Framework for the Cultivation of a Military Cybersecurity Culture

L Leenen [1] and JC Jansen van Vuuren[2]

[1] University of the Western Cape and CAIR, South Africa
leenen.csir@gmail.com
[2] Tshwane University of Technology
jansenvanvuurenjc@tut.ac.za

Keywords: Cybersecurity Culture, Cyber Operations, Cyber Warrior, Military Culture.

Abstract:

Most military forces recognise the importance and the challenges of cyber as an operational domain. In addition to specialised cyber units, cyber is present in every division and arms of service as a result the military face increasing risks from cyber threats. It is thus crucial to establish and maintain a capability to ensure cybersecurity. Most organisations purchase and use technical controls to counter cyber threats, but users are considered the weakest link in maintaining cybersecurity, even if they are cyber aware. The cultivation of a cybersecurity culture has been shown to be the best approach to address human behaviour in the cyber domain. The development and fostering of an organisational cybersecurity culture is receiving increasing attention. This paper gives an overview of existing frameworks and guidelines in this regard and applies these approaches to the military environment. The military environment differs markedly from a business environment in terms of the nature of their work and traditional military culture. The paper proposes a framework for a military force to cultivate and foster a cybersecurity culture within the traditional military culture. This framework has to be tested in a military environment.

1. Introduction

Cyber has become pervasive in modern society and all organisations; alongside the many benefits cyber offer, there are also many risks and threats. Most organisations are taking measures to establish and maintain cybersecurity. These measures include technical measures as well as measures to raise cyber awareness and influence behavior of the workforce. The cultivation of a cybersecurity culture has been shown to be a primary measure to ensure cybersecurity in a nation of in an organisation (Gcaza & von Solms, 2017).

Herskovits (1948) described culture as a collective and shared sense of relatedness to the human experience. 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.

"Cyber culture" is a macro-culture that refers to the culture found amongst cyber professionals. 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". According to ENISA (European Union Agency for Network and Information Security), the "concept of Cybersecurity Culture (CSC) refers to the knowledge, beliefs, perceptions, attitudes, assumptions, norms and values of people regarding cybersecurity and how they manifest themselves in people's behavior with information technologies" (ENISA, 2017). ENISA further states that CSC includes more than cybersecurity awareness and information security frameworks; it is also concerned with making cybersecurity an integral part of an employee's job, habits and conduct. The aim of a CSC is to "instill a certain way to 'naturally behave' in daily life, a way that subscribes to certain [cybersecurity] assumptions" (Gcaza, von Solms, & Jansen van Vuuren, 2015). A CSC includes all the socio-cultural measures that support technical security methods, so that cyber actions become a natural aspect of the daily activity (Reid & van Niekerk, 2014).

The human is the weakest link in the cybersecurity chain; staff members cause the majority of data breaches in organisations ((ENISA, 2017) (Ponemon Institute, 2012)). Although processes and technologies contribute to security, in practice security depends on the people involved in their use and implementation (Reid & van Niekerk, 2014). Cultivating a CSC 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 & von Solms, 2017). It takes time to establish a cybersecurity culture and becomes evident in the behaviour of the users (Schlienger & Teufel, 2002). Cyber secure behaviour should an integral part of an employee's job, habits and conduct. Cybersecurity culture is dynamic – organisations change over time and their CSC must thus also adapt and change (ENISA, 2017).

A military force face similar threats in terms of cyberspace as any other organisation, but the establishment of cybersecurity in a military environment is even more complex. Mission assurance is vital in the military and can be adversely affected by cyber-attacks or breaches. A military force has to create an environment in which it can conduct cyber operations in addition to ensuring that every soldier is cyber aware. Traditional military culture differs markedly from cybersecurity culture. According to Soeters (Soeters, 1997) an international military culture does exist although every military force has its own organisational culture that is related to their national culture. The culture gap between traditional military culture and cybersecurity culture is often raised in the literature ((Harris, 2016) (Leenen, Aschmann, Grobler, & van Heerden, 2018)).

