FACING THE CULTURE GAP IN OPERATIONALISING CYBER WITHIN A MILITARY CONTEXT

L Leenen[1], MJ Aschman[2], MM Grobler[3], A van Heerden[1]

[1] CSIR, South Africa
[2] Rhodes University, South Africa
[3] CSIRO Data61, Australia
lleenen@csir.co.za
michael.aschmann@sita.co.za
marthie.grobler@data61.csiro.au
avheerden@csir.co.za

Keywords: Cyber Culture, Cyber Operations, Cyber Warrior.

Abstract:

Cyber as an operational domain is widely recognised by military forces, but the process to operationalise cyber poses a number of challenges. One of the difficulties is that traditional military culture is far removed from what is commonly referred to as "cyber culture". The latter refers to the culture amongst cybersecurity professionals (and cyber warriors). In any organisation, but particularly within the military context, it is commonly agreed that cultural understanding is one of the primary concerns, taking into account that culture is fluid rather than static and that humans express their cultural systems in a variety of ways. It can be hard to understand the cultural dynamics demonstrated in various situations. Another challenge is that cyber is present at every level and division of the military. It is thus necessary to distinguish between the different roles or presence of cyber in a military force. The modern military force should recognise the presence of cyber in every division and arm of service, in addition to incorporating or establishing specialised cyber defence and warfare units. In this paper, the authors give an overview of current views on operationalising cyber, the culture gap and how to address this gap to enable the operationalisation of cyber within the military context.

1. Introduction

Cyber affects all aspects of an entity and is recognised as a force multiplier for both state and non-state actors. In the military context, cyber affects all units and divisions of a military force: every unit will require staff and processes to satisfy their cyber requirements, training and processes. Admiral Rogers, commander of the US Cyber Command, stated in 2015 that military leaders will have to understand the importance and the challenges of operating in the cyber domain (Garamone, n.d). As such, a military force also needs a capability to secure its nation against cyber threats and to launch cyber-attacks as part of its cyber defence activities in order to protect the nation's cyber sovereignty. However, the operationalisation process of cyber needs clarification (Ducheine and van Haaster, 2014). Military cyber operations are usually conducted in conjunction with military conventional operations and military operations other than war (MOOTW), but there are numerous challenges a military force faces in terms of operational structure and the recruitment of skilled staff in order to conduct and support missions in the cyber domain (Harris, 2016).

One of the challenges in establishing specialised military cyber units is the difference between traditional military culture and cyber culture. The latter refers to the culture amongst cyber professionals, including military cyber warriors. This cultural gap is increasingly recognised in the military environments (Carberry, 2017; Chezem, 2015; Goldstein, 2017; Harris, 2016; Roislien, 2015). To conduct cyber operations successfully and efficiently, military forces will have to acquire new attitudes, strategies and doctrine. Harris (2016) states: "… the service [US Army] must address four immediate personnel challenges to ensure the success of its cyber work force. It needs to understand the typical characteristics of its cyber talent; organize its operational structures to effectively employ this talent; create an environment that fosters innovation; and learn to lead these forces." Chezem (2015) recommends that the military try to mimic the culture of effective cyber organisations since cyber professionals require an environment that rewards innovation and the acquisition of specialised cybersecurity skills. Roislien (2015) notes that there is no common agreement by different military institutions and nations on how the military should acquire a professional cyber officer workforce. Therefore, the concept of a cyber officer requires investigation in order to standardise procedures and practices across military forces.

This paper considers the ongoing debate on the operationalisation of cyber and contributes recommendations for an efficient and beneficial operationalisation process within the military context. Other challenges such as the cultivation

of a cyber culture and the retention of military cyber professionals are also addressed. An overview of cyber operations is followed by considering the required specialists. In Section 4 the attention is turned towards creating an environment suitable for cyber operations with a focus on cultural aspects. Section 5 considers the cultural gap between military and cyber culture. Section 6 provides recommendations for enabling cyber culture within the military.

2. Cyber Operations

Cyber technology and communication capabilities have been acknowledged as critical in a world moving towards the operationalisation of cyber in various contexts. Pyburn (2009) studied the significance of cyberspace in the military context, referring to this new paradigm as "the newest warfighting domain". This notion is supported by Chourci and Goldsmith's (2012) observation that military operations have shifted focus — from traditional military operations entailing "national borders and territorial integrity" to a reality where cyberspace have become the new paradigm in terms of growing global tensions and new opportunities for avoiding conflict. Pyburn (2009) makes a case for the potential benefits of utilising cyber-centric operations in the military context, but also notes the accompanying risks and challenges that include the potential disruption of military systems through cyberwarfare.

Cyber operations is viewed as all cyber activities that a security cluster of a nation will be part of to either defend against or attack an adversary with a cyber-intervention. In this context, a security cluster is viewed as a nation's military and police force, departments of justice, national intelligence and finance. A joint security clustered approach is fundamental in the planning of a cyber operation to augment the different entities' capabilities. The Tallinn Manual (Schmitt, 2013) offers the following definition for a cyber operation: "The employment of cyber capabilities with the primary purpose of achieving [military] objectives in or by the use of cyberspace". The goal of cyber operations is to achieve an effect, namely influencing actors in and through cyberspace. Cyberspace can be regarded as "the global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interdependent and interconnected networks using information-communication technologies" (Kuehl, 2009).

Ducheine and van Haaster (2014) note that cyber operations share conceptual similarities with effect-based operations, but that they differ in capabilities and targets. The non-physical dimension of cyberspace includes new elements that enables new possibilities: cyber objects (the logical elements enabling communication between physical objects) and cyber identities (the digital identities of people, individuals, groups and organisations). The concepts of time and space are also different in cyber operations: operations can happen at the speed of light, and cyber objects and identities are not confined to a delimited geographical state. Another differentiating factor is that although the instigator of an attack can be traced, cyber operators may be politically, legally and technically prevented from retaliating. These novel challenges and opportunities of cyber operations have to be understood and incorporated into the military before cyber operations can be effectively deployed.

Breaking cyber operations down to its basic nature, it is viewed as the integration of Information Operations, Influencing Operations and all combinations of different cyber activities, all occurring under one mandate. Allocation of cyber activities in a cyber operation will need to be coordinated so that there is a focus of main effort (FME) maintained to reach the desired end state. The implementation of cyber operations during planning will need to take into consideration the legal implications (dependent on the nation's rules of engagement and mandate under a joint military operation) as well as the boundary clarification of different security organisations, especially in this regard with respect to the different organisational cultures. The integration of outsourced cyber activities within the security clusters will need to be managed correctly to ensure that there is an orientation of how the security cluster's culture is aligned with the cultures of the various (non-state actor) cyber professionals.

In order to incorporate cyber operations in a military force, an understanding of the nature and impact of these operations have to be gained and aligned with new approaches, concepts and doctrines. However, one of the main obstacles that has to be addressed is how to incorporate the cyber specialist and cyber warrior in the conventional, MOOTW, or traditional military environment. In the words of the commanding general of the U.S. Army Cyber Command, Lt. Gen. Cardon, "Technology, as significant as it is in the rapidly changing face of warfare, will not be the deciding factor in who will dominate in this domain. It is the people." (Harris, 2016). The next two sections consider the human factor in operationalising cyber.

3. Cyber Specialists and Cyber Warriors

Both cyber warriors and cyber specialists are required for cyber operations. A cyber warrior can be defined as a soldier who is highly skilled in the cyber environment (i.e., ICT skills in networks and security) and fighting the cyber battle

within a computer network, both from a defensive and an offensive posture. A cyber warrior can further be defined as a person who engages in cyber warfare (both defensive and offensive in nature), whether for personal reasons or out of patriotic or religious belief (Technopedia, n.d.).

A cybersecurity expert is an individual who has attained superior performance in one or more of the cybersecurity application areas (Zeltser, 2016). These cyber professionals can be defined as highly skilled ICT personnel who observe and ensure that there are no security and information breaches within the computer system that they are responsible for, according to legislation and other best practices and policies. Cybersecurity is a niche market integrated into information technology and has numerous areas of specialisation, including application security, network defence, intrusion detection, digital forensics and incident response, endpoint protection, and governance, risk and compliance.

Pyburn (2009) points to behavioural attributes required by military personnel engaged in cyber warfare operations. At the tactical level, cyber warriors need to leverage their technological knowledge to employ cyberspace weapons and systems. At the operational level, cyber warriors need to use their broad knowledge of cyberspace capabilities to plan and shape campaigns to achieve strategic objectives. Cyber warriors specialists should provide, sustain, and maintain infrastructures and systems supporting cyberspace operations. This includes a wide range of activities, from maintaining a local and wide area networks (LAN and WAN) to installing a server on an airborne platform. Cyber warriors have to perform defensive functions intended to enable operations. Similarly to current intelligence analysts, cyber analysts will investigate and analyse all possible intelligence sources to provide assessments, indications, and warnings.

