies for cyber capability development reveals a broad trend towards integrating cyber operations into multi-domain warfare, with the United States often leading the charge. Firdous (2020) compares the cyber strategies of the US (United States), China, India, and Pakistan, highlighting their policy documents, cyber units, and the execution of cyber-attacks as critical components of their military strategies. This comparative analysis emphasizes the growing significance of cyber capabilities in regional and global military contexts.
Ormrod and Turnbull (2016) examine the harmonization of cyber doctrines across various countries, aiming to establish a coherent framework for cyber warfare, conflict, and attacks. They highlight the need for a unified conceptual approach to cyber capability development. Similarly, Bellasio et al. (2018) note that major military powers like the US, UK, and Germany are integrating offensive cyber capabilities into multi-domain operations. Their strategies include the creation of military cyber commands, organizational restructuring, and doctrinal adaptations to incorporate cyber operations.

Pérez-Morón (2022) and other scholars such as Caton (2019), Smeets (2018), and Hemanidhi and Chimmanee (2017) all emphasize the focus on integrating cyber capabilities into multi-domain operations, with the United States recognized as a leader in this domain. These countries are not only developing advanced offensive cyber capabilities but are also establishing military cyber commands and refining organizational and doctrinal frameworks to accommodate the unique demands of cyber warfare.

Ormrod and Turnbull (2016) also identify common themes across national military strategies, including significant investment in Research and Development

(R&D), talent acquisition and training, the establishment of dedicated cyber command structures, and international cooperation for cyber defense and information sharing (Scharre and Riikonen (2020); Matania, Yoffe and Goldstein (2017); Skopik, Settanni and Fiedler (2016)). These efforts underscore the global recognition of cyberspace as a critical domain in modern military operations.

2.3 GAP ANALYSIS IN TRADITIONAL IMPLEMENTATION APPROACHES

The literature on cyber warfare and military integration reveals several significant gaps and challenges in current approaches. Firdous (2022) identifies a lack of international consensus on cyberspace governance, with divergent views on cyber sovereignty versus an open internet. This indicates a pressing need for a systematic approach to cyber governance that balances these differing perspectives. Additionally, Firdous highlights that while major powers are enhancing their cyber capabilities, a phased methodology is necessary to prevent unintended escalation and promote responsible behavior in cyberspace.

Ormrod and Turnbull (2016) critique the absence of a unified global doctrine that links cyberspace, cyber-warfare, cyber-conflict, and cyber-attacks. They also emphasize the lack of first-order principles and a comprehensive understanding of the inherently international nature of cyberspace security. Similarly, Bellasio et al. (2018) point out operational challenges in integrating cyber capabilities with conventional warfighting, stressing the need for a systematic and phased approach to guide this integration. This approach would ensure that cyber capabilities are developed coherently, comprehensively, and in alignment with military strategic objectives.

Pérez-Morón (2022) also identifies significant gaps, including the absence of a single narrative in global doctrine that integrates cyberspace with traditional warfare concepts. This study highlights challenges in synchronizing cyber operations with kinetic operations and establishing clear concepts for cyber warfare. The need for a systematic and phased methodology to guide the integration of cyber capabilities into military doctrine and operations is emphasized, proposing a framework that articulates fundamental principles, supports a common lexicon, and fosters the development of doctrine relevant to future conflicts.

Caton (2019) and Smeets (2018) echo these concerns, pointing out the lack of a coherent global doctrine and the difficulties in integrating cyber operations with traditional military activities. They, too, call for a systematic and phased approach to develop a comprehensive framework for cyber capabilities.

Ormrod and Turnbull (2016) further insist on addressing several persistent challenges, including the integration of cyber capabilities with traditional warfare, ensuring interoperability among military branches and international partners, and adapting to rapidly evolving cyber threats. They stress the importance of comprehensive planning, clear policy, and doctrine to guide cyber operations and address legal and ethical issues (Ablon et al. (2019); Bigelow (2019); Baylon (2014); Burton (2015); Steingartner, Galinec and Kozina (2021); Formosa, Wilson and Richards (2021); Novitzká, Korečko and Szakál (2017)).

2.4 CHALLENGES IN INTEGRATING CYBER WAR CAPABILITIES

Aligning cyber warfare with traditional military doctrines is a complex endeavor that presents several challenges due to the unique characteristics of cyberspace and the rapid evolution of technology. Some of these challenges are that the cyberspace is a dynamic, borderless digital domain where traditional military concepts are difficult to apply.

The anonymous nature of cyberattacks complicates attribution and the application of international law. The speed and scale of cyber operations necessitate rapid adaptation of military doctrines. A wide range of actors, from nation-states to individuals, can develop cyber capabilities, creating an asymmetric battlefield.