This paper considers existing research results on the cultivation of an organisational cybersecurity culture and results on cybersecurity in the military, and then applies these results to propose a framework to cultivate a military cybersecurity culture.

2. Cultivation of an Organisational Cybersecurity Culture

Although there is a growing interest in cybersecurity culture, the topic is still emerging and there are limited published research results available (Gcaza, von Solms, & Jansen van Vuuren, 2015). The International Telecommunications Union (ITU) identifies the creation of a cybersecurity culture as the most important contribution to ensure cybersecurity (International Telecommunication Union, 2008). One of the most important pillars of such a culture is awareness and education (Kortjan & von Solms, 2012). A Norwegian study on national cybersecurity culture determined the core issues of a (national) cybersecurity culture to be Collectivism, Governance and Control, Trust, Risk Perception, Techno-optimism and Digitalisation, Competence, Interest and Behaviours (Mlamedal & Roislien, 2016).

The Council on Digital Security Risk Management for Economic and Social Prosperity (OECD) recommended that a cybersecurity culture must be promoted to protect information systems and networks (OECD, 2015); this must include the raising of awareness about the risk to information systems and networks, and the adoption of policies, practices, measures and procedures available to address those risks. In addition, it is important to promote co-operation and information sharing, and to increase ethical issues in the development of standards. Their guidelines for the development of a cybersecurity culture include:

- The raising of **awareness** on the implementation of processes to reduce the internal and external cybersecurity risks to information systems and networks as well as the potential harm to others arising from interconnectivity and interdependency.
- Developers, designers and suppliers of products and services must be **responsible** for distribution of appropriate information to enhance understand of the security functionality of products and services and their responsibilities related to security.
- **Ethical** conduct is crucial and best practices must be adopted to recognise security needs and respects the legitimate interests of others.
- Security should be implemented consistent with **values** recognised by **democratic** societies.
- **Risk assessment** should be conducted to identify threats and vulnerabilities to guide the selection of appropriate controls to manage the risks.
- Security should be an integral part of system **design and implementation** of all products, services, systems and networks.
- **Security Management** should be based on risk assessment and should include all levels or participation.

- Security must be **reassessed** regularly.

ENISA published a guide to promote the understanding and uptake of Cybersecurity Culture programs within organisations (ENISA, 2017) based on results from different disciplines such as organisational sciences, psychology, law and cybersecurity. It includes best practices and a comprehensive CSC program that can be applied by an organisation of any size to cultivate a cybersecurity culture. It recognises that behavior in an organisation is based on shared beliefs, values and actions of the employees, which includes the employees' attitude towards cybersecurity. Cybersecurity awareness campaigns have been shown to be insufficient. Technical cybersecurity measures have to be incorporated with other business processes to allow compliance with cybersecurity policies to co-exist with job performance.

The main recommendations of the ENISA guide are:

- Acquire buy-in from the highest level in the company. Motivate the need for CSC program in the organisation by using statistics on cyber threats, providing internal evidence of cyber-attacks together with a cost calculation cost, and show results of a pilot CSC intervention.
- Consider the good practices gathered from successfully deployed CSC programs.
- Use their Implementation Framework:
    - Choose a core group from different departments and a champion at a higher level. The involvement of senior staff members is crucial, and they need to back up the CSC program by providing resources.
    - Develop an understanding of the organisational culture and business processes and do a risk assessment of possible misalignments. Employees must be engaged so that they do not feel the program is imposed upon them.
    - Define main goals, success criteria and identify target audiences. Some goals will be organisation-wide while others will only be relevant to a group.
    - Determine the current cybersecurity status and do a gap analysis with the aimed-for situation.
    - Select and execute activities.
    - Measure the cybersecurity status after the activities were executed and analyse the results.
    - Review your program and consider results before deciding on the next action. A CSC program is a continuous process that needs constant revision.

