DEVELOPING CYBER WARFARE CAPABILITIES AS AN INTEGRAL PART OF COMMAND AND CONTROL

AUTHORS

MR MPHAHLELA THABA
Council for Scientific and Industrial Research,
South Africa
Jthaba@csir.co.za

DR JABU MTSWENI
Council for Scientific and Industrial Research,
South Africa
Jmtsweni@csir.co.za

MRS MIRRIAM MOLEKOA
Council for Scientific and Industrial Research,
South Africa
Mmolekoa@csir.co.za

MS AVUYA MXOLI
Council for Scientific and Industrial Research,
South Africa
Amxoli@csir.co.za

ABSTRACT

The rapidly changing nature of the modern battlespace presents vast amounts of challenges to the modern Commander. Cyberspace has been identified as the fifth domain of war by North Atlantic Treaty Organisations (NATO) in addition to Land, Sea, Air and Space. The nature of this domain is such that it co-exists with all the traditional domains, and can never be isolated or treated separately from them.

The speed at which the modern Commander requires to make decisions in the cyberspace is expected to evolve to multiples quicker than the decision making cycle time in the other domains. This implies that Command and Control (C2) in its traditional sense, by form i.e. structure, and function will need to take into consideration this evolution.

The fourth industrial revolution (4IR) presents a whole new dimension of challenges to the battlespace. These could either be advantageous to the Commander's ability to accomplish a mission, or could present the opposing force with an added advantage, which the Commander will have to attend to.

This paper deals with the approach to developing cyber warfare capabilities, and how this should be an integral part of the overall military capability available to the Commander. It defines cyber warfare capability as a military capability, and proposes elements critical to develop this capability. The functional attributes for the cyber warfare capabilities as defined in the paper, are based on the National Institute for Standards and Technology (NIST) framework that focuses on five pillars: (1) Identify, (2) Protect, (3) Detect, (4) Respond and (5) Recover. In this framework, the aspects of Attack could be added in the Protect pillar.

The paper will conclude by proposing the lifecycle through which cyber warfare capabilities should be managed. It will further recommend possible amendments to traditional C2 functions, including structures supporting the Commander for successful accomplishment of a mission.

INTRODUCTION

Warfare has rapidly evolved over time, and continues to present even more challenges to the war fighter. The declaration of the cyber domain as a fifth domain of war challenges commanders and military planners to think differently. The cyber domain undoubtedly presents the most complicated challenges and cuts across almost all domains. (U.S. HOUSE COMMITTEE ON ARMED SERVICES, 2010)

The ability of the military force to deal with any eventuality presented by the cyber threats depends much on their ability to anticipate and develop relevant capabilities geared to influence the cyberspace. This domain's complex nature is fuelled more by the lack of identity of the enemy. Cyberspace can be viewed as three layers (physical, logical, and social) made up of five components (geographic, physical network, logical network, cyber persona, and physical persona) (US Joint Chiefs of Staff, 2018) as referred to in Figure 1 below.

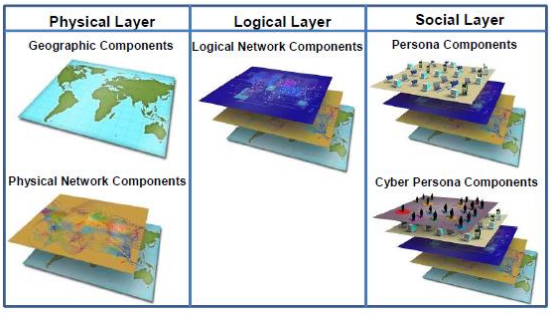

Figure 1: The Three Layers of Cyberspace

The military cyber warfare capability could be defined by using the NIST framework which is comprehensive enough to cover the full scope of cyber operations. For this paper, the NIST, and some modifications to it, is preferred to help define the military cyber capability.

Warfare in the 4IR

To understand the cyberspace as a domain of war, it is important to analyse this domain

relative to other domains, as it cuts across all of them. The main influences in the battlespace, forcing its evolution, remain the evolution of technology. Technology can both advantage the war fighters, but also equally disadvantage them, thereby empowering the opposing forces (Thaba & Benade, 2014).