The legal and ethical implications of cyber warfare are complex. Integrating cyber operations with traditional military forces requires new approaches to interoperability, command and control, and personnel training. Continuous adaptation to technological advancements is essential for maintaining effective military operations in cyberspace (Ormrod and Turnbull, 2016).

2.4.1 Doctrine

To effectively align cyber warfare with traditional military doctrines, a comprehensive approach is necessary one that addresses the unique dynamics of cyberspace, the rapidly evolving nature of technology, and the need for continuous adaptation. This process requires not only technical integration but also the harmonization of strategic thinking, legal frameworks, and operational

procedures. Given the complexity involved, a systematic and phased approach is crucial for successfully developing and embedding cyber capabilities within military doctrines.

2.4.2 Organisational and Structural

Significant challenges arise from organizational and structural barriers within existing military frameworks, which can impede the effective integration of cyber warfare capabilities. These barriers may obstruct the adaptation of military doctrines, the efficient allocation of resources, and the coordination of cyber operations with conventional military activities (Pérez-Morón, 2022).

2.4.3 Command and Control Structures

The establishment of robust cyber command and control structures is fraught with technological challenges, particularly due to the fast-paced evolution of cyber threats and the intricate nature of cyber environments (Pérez-Morón, 2022). Achieving real-time situational awareness necessitates advanced monitoring tools and integrated systems capable of processing vast amounts of data from diverse sources (Franke and Brynielsson, 2014). Moreover, maintaining secure and resilient communication channels is paramount, as cyber adversaries continually devise new methods to disrupt or exploit these channels.

The integration of cyber capabilities into existing military frameworks demands sophisticated coordination across multiple platforms and technologies, complicating the establishment of effective command and control structures (Ormrod and Turnbull, 2016).

2.4.4 Training and Human Resource development

Additionally, training and human resource development present considerable challenges in the integration of cyber capabilities. The rapid technological advancements and the complexity of cyber operations require the development of a highly skilled workforce, necessitating continuous education and hands-on experience with the latest tools and threats. Cyber personnel must not only master technical skills but also stay agile in the face of emerging cyber threats and tactics. Aligning training programs with evolving military and organizational needs is essential but often resource intensive. Ensuring that personnel are prepared to operate effectively within integrated cyber frameworks while maintaining readiness and expertise remains an ongoing challenge in the development of robust cyber capabilities.

3 CYBER WARFARE CAPABILITY FRAMEWORK

In the research work by the authors Thaba and Mtsweni (2023), a comprehensive cyber warfare capability framework was proposed and developed, which suggests that for militaries to establish, deploy and sustain their cyber warfare capabilities, the main goals in the cyberspace should be about defending territorial integrity and sovereignty. The military also needs to ensure that there are continuous improvements, through RD&I, concept development and experimentation in building, executing, and sustaining the cyber warfare capability. This capability is seen in two lenses: *(1) securing the cyber space (i.e., taking a security and protection approach)*, and *(2) exploiting the cyberspace to gain territorial and sovereignty advantage through offensive means*.

To implement the framework a maturity model was suggested to assess the different stages of cyber warfare capability within the military operations. The framework and the maturity model as proposed are the basis for the proposed phased methodology as discussed in the next section.

4 PROPOSED PHASED METHODOLOGY

A phased approach to cyber capability development is essential for militaries to systematically build and enhance their cyber defense and offensive capabilities (Ertan et al., 2020). This method allows for incremental progress, starting with establishing foundational infrastructure and advancing through integration and optimization stages. By breaking down the development process, militaries can address specific challenges, such as evolving cyber threats and technological integration, in manageable phases. This approach also facilitates the continuous assessment and adaptation of strategies, ensuring that capabilities remain relevant and effective.

A phased strategy ensures that resources are allocated efficiently, and that each development stage builds upon the previous one, leading to a comprehensive and robust cyber defense posture.

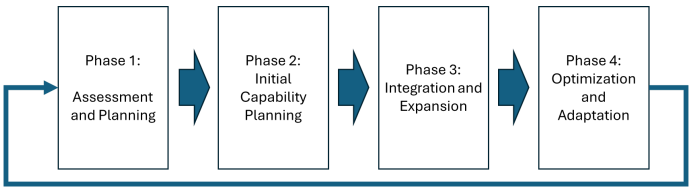

Figure 1: Cyberwarfare capability integration approach

The phased approach to cyber capability development begins with evaluating current capabilities, identifying gaps, and conducting strategic planning to prepare for

phased integration (Phase 1), as depicted in Figure 1 above. This is followed by establishing basic command and control structures and initial cyber defense and offense capabilities (Phase 2). Next, cyber capabilities are integrated into broader military operations, with an expansion of training programs and technological infrastructure (Phase 3).

The final phase focuses on continuous improvement in response to evolving threats, as well as enhancing interagency collaboration and international cooperation (Phase 4).

5 REFERENCE CASE STUDY

In this section, selected case studies highlight successful integrations of cyber warfare, providing lessons learned, while strategic insights emphasize the need for ongoing adaptation, policy changes, and flexibility in cyber warfare strategies.

The United States, United Kingdom, Israel, China, Russia, and Australia have all advanced their integration of cyber capabilities into military and national security frameworks, though each has unique approaches. This suggests that the developed nations are already ion phase 4 of the methodological approach. Common across these nations is the establishment of dedicated cyber command units and investments in specialized infrastructure and training.

The UK's National Cyber Force (NCF) and Israel's IDF Unit 8200 are examples of integrating cyber operations into broader military strategies, showing that Phase 1 and Phase 2 are critical. China's Strategic Support Force (SSF) centralizes cyber, electronic warfare, and space capabilities, while Russia's approach melds cyber operations with traditional military tactics, focusing on information warfare and espionage, demonstrating integration and expansion (Phase 3).

Australia has reinforced its defense with the Australian Signals Directorate (ASD) and the Australian Cyber Security Centre (ACSC). Notably, the US leads in developing comprehensive cyber warfare strategies and capabilities, setting a global benchmark in both offensive and defensive cyber operations.

In Africa, South Africa, Nigeria, Egypt, Kenya, and Morocco are progressively integrating cyber capabilities into their national security and defense strategies, albeit with slow progress. Common among these countries is the development of comprehensive cybersecurity frameworks (Phase 1 – Phase 2) and dedicated bodies to coordinate cyber efforts, such as South Africa's National Cybersecurity Policy Framework and Nigeria's Office of the National Security Adviser (Phase 3).

All these nations are focusing on enhancing their cyber defense infrastructure, with a growing recognition of the need for military integration (Phase 3). South Africa and Nigeria are in the early stages of embedding cyber capabilities into their military operations, while Egypt and Morocco are developing their cyber defense strategies (Maleh and Youness, 2022; Moustafa et al., 2022) with an eye toward regional and international collaboration.

Kenya stands out with its establishment of the National Kenya Computer Incident Response Team – Coordination Centre (KE-CIRT/CC) to manage cyber threats (Bada *et al.*, 2014). Despite ongoing development, these efforts underscore a regional shift towards robust cybersecurity practices.

6 CONCLUSION

This paper has presented a comprehensive approach for the integration of cyber warfare capabilities into military structures, advocating for a phased approach that is both systematic and strategic. The proposed methodology begins with an assessment of current capabilities, followed by the establishment of foundational cyber structures, the integration of these capabilities into broader military operations, and finally, the continuous refinement and enhancement of these capabilities in response to evolving threats.

This approach allows for the incremental development of cyber capabilities, ensuring that each phase builds upon the successes of the previous one. This methodical progression mitigates the risks associated with rapid, uncoordinated expansion and ensures that the evolving cyber force remains aligned with the military's strategic objectives. Furthermore, it fosters a culture of adaptability and innovation within military organizations, which is essential in the face of the rapidly changing cyber landscape.

The integration of cyber warfare capabilities into military operations is not merely an option but a necessity. The proposed phased approach provides a roadmap for militaries to navigate this complex and ever-evolving landscape, ensuring they are equipped to meet the challenges of cyber warfare with resilience, agility, and strategic foresight. As the world becomes more interconnected and reliant on digital infrastructure, the

imperative to develop robust cyber capabilities becomes more urgent. With a disciplined and phased approach, militaries can rise to this challenge, securing their nations' interests in the digital age.

References

[1] Ablon, L., Binnendijk, A., Hodgson, Q. E., Lilly, B., Romanosky, S., Senty, D., & Thompson Rand, J. A. (2019). RAND Corporation Operationalizing Cyberspace as a Military Domain: Lessons for NATO. In Corporation.

[2] Bada, M., Creese, S., Goldsmith, M., Mitchell, C., & Phillips, E. (2014). Computer Security Incident Response Teams (CSIRTs) An Overview. https://ssrn.com/abstract=3659974

[3] Baezner, M. ;, & Robin, P. (2017). ETH Library Stuxnet Report. https://doi.org/10.3929/ethz-b-000200661

[4] Baylon, C. (2014). Challenges at the Intersection of Cyber Security and Space Security Country and International Institution Perspectives.

[5] Bellasio, J., Flint, R., Ryan, N., Søndergaard, S., Gonzalez Monsalve, C., Sofia Meranto, A., & Knack, A. (2018). Developing Cybersecurity Capacity: A proof-of-concept implementation guide. www.rand.org/giving/contribute

[6] Bigelow, B. (2019). What are Military Cyberspace Operations Other Than War? 2019 11th International Conference on Cyber Conflict: Silent Battle.

[7] Burton, J. (2015). NATO's cyber defence: strategic challenges and institutional adaptation. Defence Studies, 15(4), 297–319. https://doi.org/10.1080/14702436.2015.1108108

[8] Caton, J. L. (2019). Implications of Service Cyberspace Component Commands for Army Cyberspace Operations. https://press.armywarcollege.edu/monographs

[9] Ertan, Amy., Floyd, K. H. ., Pernik, Piret., & Stevens, Tim. (2020). Cyber threats and NATO 2030 : horizon scanning and analysis. CCDCOE.

[10] Firdous, A. (2020). Cyber Warfare and Global Power Politics. In Afeera Firdous CISS Insight: Vol. VIII (Issue 1).

[11] Firdous, A. (2022). Cyber Warfare and Global Power Politics. Cyber Warfare and Global Politics, VIII(1).

[12] Formosa, P., Wilson, M., & Richards, D. (2021). A principlist framework for cybersecurity ethics. Computers and Security, 109. https://doi.org/10.1016/j.cose.2021.102382

[13] Franke, U., & Brynielsson, J. (2014). Cyber situational awareness - A systematic review of the literature. In Computers and Security (Vol. 46, pp. 18–31). Elsevier Ltd. https://doi.org/10.1016/j.cose.2014.06.008

[14] Hemanidhi, A., & Chimmanee, S. (2017). MILITARY-BASED CYBER RISK ASSESSMENT FRAMEWORK FOR SUPPORTING CYBER WARFARE IN THAILAND. In Journal of ICT (Vol. 16, Issue 2).

[15] Horschig, D. (2020). Cyber-weapons in nuclear counter-proliferation. Defense and Security Analysis, 352–371. https://doi.org/10.1080/14751798.2020.1790811

[16] Małecka, A. (2024). Non-State Actors in Nation-State Cyber Operations. Rocznik Bezpieczeństwa Międzynarodowego 2024, 18(1). https://doi.org/10.34862/rbm.2024.1.4

[17] Maleh, Y., & Youness, M. (2022). Faculty of Graduate Studies for Statistical Research. Springer.

[18] Matania, E., Yoffe, L., & Goldstein, T. (2017). Structuring the national cyber defence: in evolution towards a Central Cyber Authority. Journal of Cyber Policy, 2(1), 16–25. https://doi.org/10.1080/23738871.2017.1299193

[19] Moustafa, M., El-Hamid, A., Naguib, M., Fattah, A.-E., & Wael El-Gendy, A. (2022). Crisis of Non-Traditional Warfare and its impact on Egyptian National Security within the New [Thesis]. Cairo University.

[20] Novitzká, Valerie., Korečko, S., & Szakál, A. (2017, November 14). Combining Cybersecurity and Cyber Defense to achieve Cyber Resilience. 2012017 IEEE 14th International Scientific Conference on Informatics .

[21] Ormrod, D., & Turnbull, B. (2016). The cyber conceptual framework for developing military doctrine. Defence Studies, 16(3), 270–298. https://doi.org/10.1080/14702436.2016.1187568

[22] Pérez-Morón, J. (2022). Eleven years of cyberattacks on Chinese supply chains in an era of cyber warfare, a review and future research agenda. Journal of Asia Business Studies, 16(2), 371–395. https://doi.org/10.1108/JABS-11-2020-0444

[23] Scharre, P., & Riikonen, A. (2020). Defense Technology Strategy.

[24] Sigholm, J. (2013). Non-State Actors in Cyberspace Operations. Journal of Military Studies, 4(1), 1–37. https://doi.org/10.1515/jms-2016-0184

[25] Skopik, F., Settanni, G., & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. Computers and Security, 60, 154–176. https://doi.org/10.1016/j.cose.2016.04.003

[26] Smeets, M. (2018). Integrating offensive cyber capabilities: meaning, dilemmas, and assessment. Defence Studies, 18(4), 395–410. https://doi.org/10.1080/14702436.2018.1508349

[27] Steingartner, W., Galinec, D., & Kozina, A. (2021). Threat defense: Cyber deception approach and education for resilience in hybrid threats model.

Symmetry, 13(4). https://doi.org/10.3390/sym13040597