Steve Martino, Chief Information Security Officer at CISCO, stressed how important it is for employees to understand that their role is crucial to protect the company from cybersecurity threats. He also advises to improve cybersecurity culture by educating employees, testing them and make them accountable. (Veltsos, 2017). It is difficult to create a metric to gauge the maturity level of a cybersecurity culture. The term CSC is a concept developed amongst businesses that know what cybersecurity is (Mlamedal & Roislien, 2016) but this is not necessarily the case for other business and the average citizen.

3. Cyber in the Military

The culture gap between traditional military culture and a cybersecurity culture becomes apparent and problematic when cyber specialists are incorporated into the military. Leenen et al. (Leenen, Aschmann, Grobler, & van Heerden, 2018) discuss how this cultural gap can be bridged in terms of the cultivation of a cybersecurity culture and values for specialised cyber units in addition to a force-wide cybersecurity culture.

The US Air Force commissioned the RAND corporation to develop policy, process governance and make recommendations to improve mission assurance of military systems throughout their life cycle in terms of cybersecurity (Snyder, Powers, Bodine-Baron, Fox, Kendrick, & Powell, 2015). This study provides valuable insight in how cybersecurity manifest in military systems in ways that differ from the business sector. The main findings were:

- Cybersecurity processes and governance are designed for simpler, and more stable and predictable environments than the military environment, and usually include centralised control executed through standardised and formalised work rules. Due to the difficulty to predict future cyber threats these designs will be unlikely to cope with all possible vulnerabilities in the complex military systems. The adversary only needs to find one vulnerability while the military has to operate through any plausible attack. In addition, the focus of cybersecurity processes and controls were geared towards tactical security controls with limited focus on strategic mission assurance.

- The implementation of cybersecurity was not geared towards the life cycle of a military system. This introduces vulnerabilities for systems beyond the procurement phase and is weak in terms of cybersecurity across program boundaries.
- Control and accountability from military cybersecurity are spread over numerous division and units and poorly integrated. The overlapping roles created uncertainty in decision authority and accountability.
- Monitoring and feedback were incomplete and uncoordinated, and thus inefficient. The feedback did not a capture all systems and the format was not suitable for informed decision-making. This weakness inhibits individual accountability.

Some of the recommendations made by the RAND study are (Snyder, Powers, Bodine-Baron, Fox, Kendrick, & Powell, 2015):

- Construct a succinct, outcome-oriented objective for cybersecurity that applies to all systems throughout their lifecycle.
- Roles and responsibilities should be realigned to balance the risks of vulnerabilities and threats to systems and mission impact.
- Adopt a policy that encourages required security controls to be supplemented with cybersecurity measures.
- Centralise cybersecurity strategies and objectives but decentralise decisions on the implementation thereof in order to encourage innovation and adaptation.
- Strife for simplicity in design of the cybersecurity policy on connecting different systems; this can be done by prescribing what is allowed to be connected to what in cyberspace.
- Create a group of cybersecurity experts that can support the whole enterprise.
- Produce regular, continuous cybersecurity assessments of every program in the force.
- Create cybersecurity red teams.
- Hold individuals responsible for infractions of cybersecurity policies. Over time, meaningful monitoring systems should be built, and appropriate disciplinary actions should be introduced.
- Develop mission thread data to assess acceptable risks caused by cybersecurity deficiencies in systems.

The USA's initiated the DOD Cybersecurity Culture and Compliance Initiative in 2015 (US DOD, 2015). This initiative was launched due to tangible mission risks resulting from poor individual cyber behaviours and the ease with which the harm of intrusion enabled by human error are underestimated. It is an acknowledgement that technical measures are not sufficient to attain cybersecurity. The following five operational excellence principals for cyber operations in the military are as follows:

- **Integrity**: diligence in following cybersecurity best practices and reporting mistakes to the chain of command.
- **Level of knowledge** enables all the other principles. Every member must have a fundamental understanding of network connections to mission systems, suspicious behaviours, how networks are vulnerable and can be penetrated, and the consequences of unauthorised intrusions. Cyber professionals must be well trained and certified.
- **Procedural Compliance**: following the proper procedures without taking shortcuts.
- **Formality and Backup**: Improving resilience and voiding complacency and misunderstandings. Providing technology enabled oversight and two-person integrity for high-risk procedures.
- **A questioning attitude** is empowered by knowledge. Act on warning signals or a feeling that something is not right, and interpret what you observe.