The influences of the 4IR may not be the same for all militaries, as they range from well-funded to poorly-funded. This is because, whereas the well-funded armies may find it easy to absorb and in some instances lead technological developments, the smaller, less funded militaries may be forced to find ways of responding to the changing battlespace. (Liang Tuang, 2018).

The 4IR may influence the changing battlespace by including the use of autonomous, land drones equipped with advanced sensors, and linked to wireless command and control networks where artificial intelligence enabled decision making only requires minimal human intervention when lethal force needs to be used. (Liang Tuang, 2018).

This may imply significant reduction in the manpower requirements when autonomous drones are used. This also indicates a significant change in the Command and Control requirements for such a force. With the third industrial revolution having introduced the power of computers, the 4IR further increases the use of mobile internet, increases the intelligence of machines through Artificial Intelligence (AI), and Machine Learning (ML) and further interconnects the battlespace through Internet of Things (IoT). These phenomena introduce the significant complexity and the fifth domain of war, which is the cyberspace domain. Figure 2 below depicts the net-enabled battlespace.

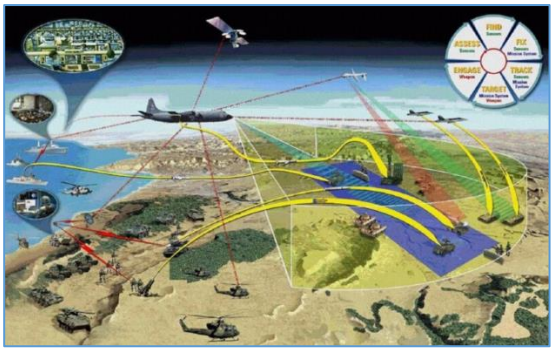

Figure 2: The Network-enabled Battlespace

Cyberspace domain

Cyberspace is defined by Porche (2016) as both a global domain and a global commons whose reach is being constantly expanded not only by wired and wireless connections, but by sneaker-netted connectors that close all air gaps (Porche, 2016). He further elaborates that everything from home thermostats to the critical infrastructure that is vital to daily life, water, power, manufacturing, etc. are within its reach. According to Porche (2016), the cyberspace is shared by all, but no one dominates the space.

Cyberspace exists across all domains of war i.e. land, sea, air and space. All operations as defined in the four domains are also, by nature of the technologies used in these operations, affected or exist in the cyberspace. With the evolution of technology and the ever changing battlespace due to this evolution, communications over computer networks have become a norm, rather than an exception.

INFLUENCES OF THE 4IR on Command and Control (C2)

The concepts of the 4IR that may have an influence on C2 will be those that affect the ability of the Commander to exercise authority over his forces. This should include all influences on the ability to plan, task, coordinate and control. These activities are not mutually exclusive to the ability of the Commander to execute the Observe-Orient-Decide-Act (OODA) loop sufficiently.

The traditional OODA loop has been improved over time to be replaced by the Dynamic-Observe-Orient-Decide-Act (DOODA) loop and subsequently the C2 cycle to include the collecting, decision making and effecting phases. Figure 3 below depicts this transition.

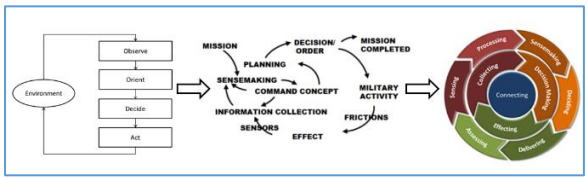

Figure 3: OODA loop, DOODA loop and the C2 cycle

The Commander's decision cycle loop, and the C2 cycle stand to be greatly influenced by the 4IR. The greater challenge to the Commander remains the fact that the cyberspace co-exists with the traditional domain, which implies that decision making in the traditional domain, will be greatly influenced by decision to be taken in the cyberspace. This means that the Command authority vested on the Commander, and the control mechanisms over his force should take into consideration the effects required in the cyberspace.

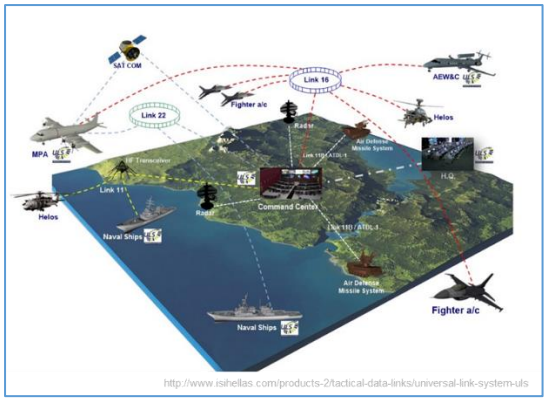

Figure 4: Tactical Data Links

Figure 4 above depicts a tactical concept use of the data link and the Command Centre control over the battlespace. Figure 4 could be used to illustrate how malicious interruptions of a data link could have devastating effects on operations. This interruption would be effected in the cyberspace.

Given the possible influences of the 4IR on warfare, it is important to highlight how these advancements may influence the development of military capabilities as discussed in the following section of this paper.

Many of the integrated (Command, Control, Communications, Computers, Intelligence and Reconnaissance) C4IR systems as part of the tactical intelligence system to collect, process and disseminate information to troops are also dependent on commercially available components which do not provide high levels of security. This is primarily due to the fact that cyber security was not part of the system design consideration from inception in order to ensure redundancy, resilience and protection of these C4IR systems. As such this presents a wide area of vulnerabilities from a system data security and cyber security point of view.

The worldwide digital technology transformation has led to the development and use of networked, agile and intelligent military C4IR systems. The agile system characteristics are brought by the fact that these are software driven and softer defined to allow the system operator, for example, to change system parameters on the go.

The intelligent characteristics are brought by use of artificial intelligence algorithms to allow for predictive system behaviour and intelligence to enable the determination of the possible course of action. The challenge with these is the fact the software of such systems is easily prone to Electronic Warfare (EW) influences and cyber vulnerabilities through manipulation and exploitation of the software applications and source code running on such systems.

DEVELOPING MILITARY CAPABILITIES

Military Capability

The definition of a military capability is derived from the systems engineering definition of a capability as the ability to achieve a desired effect under specified standards and conditions through combinations of ways and means to perform a set of tasks. (Office of the Deputy Under Secretary of Defense for

Acquisition and Technology - Systems and Software Engineering, 2008). The Australian Defense, in the capability development handbook, defines capability as the capacity or ability to achieve an operational effect. The handbook further states that operational effect may be defined or described in terms of the nature of the effect and of how, when, where and for how long it is produced. (Andrew Dakin, 2012).

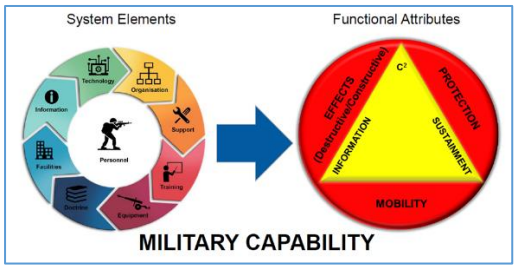

Figure 5: Military Capability: System Elements and Functional Attributes

From the definition above, cyber warfare may be considered a military capability and may be critical for use by the Commander to win wars. This cyber capability exists in the cyberspace. In applying the capability definition in the cyberspace, the complexity remains the fact that the specified conditions and standards are in most cases non-existent. Therefore, the attention required in this space may require more out of the ordinary approach from the Commanders and planners.

A military capability is made up of system elements namely, Personell, Organisation, Support, Training, Equipment, Doctrine, Facilities, Intelligence and Technology (POSTEDFIT) as depicted in Figure 5 above. This capability in the South African context has six functional attributes, namely Effects (Firepower), Mobility, Protection, Command and Control, Information and Sustainment (FMPC2IS). (Thaba & Benade, 2014).

From the Functional Attributes depicted in Figure 5, the offensive and defensive nature of cyber capabilities may be categorised in the Effects (Destructive/ Constructive) and used in the same manner Firepower is. However, its influence and use may be more complicated than Firepower hence it is the objective of this paper to motivate for cyber as an integral part of C2.

The NIST framework has been used for this paper to guide the definition of capabilities in the cyberspace. The framework has been adapted to include "predict" (see **Error! Reference source not found.**). (Mtsweni, Gcaza, & Thaba, 2018). In order to fully understand the cyber capability required for the military, it is critical to understand the operations that the military will conduct in the future. It is also clear from the discussion above on warfare in the 4IR, that the cyberspace has become an important domain of war to consider, and that this domain affects (and or exists) in the other domains, land, air, sea and space.

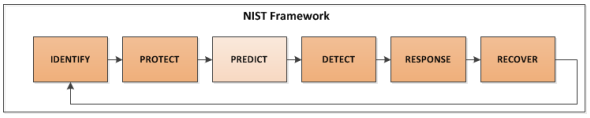

Figure 6: Adapted NIST Cybersecurity Framework

The evolution of technology should be treated as one of the factors to analyse in order to understand the impact to how the military intends to conduct operations in the future. The rise in the use of technology, especially computers, cellphones, etc. is directly proportional to the rise in vulnerability of any force. To understand the effects required in the cyberspace, we must understand how own operations may be affected in this domain. To understand this, the NIST framework as adapted is used to analyse the problem.

NIST Framework

The NIST commences with the need to know and understand own Assets. This means the military must **Identify** all relevant and related assets required for successfully conducting operations, including their own assets to protect against adversaries. This also should take into consideration the complexity, advantages and disadvantages posed by the 4IR in the battlespace. The phase helps

organizations to understand their environment to manage cybersecurity risk to systems, assets, data and capabilities. (NIST, 2018).

Once the Assets are Identified, there is a need to **Protect** them. The protection of the assets is against any possible unathorised access by the opposing forces. Development and implementation of the appropriate safeguards to nullify, or limit the impact of a potential cybersecurity event must be high on the priorities of any organisation (NIST, 2018).

In order to be proactive, there must be an ability to **Predict** any possible malicious actions that could be attempted against own operations. This ability requires systematic use of data to predict possible actions against own operations, and the ability to use these predictions to gather threat intelligence in order to implement proactive measures. (Mtsweni et al., 2018)

Supporting the protection mechanisms put in place, the ability to **Detect** any anomalous activity and other threats to operational continuity is required. This ability must include being able to have visibility into its networks to anticipate a cyber incident and have all information at hand to respond to one. (NIST, 2018). This must be a continuous activity throughout the operation.

In the event there is penetration through protection mechanisms without prior detection, and a cyber incident occurs, there must be an ability to **Respond** and nullify or limit the impact. This ability should include development of a response plan, definition of incident response standard operation procedures, collection and analysis of information about the event (NIST, 2018).

In the event the response actions are not sufficient to nullify or limit the impact, there must be an ability to **Recover** from such an even. This ability must address the development and implementation of a recovery plan, and the ability to coordinate restoration activities with all relevant stakeholders (NIST, 2018).

Offensive Capabilities

The adapted NIST as discussed above addresses cybersecurity, which by nature is defensive. Cyberspace operations can be both offensive and defensive. The US defence identifies three missions associated with the cyberspace operations, these are offensive cyberspace operations (OCO), defensive cyberspace operations (DCO) and Department of Defence Information. (US Joint Chiefs of Staff, 2018). The defensive operations and associated capabilities are sufficiently covered and characterised by the NIST. The offensive related capabilities could be defined with a view to create freedom of operations by own forces. This could include denial of sevice to disrupt the opposing force battlefield operating systems like C2, firepower resources and many services as required to conduct their operations. The offensive capabilities could be linked to the adapted NIST through the Predict function. The predict function would represent the sensor for potential information to be used to exploit the enemy's weaknesses.

Capability Lifecycle

A military capability exists and evolves through a capability lifecycle depicted in Figure 7 below. The lifecycle consisting of 4 process phases, proposes the process of capability definition by determining what the military needs to be able to do; capability specification which determines how the force intends achieving what they need to do; capability establishment referring to the process of establishing the operating baseline for the capability and lastly the capability employment which deals with employing the capability for operational effectiveness.

Figure 7: Capability Lifecycle

Capability Definition

The first step to defining the capability is understanding what an organisation needs to be able to do. This includes thorough analysis of the operational environment and development of various possible scenarios within these environments. During this phase, an analysis of the cyberspace must also be undertaken to understand the possible cyber challenges it may be phased with, this should also include the possible vulnerabilities that can be taken advantage of.

The analysis using the NIST, allows for the determination of what the ability required should be, and overall what a military force should be able to do in order to deal with cyber eventualities. This ability cannot be seperately considered without understanding the overall operations of the force across all the domains of war. Therefore, the plan to establish the cyber capability cannot be viewed in isolation to other military capabilities.

Capability Specification

Once the definition phase has been completed, there is a need to explore ways of how to solve the problem. This is underpinned in how a force plans to operate. This is achieved by developing various possibilities of Concepts of Operations (CONOPS) which should also detail operations that will be conducted in the cyberspace.

Further to the analysis of the CONOPS, it is important to apply the NIST to develop a subordinate operational concept to identify all necessary assets as they will be required in the operations, and the means as an intergral part of the CONOPS to protect these assets. Furthermore, this concept must address how to detect any possible malicious activities meant to influence own operations, and when necessary respond accordingly to any detected event.

In the event where malicious activities may have succeeded in penetrating and causing some level of damage, the concept must address recovery mechanisms. It must be also be noted that while developing these various iterations of concepts, it is important to also thoroughly analyse how own forces could predict possible cyber eventualities, and create threat intelligence that could be used in scenarios to develop proactive mechanisms to deal with cyber events.

Once the concepts are developed, critical tasks will be identified and capabilities required will be specified from these. Once the capabilities are identified, it is important for already existing military capability, that an audit is conducted to determine what the force can or can not do. This will be done by mapping determined capabilities with existing legacy capabilities.

The Capability Maturity Model depicted in **Error! Reference source not found.** below is recommended to be applied to determine the level of maturity. This model provides a benchmark against which the current level of capability of its practices, processes, and methods and set goals and priorities can be evaluated and improved. (Christopher et al., 2014).

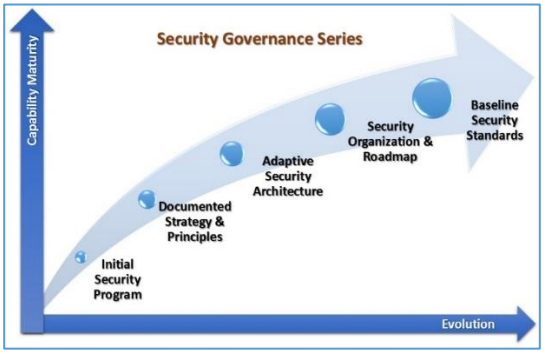

Figure 8: Cybersecurity Capability Maturity Model

The results of applying the maturity model will be the identification of capability gaps. These gaps may be due to capabilities being phased out, or it could be that they never existed. These gaps, for a military capability, would then be expressed into requisite capability elements required to fill the gaps. The ultimate goal of this phase is also validation, i.e. the process of ensuring that specifications respond

adequately to the capability requirements. (Stuart, 1980).

Capability Establishment

During Capability Establishment , the empasis is in responding to the gaps identified to address how they will be filled. This also includes continued improvement of existing capabilities (upgrades where necessary). Mtsweni et al (2018) argue that, in order to improve the cybersecurity posture of complex organizations, a holistic approach is necessary to achieve adequate security and resilience as depicted in Figure 9 below.

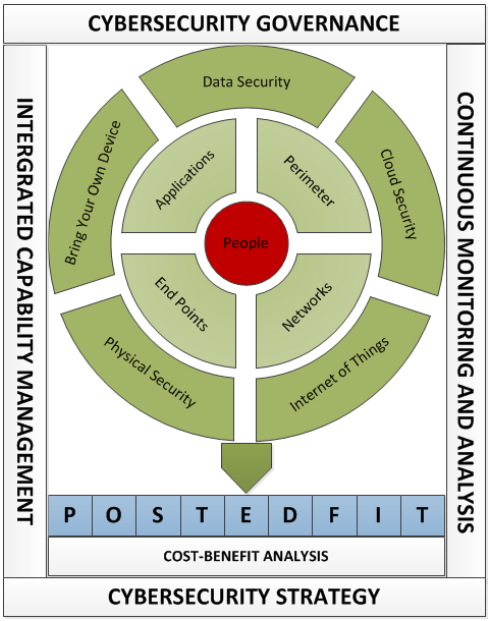

Figure 9: Unified Cybersecurity Framework for Complex Environments

This argument supports the caution with which the establishment of cyber capabilities in military operations should be undertaken. Mtsweni et al (2018) further propose the Lines of Development for cyber capabilities in complex environments as seen in Table 1 below (Mtsweni et al., 2018). These have been adapted from the military Capability Elements in order to fit in the cyber security space.

Capability Employment

Since the cyberspace co-exists with the other four domains for as long as computer networks are relied on to facilitate communications and execution of activities, cyber capabilities will need to be employed as part of the broader employment of military capabilities during missions. The capability employment phase for military capabilities is more concerned with ensuring that the capability established reaches the required levels of Operational Effectiveness (OE). It is during this phase when verification is conducted to ensure that the established capability meets the capability specification. (Stuart, 1980). For this to be achieved for a Joint operational capability, cyber defence experimentation and validation capability must be established and maintained. (Jordan & Hallingstad, 2013).

Table 1: Capability Elements (Lines of Development)

Element	Relevance
P-Personnel	For any capability to be effective and sustainable, qualified resources to support the capability are important. This include maintaining such resources, recruiting correct skills, career development, and leadership.
O-Organization	The structure and nature of the business need to be considered when establishing and maintaining the cyber capability. This will include aspects such as the size, shape, culture, processes, etc.
S-Support	The cyber capability cannot be effective without organizational, logistical, infrastructural, informational, and financial support. These need to be honestly considered when deciding on establishing or improving the capability.
T-Training	Individuals, departmental, and organizational training must not be ignored during the capability planning process. Factors that need to be considered in this element may include training content, methods and resources required to train the people so as to enable adequate performance of the capability. Also training needs to be dynamic and adaptive and suit the forever changing cyber environment.
E-Equipment	Over and above technology, the equipment required supporting the capability need to be factored in, and this may include physical security equipment and telecommunication equipment and so forth.
D-Doctrine	This element can be likened to governance including regulations, operating procedures, policies and strategies that must be in place to affect the cyber capability in a complex environment.
F-Facilities	A cyber capability cannot exist in the “space”, but needs to also be housed in some physical space is accessible and secure. As such during a cyber capability planning activity, facilities should be

	considered, and this may include facilities for servers, digital forensics, operations centres, and data centres.
I-Intelligence	A cyber capability without threat intelligence is not enough. It is therefore important that information, data, data processing systems, knowledge management systems, are always available to support the cyber capability and enable continuous improvements and predict future cyber incidents.

CONCEPT DEVELOPMENT AND EXPERIMENTATION (CDE) CAPABILITY

The rapidly evolving nature of the cyberspace, requires for more agile and responsive ways to the capability development, and management of current capabilities. The influences of the 4 IR, with more autonomous systems infiltrating the battlespace, AI being an integral part of these systems, planning for future capabilities has become a complex phenomenon. This, therefore, requires an establishment of a CDE capability where various concepts could be developed and validated, and once capabilities are developed be verified in these environments. This capability should consist of skilled and experienced people, well defined processes and procedures and technologies and tools readily available for use. Figure 10 below shows some of the environments established for validation and verification interoperability in the South African National Defence Force.

Figure 10: The Interoperability Development Environment

CONCLUSION

Since the advent of computers and computer networks, and their adoption in military operations, the complexity of the battlespace has increased tremendously. This complexity has even led to the introduction of the fifth domain of war, cyberspace, as adopted by NATO. This new domain of war unarguably cuts across all domains, due to the evolution of technology and the prominent use of computers and networks in warfare across all domains. The ability to deal successfully with the challenges posed by the new domain, depends largely on the ability to develop requisite capabilities ready to efficiently be employed by the commanders.

The influence of technology on C2 continues to increase even more in the 4 IR. Use of autonomous land vehicles, AI, machine learning, 3 D printing, continues to complicate the operating space for the commander, and in some cases even limits the ability of the commander to operate as was trained. The 4 IR also emphasises more on cybersecurity as many systems available to the commander now operate in the cyberspace. This makes the cyberspace an integral part of the commander's operating environment. This forces commanders to consider factors in the cyberspace for analysis as part of planning and execution of operations. The NIST has been demonstrated as one of the ways to guide analysis of the cyberspace, from identification of assets, protection of these assets, prediction of possible events, to develop threat intelligence, detection of any malicious activities that may influence the operations, responding to these events to nullify or limit their impact, and in the case penetration of malicious activities could not be detected, respond to the damage caused by this. All these must be an integral part of the commander's considerations during the planning and execution of operations.

The ability to control the cyberspace (and the intersecting electromagnetic spectrum) could be tantamount to controlling the information environment. (Porche, 2016). This could be

advantageous to the commander's ability to successfully conduct operations. If not well considered, it could be exploited by the opposing force at the detriment of own forces.

RECOMMENDATIONS

Cyberspace cuts across all domains of war, and should be analysed thoroughly as part of the environment, including the analysis of opposing forces for cyber. Due to its existence in all domains of war, cyber or cybersecurity should be an integral part of the Command and Control considerations, and should be treated in the same manner as Firepower for both offensive and defensive use.

Cybersecurity specialists and the team should form an integral part of the commander's staff compliment and must be given high priority during all phases of planning to give a thorough analysis of the cyberspace and advise the commander on the strengths and possible vulnerabilities.

Cyber Command should be established to exploit operations in the cyberspace autonomous to operations in other domains. Specialists from this Command should be deployed in all other operations as part of the command staff.

Cyberspace offensive operations, as and when required must be sanctioned by the highest command authority available, and must be carefully assessed for military benefit, before implemented. This remains a Command function.

REFERENCES

Andrew Dakin, L. (2012). *Defence Capability Development Handbook 2014*. Retrieved from

Christopher, J. D., Gonzalez, D., White, D. W., Stevens, J., Grundman, J., Mehravari, N., … Dolan, T. (2014). Cybersecurity Capability Maturity Model (C2M2). *Department of Homeland Security*, (February), 1–76.

Jordan, F., & Hallingstad, G. (2013). Towards Multi-National Capability Development in Cyber Defence. *Information & Security: An International Journal*, *27*, 81–89.

Liang Tuang, N. (2018). *the Fourth Industrial Revolution ' S Impact on Smaller Militaries : Boon or Bane ?* (November).

Mtsweni, J., Gcaza, N., & Thaba, J. (2018). *A Unified Cybersecurity Framework for Complex Environments*.

NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity*.

Office of the Deputy Under Secretary of Defense for Acquisition and Technology - Systems and Software Engineering. (2008). Systems Engineering Guide for Systems of Systems. In *Technology*.

Porche, I. (2016). Emerging Cyber Threats and Implications. *Emerging Cyber Threats and Implications*. https://doi.org/10.7249/ct453

Stuart, W. D. (1980). Guide to the Systems Engineering Body of Knowledge (SEBoK) v1.8. *American Society of Mechanical Engineers, Applied Mechanics Division, AMD*, *42*, 73–80.

Thaba, J., & Benade, S. (2014). Aligning force planning and systems acquisition. *INCOSE International Symposium*, *24*(s1), 514–527.

U.S. HOUSE COMMITTEE ON ARMED SERVICES. (2010). CYBER OPERATIONS: IMPROVING THE MILITARY CYBER SECURITY POSTURE IN AN UNCERTAIN THREAT ENVIRONMENT. *Sda*.

US Joint Chiefs of Staff. (2018). CYBERSPACE Operations. *Joint Publication 3-12*, (June), 104.