For cyber specialists and cyber warriors to be successful in the cyber domain, the acts of cyber aggression (battles within the cyber domain) need to be understood. There are five distinct characteristics that sets the cyber domain apart from other more traditional battlefields (Grobler and Swart, 2014):

- Dematerialisation. Anonymity is a key factor in cyber war: the true origin of the attack must remain hidden.
- Cancelling time and space limits. All traditional restrictions are removed from the planned attack, making the potential scope for attack much bigger. Network connections will make it possible to have immediate access from anywhere and at any time.
- Gaining control over time and space, over physical resources. The aim of war is to gain such control over the physical world in order to use time and space to the maximum benefit of the cyber war's intended outcome.
- Exploit the complexity and interdependencies of modern systems. The attacking nation does not have to directly attack the target, but rather attack unsecured targets which have some kind of interdependencies on the actual target.
- Exploit generalised intelligence. The aim is to openly collect a large amount of possibly useless or common data and compile it in order to have significant and deep knowledge of a given target.

4. The Culture Gap: Cyber Culture vs Traditional Military Culture

Insight into cultural differences, particularly from an organisational level of analysis, has become a critical priority within an increasingly interconnected world. Culture has been defined in terms of a collective and shared sense of relatedness to the human experience (Herskovits, 1948). According to Schein (1985), there are four categories of culture: macro-cultures (nations or occupations that exists globally), organisational cultures, sub-cultures (groups within organisations) and micro-cultures (microsystems within organisations). Within the cultures there are three levels that include visible artifacts, espoused beliefs and values, and basic underlying assumptions.

To measure and fully understand culture, different cultural dimensions can be identified. A dimension can be seen as "an aspect of a culture that can be measured relative to other cultures" (Hofstede, 1980). Hofstede identified four cultural dimensions in his original theories and later two additional dimensions (Hofstede, 2011):

- Individualism vs. collectivism – defines the extent to which individuals are inclined to remain in networks or prefer to look after themselves.
- Masculinity vs. femininity – masculinity points to a group's preference for assertiveness, achievement and material award as an indication of success whilst femininity indicates a preference for modesty, cooperation and striving towards quality of life.
- Uncertainty avoidance – indicates the extent to which members of a group are not at ease with ambiguity and uncertainty; a high level of uncertainty avoidance is associated with more rule orientation.
- Power distance – the extent to which societies and organisations accept power differentials; high levels of power distance are associated with authoritarian leaders and a reluctance to express disagreement with superiors.

- Long term vs. short term orientation – points to an inclination to search for virtue (over a longer term) as opposed to groups that are inclined to the establishment of an absolute truth.
- Indulgence vs. restraint – indicates the degree to which a group can exercise control over their impulses and desires.

Hofstede's comparative studies focused on the comparison of the values and behaviours of culturally diverse individuals, as well as their institutional and organisational cultures across various nations around the world.

"Cyber culture" is a sub-culture that refers to the culture found amongst cyber professionals; it can also be argued that it is becoming a macro-culture. Da Veiga (2016) defines cybersecurity culture as: "the intentional and unintentional manner in which cyberspace is utilized from an international, national, organizational or individual perspective in the context of the attitudes, assumptions, beliefs, values and knowledge of the cyber user". It stems from the cybersecurity procedural knowledge and consistent application thereof by a cyber user. Cyber culture tends to have low power distance relationships that allow subordinates to challenge their managers, exhibits low levels of uncertainty avoidance and value individualism.

Cyber culture differs markedly from traditional military culture. Soeters (1997) found that although military institutions have their own organisational cultures which are related to their national cultures, an international military culture does exist. The institutional aspects of military life is accentuated in the military culture as opposed to an occupational aspect; in other words, a military career is not just seen as a job; it is viewed to be a lifestyle and a sacrifice. Military culture is bureaucratic and relatively isolated from society. Military staff work, and often live on military bases, they tend to get their training in specific academies and thus a sense of uniqueness is cultivated. (Soeters, Windslow and Weibull, 2016). Cyber warriors and military cyber specialists will probably share many values and traits with non-state actors but they may be more disciplined in nature. They are likely to value individualism but also place value on being part of a unique network such as a cyber command.

Military culture generally has high levels of power distance. Authority in the military is absolute and thus integration of cyber culture with military culture is more of a leadership challenge to motivate esprit de corps and unity through the effort of looking at the strengths of both cultures; and then focusing that effort on the cyber operation at hand. Military culture usually exhibits high levels of uncertainty avoidance due to strict processes that are followed. These rigid processes will clash with tactics and techniques required for cyber operations. The military uses logical thinking based on facts to solve problems and thus tend to have a shorter term orientation. Aggressive impulse control is enforced by a stern approach in conventional military culture due to desire to maintain the aim or focus of main effort of the operation. Masculine practices is usually apparent in the training processes of the military and often involves harsh mental physical and verbal treatment of recruits. However, feminine aspects appear at later stages of training when the training process acquire a more nurturing aspect (Kovach, 2015).

The military has to address the gap between these two cultures to create an environment in which cyber specialists and cyber warriors can thrive. Traditionally, military decision making is a slow process. The application of traditional military thinking in cyber is likely to lead to incorrect conclusions regarding strategic achievements and abilities in the pre-conflict stage, increasing the risk of strategic failure in actual conflict (Kallberg & Cook, 2017). The consequence of training and education of military officers based on traditional military theories is a military that is unable to adapt. Cyber is an ever-evolving battlefield that changes very fast and allows a very short time frame for human decision making. Kallberg and Cook questions whether future cyber conflicts execute too quickly for involvement of leadership at any level other than the lowest and most tactical.

In the context of cybersecurity, users have certain perceptions that can either positively or negatively impact the security process. It is especially cybersecurity misbehaviour that has a negative impact on cybersecurity culture. Resistance to cybersecurity measures can compromise the effectiveness of the security level and have an impact on a national level in the military context (Gcaza, von Solms, Grobler & Jansen van Vuuren, 2017). Cybersecurity is much larger than only cybersecurity awareness. Users with an advanced level of knowledge may still act in an insecure manner, despite knowing the theory. Milazzani and Sarcia (2011) note that information leakage from military networks can have a dire effect on deployed troops. They also found that military planners underestimate the potential for leaks from deployed networks; especially within the Operational Security (OPSEC) environment with respect to social media applications and the use of mobile devices.

Another feature of the culture gap is the generation gap. Cyber specialists and cyber warriors in the military tend to be much younger than their superiors. The term generation gap refers to the cultural and normative attitudes between the generations that cause friction and misunderstandings: on the one hand cyber requires one to be dynamic and keep up

to speed whilst on the other hand, there is a need to maintain continuity, predictability and preserve traditions. Roislien (2015) investigated the generation gap and stated that: "the focus is on the cyber officers' conceptualization of 'cyber' and how this resonates with that of their superiors". As part of her study she conducted interviews with students between the ages of 20 and 23 at the Norwegian Defence Cyber Academy. Most of these recruits are from "Generation Y", born in the late 1980s or early 1990s. Generation Y is recognised for its individualism, its disregard for existing maxims and an ease of familiarity with technology. Generation Y relates to tech in a way their superiors will never be able to. Roislien notes that these recruits exposed a clash with the conformity of the military system. Cyber has always existed for Generation Y, but older generations may feel less comfortable with and have less trust in cyber. These younger cyber officers are expected to excel in their cyber competence but at the same time adhere to superiors who has less knowledge in this field. Their conceptualisation of cyber is very different from their superiors. A recruit from the Roislien study remarked:

> *"They use the term 'cyber' in a way that… they toss it around as if it's some magic powder. As if adding 'cyber' to something makes it more complex or more interesting, when in fact they remove all meaning from the word by doing so. Now 'cyber' means nothing, as I see it."*

Roislien (2015) found that the recruits separated cyber competence from military competence. They also saw no significance to trying to compare cyber as it used to be to the current state, nor to try to explain cyber in terms of physical things (e.g. "imaginary wires"). She concludes that the differences in narrative and understanding leads to friction and doubts in terms of competence. However, she also states that one should not believe the problem is merely a question of difference in age and generations. The dilemma of how to turn cyber recruits into soldiers and incorporate them in the chain of command is complex.

There is no such thing as a digital only war. It is therefore not accurate to assume that cyber war is a war fought only in the cyber domain, only between cyber elements. It is therefore imperative that the gap between traditional military culture and cyber culture is substantially reduced in order to ensure the effective deployment of cyber operations. To suit this broader context of cyber warfare and cyber operations, security solutions with a greater scope than purely cyber focused is required.

5. Enabling cyber culture within the military context

One of the main changes required to operationalise military cyber operations is a culture change to accommodate cyber warriors and cyber specialists as part of the force. In addressing the cultural gap between cyber and military forces, it becomes necessary to combine the two disciplines to obtain a richer set of cultural values. According to Myers (2017) a hybrid culture is still being formed for cyber operations: "a strange intersection where a well-defined military culture of order and discipline meets hacker culture that, while not as disciplined focused, values curiosity, creativity, and intellectual challenges".

A number of actions and changes need to take place to enable a military cyber culture: force-wide cyber awareness, cultivating an appropriate culture and vales for cyber units and collaboration between the military and industry.

5.1. Force-wide cyber awareness

To counter the human factor as the weakest link within security, researchers suggest the fostering of a culture of a force wide cybersecurity culture. A cybersecurity culture includes all the socio-cultural measures that support technical security methods, so that cyber actions becomes a natural aspect of the daily activity (Reid and Van Niekerk, 2014) of every cyber warrior, cyber specialist and soldier in the military. Schwarz (2009) notes the importance of ensuring that every soldier is cyber aware. Every soldier should be cyber aware up to the extent of not exposing the force to cyber threats due to unsafe cyber behavior and should thus receive basic cybersecurity training. Many military forces are incorporating mandatory cyber courses – e.g. CyberWorx (US Air Force) (Goldstein, 2017).

A cybersecurity culture should reflect on the social, cultural and ethical aspects of the users in order to alter the users' overall cybersecurity behavior. Furthermore, a culture can only be established over time, and it would be evident in the behaviour of the users (Schlienger and Teufel, 2002). Although processes and technologies can be created to be theoretically secure, how truly secure they are depends on the people involved in their use and implementation (Reid and van Niekerk, 2014). Cybersecurity practices can mitigate cyber risks but not completely negate them. Cultivating a cyber culture is crucial to alter the behaviour of users and to instill a certain way to behave naturally in a manner that subscribes to certain security assumptions (Gcaza et al., 2017).

The recommendation is that a military force should take concrete steps to educate all members about cybersecurity and the necessity and role of special cyber units. All soldiers should understand why the special cyber units (and cyber warriors) need and have a different culture so that they perceived to be of value and accepted as part of the military.

5.2. *Cultivate an appropriate culture and values for Cyber Units*

A subculture forms when a group is stable (Schein, 1985). In order to cultivate a suitable culture these units need artifacts (visible structures and processes), to develop values and beliefs (strategies, goals and philosophies) which can lead to underlying assumptions (taken for granted beliefs, habits of thought and feeling) over time. If these levels of culture are all present new members can be socialized upon entering the group. Care should thus be taken with initial establishment, recruitment and leadership.

New doctrine, procedures, training and structures

Ducheine and van Haaster (2014) note that cyber operations require doctrinal and operational preparation. The unique challenges and opportunities posed by cyber operations also necessitates training and education, as well as motivated and focused personnel. An assessment and understanding of the potential contribution of cyber operations and cyber capacities to instruments of state power, fighting power and military operations is required. However, for this to happen, military planners should have a working knowledge of the interrelated dimensions of cyberspace in order to comprehend the links between social, technical and (military) operational processes. Other authors (Harris, 2016; Kern, 2015) also highlight the lack of an encompassing doctrine for cyber operations. Young (2010) found that the majority of soldiers, sailors, airmen and marines continue to see cyber operations only as an element to be governed by the information operations doctrine of their Service. In addition, each Service implements different organisational structures and speak with different voices on their visions of the role of cyber power.

Retention, career growth and leadership

Specialised cyber career paths and cyber units can address cultural and retention problems. These units may need flexibility in terms of dress code, discipline, recruitment and remuneration. They will benefit from a lesser hierarchical structure and lesser authoritative leadership styles than the more traditional military units (Goldstein, 2017). It may be necessary to train cadets on how to deal with a commanding officer that is resistant to new ideas. According to Harris (2016) a new generation of leadership that has a base knowledge of the technical aspects of cyber work force skills is essential for effective cyber operations. Traditional leaders are unable to converse in a meaningful way with skilled cyber operators. Roislien (2015) discusses the inability of the current leadership to engage with cyber operators and the need for institutional changes. Both authors mention that conversations between current leadership and cyber operators tend to revolve around the use of jargon. Chezem (2015) recommends a study to be done on the culture of effective cyber organisations. Studies should be conducted on incentives for cyber operators to join and stay in the military.

Innovation

Military cyber units need an open innovation process to leverage innovation from civil sector and adversaries. Harris (2016) mentions rigid organisational structures as another stumbling block for some forces. Russia is a counter example in that they managed to seamlessly converge information operations, electronic and network warfare in both digital and physical operation to succeed in the Ukraine. Myers (2017), previously a Cyberspace Operations Officer in the US Airforce, is the co-founder of a cybersecurity startup. He recommends cyber units should act more like startups to try and keep up with the benefits offered by the industry, and that the initial recruits for a cyber unit should be experts in their fields so that they will be able to tackle the challenges. Innovation education can also be offered.

5.3 Collaboration between the military and industry

McCaney (2016) notes the necessity of collaboration between the military and industry. Trust for sharing information between private industries, research, government and the military can be established through structures such as Cybersecurity Centres and non-disclosure agreements. This means collaboration on education, training and exercises.

7. Conclusion

This paper considers the requirements for military forces to operationalise cyber operations. One of the main obstacles to overcome is the cultural gap that exists between a cyber culture and traditional military culture. Addressing this gap is necessary to provide cyber warriors and cyber specialists with an environment in which they can excel. A cybersecurity culture should also be cultivated force wide: every soldier needs to be cybersecurity aware and have basic cybersecurity knowledge.

Other considerations are gaining an understanding of the nature and impact of cyber operations, developing new doctrine and policies to reflect this understanding, creating career paths for cyber specialists and cyber warriors which include specialised units and appropriate leadership, developing incentives for the retention of cyber operators, and enhancing collaboration with the private sector. In short, the military will have to adapt to accommodate and integrate cyber. There may be resistance to these adaptations from the military in general.

The views and opinions expressed in this article are those of the authors and do not necessarily reflect the position of any agency.

8. References

CarBerry, S. D. (2017). "New Cyber Warriors Face Culture Shock", [online] FWC Magazine. https://fcw.com/articles/2017/03/24/cyber-forces-carberry.aspx. March 24, 2017.

Chezem, J. (2015). "Air Force Cyber Mission Success Depends on Cultural Change", [online] Signal http://www.afcea.org/content/?q=Article-air-force-cyber-mission-success-depends-cultural-change October 1, 2015.

Choucri, N. and Goldsmith, D. (2012). "Lost in Cyberspace: Harnessing the Internet, international relations, and global security", [online] Bulletin of the Atomic Scientists, Vol 68, No.2.

Da Veiga, A. (2016). "A cyber security culture research philosophy and approach to develop a valid and reliable measuring instrument", SAI Computing Conference, IEEE. London. p. 10.

Ducheine, P.A.L., and van Haaster, J. (2014). "Fighting Power, Targeting and Cyber Operations", [online], Amsterdam Center for International Law (ACIL) Research paper 2014-04. http://ssrn.com/abstract=2392373.

Garamone, Jim. (n.d.). "Cybercom Chief Discusses Importance of Cyber Operations", DoD News, Defense Media Activity. https://www.defense.gov/News/Article/Article/604453/cybercom-chief-discusses-importance-of-cyber-operations/ Acc: Jul 2017.

Gcaza, N., von Solms, R., Grobler, M.M. and Jansen van Vuuren, J. (2017). "A general morphological analysis: delineating a cyber-security culture". *Information & Computer Security*, Vol. 25 Issue: 3, pp.259-278, https://doi.org/10.1108/ICS-12-2015-0046.

Goldstein, Phil. (2017). "The Military Might Need to Change its Culture for Younger Cyberwarriors" [online] FedTech https://fedtechmagazine.com/article/2017/04/military-might-need-change-its-culture-younger-cyberwarriors 13 April 2017.

Grobler, M., and Swart I. (2014). "On the probability of predicting and mapping traditional warfare measurements to the cyber warfare domain". 11th Human Choice and Computers International Conference in Finland, July/August 2014.

Harris, R.D. (2016). "Army Braces for a Culture Clash", Signal https://www.afcea.org/content/?q=Article-army-braces-culture-clash 1 January 2016.

Herskovits, M. J. (1948). "The contribution of Afroamerican studies to Africanist research", *American Anthropologist*, Vol. 50, No. 1, pp. 1-10.

Hofstede, G. (1980). Culture and organizations. International Studies of Management & Organization, 10(4), 15-41.

Hofstede, G. (2011). "Dimensionalizing Cultures: The Hofstede Model in Context", [online] *Readings in Psychology and Culture*, Vol. 21, No. 1. https://doi.org/10.9707/2307-0919.1014

Kallberg, J. and Cook, T.S. (2017). "The Unfitness of Traditional Military Thinking in Cyber", *IEEE Access*. Vol 5, pp. 8126 – 8130.

Kern, S.C.G. (2015). "Expanding Combat Power Through Military Cyber Power Theory", *Journal Force Quarterly*, 4th Quarter, 88-95.

Kovach, C. (2015). “How important are Masculinity and Feminity in the Cultures of Militaries?”, [online] *Interstate – Journal of International Affairs*, Vol. 2015/2016, No. 1. http://www.inquiriesjournal.com/articles/1235/how-important-are-masculinity-and-femininity-in-the-culture-of-militaries

Kuehl, D.T. (2009). *Cyberpower and National Security*, Potomac Books and National Defense University, Chapter from Cyberspace to Cyberpower: Defining the Problem, pp. 24-42.

Liles, S., Dietz, J.E., Rogers, M. and Larson, D. (2012). “Applying traditional military principles to cyber warfare”, 4th International Conference on Cyber Conflict (CYCON). 5-8 June 2012. http://ieeexplore.ieee.org/document/6243973/

McCaney, K. (2016). “Halvorsen: Cyber war is a culture clash”, [online] Defence Systems.https://defensesystems.com/articles/2016/04/22/halvorsen-dod-industry-culture-change.aspx

Myers, J. (2017). “Bridging Startups and Military Cyber Cultures Part I: A Startup Chief Technical Officer Reflects on his Military Roots”. March 24, 2017. https://overthehorizonmdos.com/2017/03/24/bridging-cyber-culture/

Mulazzani, F. and Sarcia, S.A. (2011). “Cyber security on military deployed networks”, International Conference on Cyber Conflict (ICCC), 7-10 June 2011, p. 1-15. http://ieeexplore.ieee.org/xpls/icp.jsp?arnumber=5954697&tag=1

Pyburn, B. L. (2009). Application of US Special Operations Command Model to Department of Defense Cyberspace Force. Published by the Marine Corps Command and Staff Coll, Quantico, VA, USA.

Reid, R. and van Niekerk, J. (2014). “From information security to cyber security cultures”, Information Security for South Africa (ISSA) Conference, 2014.

Roislien, H.E. (2015). “When The Generation Gap Collides with Military Structure: The Case of Norwegian Cyber Officers”, *Journal of Military and Strategic Studies*. Vol 6(3).

Schein, E.H. (1985). *Organizational Culture and Leadership. A dynamic view*. San Francisco, CA:Jossey-Bass.

Schlienger, T. and Teufel, S. (2002), “Information security culture – from analysis to change”, Security in the Information Society, Springer, Berlin, pp. 191-201.

Schmitt, M.N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press. p. 258.

Schwartz, N. (2009). “Cyberspace Operations Culture Change”, [online] Anderson Airforce Base. http://www.andersen.af.mil/News/Article-Display/Article/415808/cyberspace-operations-culture-change/

Soeters, J.L. (1997). “Value Orientations in Military Academies: A thirteen Country Study”, *Armed Forces & Society*, Vol. 24, No. 1, Fall 1997, pp.7-32.

Soeters J.L., Winslow D.J. and Weibull, A. (2006). *Military Culture*. In: Caforio G. (eds) Handbook of the Sociology of the Military. Springer, Boston, MA pp 237-254

Technopedia. (n.d.) “Cyber-warrior”, Retrieved January, 2015 [online]. https://www.techopedia.com/definition/28615/cyber-warrior

Young, M.D. (2010). “National Cyber Doctrine: The Missing Link in the Application of American Cyber Power”, *Journal of National Security Law & Policy*. Vol. 4, No. 1.

Zeltser, L. (2016). “What is an Information Security Expert?”, https://zeltser.com/what-is-an-infosec-expert/ Acc: 28 September 2017.