The DOD recommends that each of the different populations that use DOD networks and mission systems must be accounted for in a strong cybersecurity culture in terms of their particular needs, vulnerabilities, risk profiles and expectations associated with cybersecurity discipline. They classify the different populations as leaders, providers, cyber warriors and users.

Also consider the generational gap that exists between the (generally) younger cyber operators and their superiors in the military (Roislien, 2015). Senior officers often have less knowledge regarding cyber than their underlings. This may cause a lack of confidence from the younger members towards their superiors in cyber units. A CSC can consider this gap by tailoring different awareness activities for less tech-savvy staff.

4. A Framework for a Cultivating a Military Cybersecurity Culture

In this section, we present a framework for establishing and running a CSC program in the military.

Table 1: A Framework for a Military CSC Program

Preparation Phase	**Design Phase**	**Execution Phase**
a: Cybersecurity strategy and policies must be in place	***1***: Set up the core CSC task team	***i***: Run awareness and educational campaigns
b: Cyber specialists must be well trained and certified	***2***: Define main goals, success criteria and target groups	***ii***: Run cybersecurity exercises
c: Understand current culture and processes, and access the risks	***3***: Identify roles and responsibilities	***iii***: Measure the success of the exercises
d: : Set up an initial baseline, i.e. the current behaviours	***4***: Identify supporting divisions	***iv***: Return to Step 6.
e: Run a pilot activity and measure the impact	***5***: Design cybersecurity exercises and identify metrics	
f: Get buy-in from upper level command	***6***: Review and update the program	

4.1 Preparation Phase

Step a: Cybersecurity Strategy and Policies must be in place

The CSC program aims to foster a culture where cybersecurity policies and knowledge become instilled in force members; it does not replace the accepted governance and best practices prescribed by the cybersecurity strategy and policies. ICT support services must have a policy to describe the distribution of appropriate information including updates in a timely manner to enhance user understanding. Policies must include best practices that describe ethical conduct and values. Security Management based on risk assessment and inclusion of all levels and participation should address prevention, detection and response to incidents, systems recovery, on-going maintenance, review and audit. Information system and network security policies, Practices, measures and procedures should be co-ordinated and integrated to create a coherent system of security.

Step b: Cyber specialists must be well trained and certified

Similarly, to any business, a military force must have network and other cybersecurity professionals to maintain and protect systems.

Step c: Understand current culture and processes, and access the risks

Interact with force members to determine the existing cultures in the force and in different units and divisions. Risk assessment should be conducted to identify threats and vulnerabilities to guide the selection of appropriate controls to manage the risks. This will identify where there may be misalignments between existing practices and processes and security measures. Misalignments may require engagements to ensure understanding for the security measures and compromise to find resolutions that will ensure commitment from the units and divisions.

Step d: Set up an initial baseline, i.e. the current behaviours

Set up an initial baseline of the current maturity level of the cybersecurity culture by employing appropriate metrics. The Payment Cards Industry (PCI Security Standards Council, 2014) provides examples of metrics for various CS awareness activities. The baseline will be refined and used for the measurement of the impact of the CSC program.

Step e: Run a pilot CSC activity and measure the impact

Run a small-scale test program using limited resources. Select one target unit and a single behaviour. After the exercise, measure changes in the selected behaviour against the initial baseline to show the impact. For example, the activity can support the targeted group to use a password storage app instead of storing personal passwords in a plain text or hand-written format. It is easy to measure the improvement in this specific behaviour.

Step f: Get buy-in from the upper level command

It is crucial to provide a strong motivation to convince the upper level of command in the military to support and fund a force-wide CSC program. Such a program require resources, funding and a dedicated team to run the program and adapt it over time. Incorporate three sources of evidence:

- Statistics on current cyber treats including statistics relating to military forces. Include global, national and regional statistics.
- Collect evidence of cyber-attacks drawn from the cybersecurity personnel in different units and the IT support units.
- Present the results from the pilot activity.
- Present estimates of the monetary impact of cyber-attacks and breaches, the possible impact on missions and the loss of reputation and trust in the military. Ultimately, a lack of cybersecurity can have an impact on national security.

4.2 Design Phase

Step 1: Set up a core CSC task team

The core task group is responsible for the development, implementation and maintenance of the CSC program and must represent a cross-section of the force and include members of different arms of service and units. The members of the core group must understand the current group cultures in the different units and the mandates of the units. One CSC program will not be flexible enough to cater for every unit; the main CSC program should allow for adaptation to individual groups' requirements to be relevant. Every subgroup in the force must feel included in the design of the program. The core group must be mandated and supported by the high-level command to formulate CSC policy and strategy and to oversee the implementation and execution of the program. Allow different divisions and units to give inputs and feedback on the implementation of cybersecurity implementation in their group so that they can use their internal expertise and be innovative.

Step 2: Define main goals, success criteria and target groups

Define the main goals of the CSC program and prioritise the most important issues and the success criteria and target groups. Snyder et al. (2015) suggest "to keep the impact of adversary cyber exploitation and offensive to an acceptable level as guided by a standardized process for assessing risk to mission assurance" as a goal. Aim to foster a CSC where every member has a role and a responsibility in cybersecurity.

Identify criteria of success to measure the success of the program at this early stage. Certain behaviours are easy to measure, for example, how many users click on unsafe links in phishing emails. It is important to be able to measure the actual state of cybersecurity and the mission impact and not just compliance with the directives; performance outcomes are critical. However, culture is more than just behaviours; it also has to do with values, attitudes and perceptions about cybersecurity and these dimensions of culture are more complex to measure. A Norwegian study on a national CSC (Mlamedal & Roislien, 2016) motivates the identification of a robust set of indicators that also reflect the beliefs, values and attitudes, enables the creation of an appropriate baseline for the measurement of a CSC.

Actors should also be held appropriately accountable (Snyder, Powers, Bodine-Baron, Fox, Kendrick, & Powell, 2015). Create a vehicle for a free exchange of cybersecurity information and solutions among workers. All members of the force must receive basic cybersecurity training.

The identification of target groups is more complex than it is for the average business because the military consists of many different divisions, units and arms of service. Each of these internal institutions has their own organisational culture and often their own ingrained way of going about their business. A CSC cannot be enforced on a group; it is cultivated and accepted over a period, and it must be adapted to fit the target group. Examples of different target groups are the Commanding Officers, IT providers and cybersecurity professionals, cyber units (i.e. cyber warriors) and other members of the force. Take note of special requirements for the different divisions (Personnel, Intelligence, Operations, Logistics, Finance, and Planning) and Arms of Service (Army, Navy, Air Force and Medical Service).

Step 3: Identify roles and responsibilities of force members

Determine roles for cybersecurity – a role-based approach provides a reference for training force members at appropriate levels in their job functions. A reference catalogue of different types and depths of training will help the delivery of the right training to the right people (PCI Security Standards Council, 2014). Assign responsibility for the integration and balancing of the assessments of risk posed by system vulnerabilities, threats to systems and impacts on missions to an officer. Ensure that security controls for programs are supplemented with cybersecurity measures.

The following figure is an adaptation and extension from a figure that appeared in the PCI report.

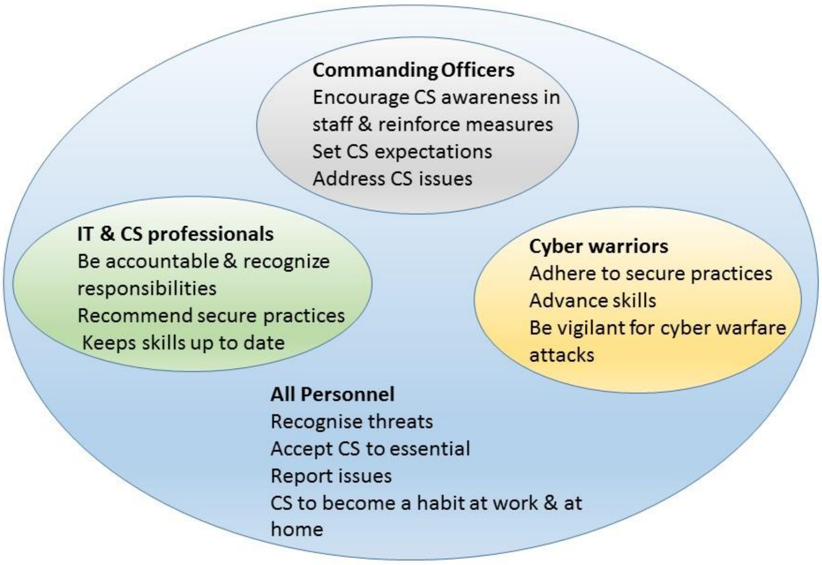
Commanding Officers
Encourage CS awareness in staff & reinforce measures
Set CS expectations
Address CS issues
IT & CS professionals
Be accountable & recognize responsibilities
Recommend secure practices
Keeps skills up to date
Cyber warriors
Adhere to secure practices
Advance skills
Be vigilant for cyber warfare attacks
All Personnel
Recognise threats
Accept CS to essential
Report issues
CS to become a habit at work & at home

Figure 1: Cybersecurity (CS) Roles Awareness for the Military

Step 4: Identify supporting divisions

Enlist the assistance of the IT providers, and divisions such as Personnel, Finance and others that can support the execution of the CSC activities. Commanders and leaders at every level should actively encourage personnel to participate in the program. Cybersecurity behaviour metrics should be included into performance reviews.

Step 5: Design cybersecurity exercises and identify metrics

Detailed planning for suitable exercises for the different target groups can now take place. Use diverse platforms for the delivery of information such as videos, instructor-led training, quizzes, games, email, internal social media etc. Communicate activities to the target groups on a regular basis, especially so that the participants understand why the program is important. The CSC core team has to consider the integration of the exercise activities across the different target groups such that they all support the main goal. Identify one or more metrics for each exercise. The PCI report contains examples of operational and training program metrics (PCI Security Standards Council, 2014).

Customise exercises for the higher-ranking force members to focus on policies. In addition, incorporate activities geared for staff with a high level of ICT knowledge and competence, and for members with little or no technical knowledge. Note that there will be overlaps in the target groups and those members should receive the opportunity to belong to more than one target group.

An example of an exercise for the senior staff members is to organise a strategic game scenario based on a fictional military operation. Divide the group into opposing teams and include cyber incidents to interfere with the game play, for example, a loss of connectivity that interrupts the communication channel. The cyber incidents should be accompanied by information on cybersecurity risks and the presence of cybersecurity experts to facilitate the game play. An interesting exercise is to create a *Wall of Shame* at a gathering of staff. A *Wall of Shame* illustrates how random connections to a mobile hotspot can pose risks due to data leakages from mobile phones. Participants should not be made aware of the exercise but be presented with the result afterwards. The results should be anonymous to protect privacy. Quizzes and physical activities, for example, a cybersecurity themed obstacle course, are usually fun for the participants. The hosting of exercises during Cyber Security Month (usually in October) or a special Show Day (with various activities and presentation at different stands) can be aimed at reaching a large number of participants.

Develop Best Practices to encourage military forces to adopt practices aimed at promoting secure online behaviour throughout the wider military community, and distribute low-cost tools to help soldiers to prevent and detect online threats.

Step 6: Review and update the program

The CSC program has to be maintained and updated. Culture is dynamic and CSC programs should become ingrained as part of continued training of personnel. To behave in a cyber-secure manner should be just as important as other safety and security behaviours that are drilled into member of military forces. