A Strategic Path for Digital Transformation in Cyber Warfare for African Militaries

Mphahlela Thaba[1] and Jabu Mtsweni[1,2]
[1]Council for Scientific and Industrial Research, Pretoria, South Africa
[2]Stellenbosch University, Security Institute for Governance and Leadership in Africa, Faculty of Military Science, Saldanha, South Africa

jthaba@csir.co.za
mtswenij@gmail.com

Abstract: Digital disruption has changed the battlefield and increased its complexity for the war fighter. The modern battlefield continues to increase this complexity, due to the evolution of components that constitute military capability. The technologies, processes and the users are such components. The modern battlefield relies on advanced technologies tapping on high connectivity, are more lethal, precise, and autonomous. Due to this evolution, areas once thought to be safe from conventional attacks are increasingly becoming vulnerable. This evolution of technology and shorter development curves have also increased the prominence of the cyberspace, as a domain of war. However, many militaries, especially in Africa are still operating legacy systems and struggling with modernizing their systems to take advantage of the digital evolution. This paper, therefore, uses a systematic literature review and benchmarking focusing on selected super cyber power nations' indices to propose a strategic path for African militaries to drive digital transformation in their operational environments. The roadmap is proposed to stimulate the establishment and enhancement of African militaries' cyber warfighting capabilities in the digital age. The objectives of this digital transformation path include establishing a digital backbone, where all the sensors, effectors and the deciders are plugged to share information and intelligence.

Keywords: Digital transformation, Cyber warfare, Cyber operations, Cyber defence, Cyber attacks, Africa battlespace

1. Introduction

Tom Abke argues that the development of the first computers in the 1950's was also beneficial in military operations, in applications such as code-breaking, and logistics (Abke, 2022). He further states that towards the end of the 1980s, beginning of the 1990s, militaries began to adopt more advanced digital technologies, such as Global Positioning System (GPS) and military satellites. These developments significantly improved navigation and intelligence gathering in military operations (Abke, 2022).

Consequently, in the early 1990's many militaries were involved in what was then believed to be an information war, using integrated technologies that gave access to information for the war fighter (Dombrowski & Ross, 2008). It is also during this period that many nations were looking at making their militaries more lethal, and survivable, which included ways of decreasing boots on the ground. The era succeeding this, to the current digital battlefield, has also seen an increase in the use of modern technologies, which are highly connected, advanced, lethal, and intelligent.

The prominence of unmanned vehicle systems, and their evolution into autonomy has made the battlespace even more complex. Today's wars are fought amongst communities, the technologies required for war are dependent on systems that communities require for their livelihoods, and vice versa. This also makes it difficult to determine the boundaries of war, and more exacerbated by the prominence of cyberspace as a domain of war. Many militaries are therefore leveraging the capabilities of the latest technologies, to optimize skills and techniques of the soldiers (Billinga, et al., 2021).

Nevertheless, research reports suggest that African militaries are lagging in digitally transforming their capabilities to be effectively prepared for the modern battlefield in the cyberspace. Therefore, the main objective in this research paper is to investigate the digital transformation journeys of military superpowers to dominate cyberspace. This is done to develop a strategic path that African militaries could adopt in digitizing their capabilities in a systematic manner.

The rest of this paper is structured as follows: Section 2, provides background literature on the modern battlespace, demonstrating how digital transformation is giving dominance to the cyberspace, and the African battlespace is also discussed. In Section 3, the research approach for this study is presented as well as limitations. The concept of digital transformation is presented in Section 4. The benchmarking results based on selected superpowers are presented in Section 5. The main contribution of this paper is presented in Section 6 providing a strategic roadmap for African militaries to digitally transform their capabilities as well as the workforce for cyber warfare. The paper is concluded with recommendations in Section 7.

2. The Modern Battlespace

The future battlespace will be dominated by the evolution related to technologies, the advancing soldier, and the agile doctrine guided by these changes. As we advance towards the fifth industrial revolution, military operations will be dominated by even more advanced weapon systems, which are vastly connected and able to share data and intelligence, leading to better situational awareness. As these weapon systems improve, their sustainability on the battlefield also improves, with new energy sources being developed for them, and their ability to seamlessly relief each other or support in battle.

Figure 1 illustrates the connectivity of the modern battlespace, giving dominance to the cyberspace.

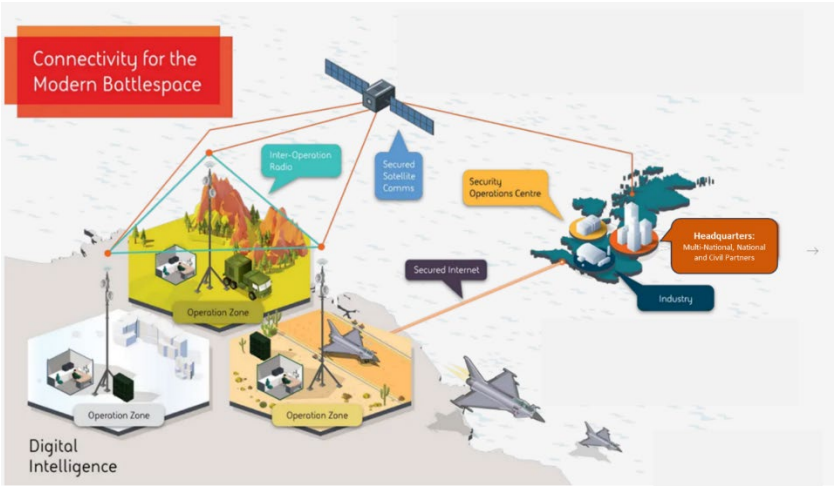

Figure 1: Connectivity of the Modern Battlespace (Adapted)[1]

The evolving technology necessitates changes in how militaries approach warfare. This phenomenon is already manifesting itself in the recent wars, including Russia – Ukraine conflict, where it has been reported that the Wagner group was engaged in the conflict using advanced digital tools (Williamson, 2009). The same has been reported on the African Continent, including alleged involvement of these type of groups in the Mozambique conflict. Global and regional powers also recognize the fact that no one nation will be able to fight the modern battlefield on their own, and many strategize around coalitions, and alliances. The increasing expansion of terrorist and insurgent groups across the world will remain a challenge in the future battlespace because of unrestricted access to digital technologies.

The availability of technologies, infiltrated globally, makes the pace of military offensive fast, and leaves little room for those attacked to respond. Adding to these challenges is cyberspace, which integrates all domains, and is borderless (McGuffin & Mitchell, 2014). Warfare in this domain will continue to be complex and will require militaries to have a complete shift of paradigm in how to plan and develop capabilities for this domain. Battlespace is at a point of no return, where technologies are relied upon for effective and efficient operations (Correia, 2019).

2.1 The African Battlespace

The days of only advanced nations having access to advanced technologies are over. Multinational companies, renowned for developing innovative military technologies, are rapidly increasing their footprint in Africa. Many African militaries accept that to remain ready and capable of fulfilling their mandates, they will have to evolve with the operational environment. The same remain with the increasing terrorists and insurgent groups on the African continent, with links to the base groupings in countries in the middle east and Europe.

The evolution of technology even in the African battlespace, implies the prominence of the cyberspace, and calls for African militaries to plane and develop capabilities that will exploit this complex domain. Whether it is through technology such as intelligent planning tools, digital twins, virtual and augmented reality, or combating threats in new domains, the dividing line between the cyber and the physical world is beginning to blur.

[1] https://www.baesystems.com/en/digital/blog/introducing-trinity-the-future-of-connectivity-for-the-modern-battlespace#

The African cyberspace has matured over time and has in recent times seen emergence of cyber warfare related activities used in conflicts. Recently in the Mozambique conflict, a Yemen Cyber Army claimed responsibilities for cyber-attacks on several websites from various government entities and ministry of defence in Mozambique (All Africa, 2022). Following the reports that Boko Haram hacked the personnel records database of Nigeria's secret service (Baken, 2013), the Nigerian Chief of the Army ordered the creation of the Cyber Warfare Command as well as the Cyber Warfare School (The Nigerian Army, 2022). On 24 January 2022, in Mali, reports surfaced of information campaigns designed to launch cyber-attacks on humanitarian relief organizations2. The infiltration of technologies such as the use of drones as weapons in the Horn of Africa, Sahel and Mozambique by extremist armed groups, state actors or their proxies also signals the emerging trend of the hybrid war, and the exploitation of the cyberspace. (Thaba and Mtsweni, 2023).

3. Research Approach

The evolution of technology has prompted the authors to think about how military operations are affected, especially in Africa. The world over, militaries continue to review their capabilities, in line with the changing battlespace. This paper investigates how some militaries plan to transition their capabilities for the future battlespace. The nations studied in this paper have strategized digital transformation to help their militaries transform for effective operations in the future battlespace. The authors systematically review these open literatures and draw conclusions on how African militaries can use digital transformation to prepare their military capabilities for the modern battlespace and prepare for the cyberspace operations. The authors will also review how the transition could be measured to ensure success of implementation.

4. Digital Transformation

As acknowledged by various militaries, especially those of advanced nations, digital transformation is critical to achieving high levels of operational efficiency and effectiveness. Most of these nations have undertaken the process and invested lots of money in transforming their militaries for future battles. The general objectives of digital transformation, will be to enable the militaries to:

- Make informed, better, and pro-active operational decisions.
- Have superiority of information over adversaries.
- Better Situational Awareness allows them to adapt more quickly and effectively than adversaries.
- Improve competitiveness and operational effectiveness.
- Efficient use of resources by diversifying capabilities that take advantage of the evolving battlespace.
- Plan, prepare and to operate in cyberspace.

One of the driving factors to transforming military capabilities is the availability of data that makes them more intelligent and lethal, the effects required remain relevant with the evolution (Office of the National Director of Intelligence, 2021). The digital transformation addresses the ability to collect, process and transmit data relevant to operations. Migrating from legacy systems in this regard remains a great challenge. This stems from an already existing challenge of integration and interoperability of current systems. Digital transformation, if achieved, would address these challenges. Where new advanced technologies are inserted, the drive to ensure they are interoperable should be one of the challenges to be addressed by digital transformation. The digital backbone must be versatile to be able to handle evolving technologies (Abke, 2022).

5. Benchmarking

In this section, we systematically selected countries that have considered, planned, or are already on their journey to digital transformation to benchmark against African militaries. According to Scott (2011), benchmarking is a systematic approach of comparing processes, outcomes, products, services, and strategies of organizations, nations, or governments for improvements, lessons, and/or best practices. For this research study, we selected five (5) countries based on the indicators as shown in the Table 1 to benchmark against.

The National Cyber Power Index (NCPI) is used to measure the cyber intent and capability of nations in the cyber space and is limited to 30 countries, mostly first world countries (Voo, et al., 2022). The indices of the top countries are based on publicly available data focusing on 29 capability indicators across eight (8) cyber objectives. This simply means a nation is measured based on the intent to pursue multiple objectives using cyber

[2] https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know

means and has the required cyber capabilities to pursue and achieve the setout objectives. In the benchmarking exercise, we only focus on the superior and/or mature capabilities for each of the selected countries.

Table 1: Selection of countries for digital transformation and capability benchmarking

Selected Country	Digital Transformation Strategy Status	Digital Military Capabilities (Current or Envisioned)	Cyber Warfare Capability, Intent & Rank
United States of America	US Army Digital Transformation Strategy (2035 - Aimpoint)	Organic Digital Workforce Data-driven Army Cloud Native Adoption Strengthen collaboration and interoperability of data, software, and systems	-Ranked #1 -Cyber Offense -Information Control -Cyber Norms -Cyber intelligence
Republic of China	China's Military Modernization (2050)	Informatization AI and Advance Robotics Biotechnology Hypersonic and Energy Weapons	-Ranked #2 -Cyber Surveillance -Cyber Financials -Information Control -Cyber Commercials
United Kingdom	UK Army Digital Transformation Strategy	Artificial Intelligence One Defence Upskilling Data-driven military capabilities Digital Backbone	- Ranked #4 -Cyber Defense -Cyber Norms -Cyber Intelligence
Russia	Unknown	Unmanned ground, underwater, and air systems Artificial Intelligence in Weapon Systems	- Ranked #3 - Information Control - Cyber Defense - Cyber Intelligence - Cyber Commerce
Egypt	Digital Egypt (Vision 2030)	Unmanned Aerial Vehicles Surveillance	- Ranked #24 - Cyber Defence - Cyber Surveillance - Cyber Norms

5.1 United States of America

The US leads in various cyber warfare capabilities and has a digital transformation strategy (2035) in place for the US military (Office of the Army Chief Information Officer, 2021) that seeks to drive organic digital military workforce, and data-driven military operations. The strategy posits the modernization of the US Army's underlying network and computer infrastructure, which is essential to their success in the modern battlefield. The US digital transformation represents a shift in operations and culture that fundamentally changes how can the US defense delivers value through the adoption of advanced technologies such as cloud, data, and artificial intelligence (AI) (Dombrowski & Ross, 2008).

In terms of cyber warfare capabilities, the US is also ranked in the first position with superior cyber destructive capabilities, including control and manipulate the information environment. The US also plays a critical and leading role in the development of cybersecurity norms and technical standards across different forums including the United Nations. The US military also has a strong and superior cyber intelligence gather capability to deal with foreign and local threats including cyber terrorism. On the limitations, the US comes second on cyber technology competence, financial gain through cyber means, and cyber surveillance.

5.2 Republic of China

The Republic of China believes that emerging technologies will shape and increase the speed of warfare, meaning future military success will require forces that are "mechanized, informatized, and intelligentized"

(Horowitz & Kahn, 2021). As a result, China have achieved significant progress in their Digital Transformation Strategies, and strategic plans for Emerging and Disruptive Technologies such as Data and Artificial Intelligence. For example, China's 2016 document "China's National Defence in the New Era" aims to make significant progress in achieving the "Informatization" goal representing digital transformation by 2020; and implement the "Intelligentisation" concept by 2035-2050." (Dombrowski & Ross, 2008).

In the Cyber Power Index (CPI), the Republic of China is ranked #2, respectively. According to the CPI, China has a very strong cyber surveillance capabilities to deal with domestic and foreign cyber and traditional threats. Moreover, China is way ahead in using cyber means for amassing and protecting its financial power as well as localization the cyber industry working with public and private partners. From the Chinese case study, it is also clear that there is a strong link between the military and industry partners, including R&D institutions. This collaboration is interesting and indicates that future wars will be fought by the military collaborating with civilian stakeholders.

5.3 United Kingdom

The United Kingdom (UK) has one of the comprehensive military digital strategies amongst the superpowers. According to the United Kingdom's (UK) strategy (UK Army, 2023). The military capability elements in the physical world must be created in the digital world. Then the digitalization of relationships will be reflected in the virtual domain. The strategy continues to note that there are operational behaviors in which physical assets are utilized, and that these activities are carried out for the execution of tasks and duties. They include situational awareness (including evaluation), planning, decision-making, command, and administrative activities. These occur via processes that are well-defined in various forms of regulations. The outcomes of these activities create outputs or actions in the main mission areas of Force Employment, Force Development, and Force Sustainment.

Nevertheless, the UK lags in terms of digital and military capabilities against the superpowers being ranked#4 in the CPI having a strong cyber defence, are involved in the development of cyber norms and technical standards and have demonstrated the intent and capability of cyber intelligence gathering.

5.4 Russia

According to the benchmarking exercise, the Federation of Russia was found to be the only superpower with no publicly available digital transformation strategy for its military. Nevertheless, based on public documents, Russia has demonstrated digital capabilities for the modern battlefield (Lewis, 2022), and these include unmanned ground and underwater systems, AI in weapon systems as well as information control.

Russia is ranked #3 in the CPI. They exhibit a superior intent and capability in the control and manipulation of information environment, their cyber defence capabilities have been demonstrated during the Russia-Ukraine conflict and they have also demonstrated intent of building home-grown cyber capabilities without much defence on foreign countries.

5.5 Egypt

Egypt has a digital transformation strategy that cuts across the different national domains underpinned by vision 2030. Specifically on the cyber warfare, Egypt is ranked #24 out of 30 countries due to their developing cyber defence and surveillance capabilities. In addition, Egypt appears to be playing a participatory role in the development of cyber norms and technical standards. It is worth noting that Egypt is the only African country that is included in the rankings based on publicly available information.

It is evident that superpowers are gearing ahead in their digital transformation journeys to prepare and participate in the modern battlefield. In Africa, it is also clear that there is still a lot of work to be done to catch up in the 4th industrial revolution, and as such the lessons from other nations could be valuable in provided a roadmap for digital transformation in Africa, and this is proposed in the next section.

6. A Strategic Path to Digital Transformation for African Militaries

Digital transformation and cyber warfare capabilities are interconnected; hence this paper proposes that digital transformation to enable militaries to exploit the cyberspace and use its integrating factor to increase battle dominance. The cyberspace is imposed in military operations due to the evolving technological landscape. This implies that capabilities to operate in this domain are critical. There are both opportunities and challenges due to the adopting of digital technologies, and the dominance of the cyberspace for militaries. The challenges include the security vulnerabilities that come with digital technologies, as these create more entry points that can be possibly created by adversaries (World Economic Forum, 2022).

A survey conducted by Jang-Jaccard et al in 2014 established that as digital systems become more pervasive, the potential impact and sophistication of cyber warfare activities also increase (Jang-Jaccard & Nepal, 2014). This is true for and affects military operations. In this evolving operational environment, militaries must establish capabilities to enable operations in the cyberspace. These capabilities must be able to secure and exploit the cyberspace. The details of the required cyber warfare capabilities are addressed in the framework proposed in Thaba and Mtsweni (2023).

6.1 Capability Definition

Figure 2 overleaf depicts the proposed framework or strategic path towards digital transformation, with the specific focus on how African militaries can implement this. The path uses the Capability Lifecycle model (Smit & Oosthuizen, 2011) representing development phases for the military capability, encompassing related activities geared towards assisting African militaries to achieve digitally transformed capabilities. The model defines the capability in terms of POSTEDFIT model (Thaba & Benade, 2014), encompassing an extended view of the people, processes, and technology. In the capability definition phase, militaries must define the context and understand the strategic direction guiding the force's modernization. This phase must answer the question on why digital transformation is required. This phase must culminate in the development of a Digital Transformation Strategy that will enable African militaries to operate effectively especially within the cyberspace. In the context of cyber warfare, the capabilities requiring transformation are related to the ability to secure and exploit the cyberspace, and continuous improvement in operating cyber warfare capabilities as described in the proposed framework by Thaba and Mtsweni (2023).

However, transforming military capabilities, dominated by legacy systems that have been in operation for decades requires careful thought and consideration, because the threats these capabilities were established for still exist.

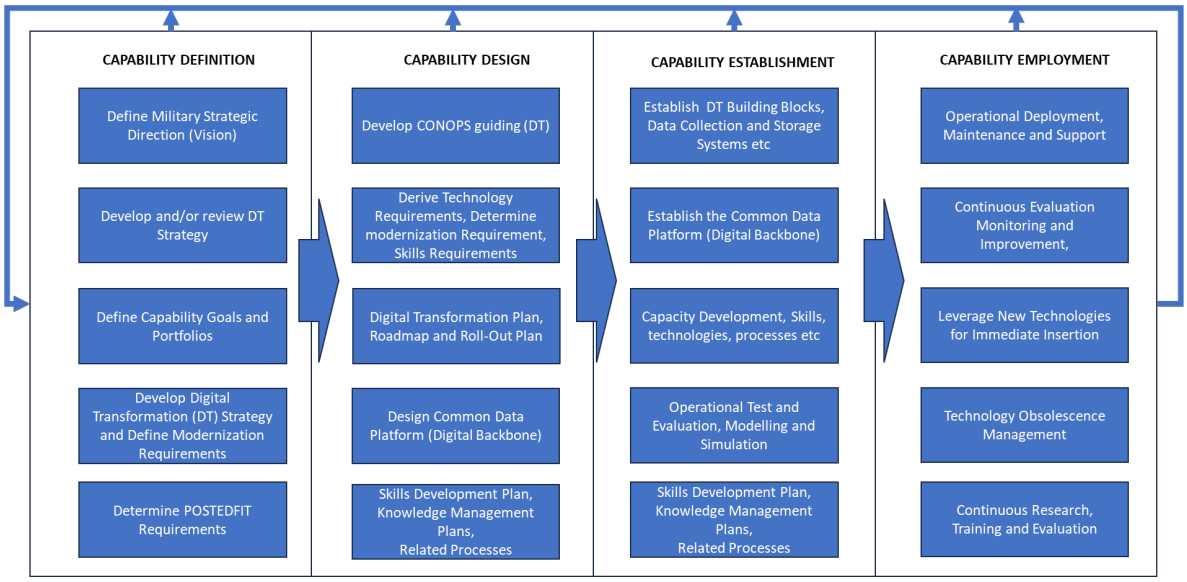

Figure 2: Proposed Path to Digital Transformation for African Militaries

6.2 Capability Design

Digital transformation significantly influences the landscape of cyber warfare by shaping the targets, tactics, and technologies involved in both offensive and defensive cyber operations (Osamo, et al., 2022). During the capability design phase, the efforts must be directed at developing the means to solve the problem as identified in the context in phase 1. During this phase, a concept of operation (CONOPS) must be developed. CONOPS will help derive technology and modernization requirements, leading to the development of the Digital Transformation Plan. This phase must answer the question on how African militaries digitally transform their capabilities to competently operate in the cyberspace. This phase will culminate in the Design of the Common Data Platform, the digital backbone as the critical component required to achieve digital transformation (UK Army, 2023). African military capabilities must be aligned to the current and future challenges and design capabilities for operations in the cyberspace.

6.3 Capability Establishment

This phase involves the establishment of the various building blocks contributing towards a digitally transformed force. As derived from the UK strategy, this must be a secure, singular, modern Digital Backbone (see Figure 3 overleaf) connecting sensors, effectors, and deciders across domains and with partners, driving integration and interoperability (UK Army, 2023). It must be an ecosystem, composed of a combination of people, process, data and technology that will enable friction-free access to our data, connecting sensors in one domain to platforms in other domains, via decisionmakers at the relevant levels in real time (UK Army, 2023).

6.4 Capability Employment

During the capability employment phase, a digitally transformed force will be tasked and deployed to perform various tasks. The phase also includes operational maintenance and support of a digitally transformed force. Technology develops at a fast pace in the modern battlespace; this phase also includes the ability to manage obsolescence and timeously insert technologies available or developed. The phase is concerned with the operational efficiency and effectiveness of the force (Anon., 2018). However, with digital transformation comes the availability of data as a strategic asset and a threat, which are more central to the operational efficiency or effectiveness of the military. However, data availability alone does not create necessary effects; it must be processed and packaged in a way suitable to provide decision support and intelligence to the decision makers.

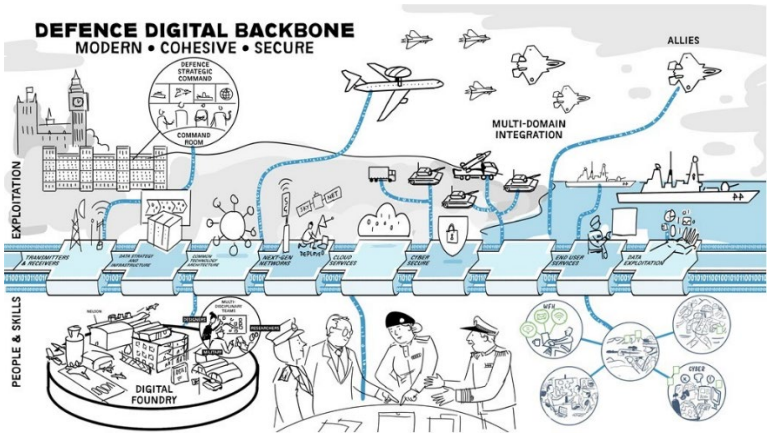

Figure 3: The Digital Backbone (Adapted from (UK Army, 2023))

7. Recommendations and Conclusion

The modern battlespace is characterized by the dominance of cyberspace, which is cutting across all the other traditional domains. This means actions in cyberspace have significant impact in the traditional domains. The boundaryless nature of cyberspace further complicates the battlespace, where the definitions, and boundaries for friend and foe are fluid, and can change any time. The ability to operate in the cyberspace for African militaries is no longer a choice, but a critical necessity. To operate in cyberspace, militaries need the ability to take full advantage of the digital space, by digitally transforming capabilities through digital transformation. In this paper, we propose a capability-driven strategic path for African militaries to transform their capabilities for the modern warfare. The roadmap is supported by an adopted digital maturity model that could aid and support African militaries to systematically develop to equally operate in the modern warfare.

Even for advanced militaries, digital transformation is acknowledged to be a process that will require dedicated effort and resources including time. African militaries must invest significant resources to the effort to be able to achieve this at least in the medium and long term. However critical is the strategic guidance, to give direction and initiation of the process, including availing necessary resources to undertake this process. The strategic guidance role also should be to facilitate this process amongst all the stakeholders, to ensure synergy, and movement towards one common goal. From this paper, the authors have demonstrated the applicability of the Capability Lifecycle management process, which was defined as the guiding phases towards establishing and managing digitally transformed military capabilities.

References

Office of the Army Chief Information Officer, 2021. *Army Digital Transformation Strategy,* s.l.: US Army.

Abke, T., 2022. *Digitalization in the Armed Forces.* [Online] Available at: https://www.linkedin.com/pulse/digitalization-armed-forces-tom-abke/

Anon., 2018. *US DOD.* [Online] Available at: https://irp.fas.org/doddir/dod/jp3_12.pdf

Billinga, D. C., Fordy, G. . R., Friedl, K. . E. & Hasselstrøm, H., 2021. The implications of emerging technology on military human performance research priorities. *Journal of Science and Medicine in Sport,* pp. 947-953.

Correia, J., 2019. Military Capabilities and the Strategic Planning Conundrum. *Security and Defence Quarterly.*

Delloitte, 2018. *Digital Maturity Model Achieving digital maturity to drive growth,* s.l.: s.n.

Dombrowski, P. & Ross, A. L., 2008. The Revolution in Military Affairs, Transformation and the Defence Industry. *Institute for Regional Security,* pp. 13-38.

Global Firepower, 2023. *2023 Military Strength Ranking.* [Online] Available at: https://www.globalfirepower.com/countries-listing.php

Hamilton, J., van der Smissen, S., Ruth, L. & Dailey, L., 2022. *Military procurement in a digital age,* s.l.: Deloitte Center for Government Insights.

Horowitz, M. & Kahn, L., 2021. *DoD's 2021 China Military Power Report: How Advances in AI and Emerging Technologies Will Shape China's Military.* [Online] Available at: https://www.cfr.org/blog/dods-2021-china-military-power-report-how-advances-ai-and-emerging-technologies-will-shape

Jang-Jaccard, J. & Nepal, S., 2014. A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences.*

Lewis, J. A., 2022. *Cyber War and Ukraine.* [Online] Available at: https://www.csis.org/analysis/cyber-war-and-ukraine

McGuffin, C. & Mitchell, P., 2014. On domains: Cyber and the practice of warfare. *International Journal,* pp. 394-412.

Office of the National Director of Intelligence, 2021. *The Future of the Battlefield,* s.l.: Global Trends.

Osamo, V. C., Azeta, A., Guembe, B. & Misra, S., 2022. The Emerging Threat of Ai-driven Cyber Attacks: A Review. *Applied Artificial Intelligence.*

Scott, R., 2011. Benchmarking: A literature review. *Academic Excellence Centre for Learning and Development.*

Smit, C. J. & Oosthuizen, R., 2011. *APPLYING SYSTEMS ENGINEERING PRINCIPLES TOWARDS DEVELOPING DEFENCE CAPABILITIES.* s.l., s.n.

Spak, U., 2021. *The common operational picture: A powerful enabler or a cause of severe misunderstanding?.* s.l., ICCRTS.

Thaba, M. & Benade, S., 2014. *Aligning force planning and systems acquisition.* Somerset West, Western Cape, In Proceedings of EMEASEC.

Thaba, M. & Mtsweni, J., 2023. *Developing Robust Cyber Warfare Capabilities for the African Battlespace.* Athens, Greece, s.n.

UK Army, 2023. *The Army Digital and Data Plan 2023 - 2025,* s.l.: UK Army.

Voo, J., Hemani, I. & Cassidy, D., 2022. *National Cyber Power Index 2022,* Cambridge: Belfer Center for Science and International Affairs, Harvard Kennedy School.

Williamson, S. C., 2009. *From fourth generation warfare to hybrid warfare,* Pennsylvania: United States Army.

World Economic Forum, 2022. *The Global Risks Report 2022,* s.l.: s.n.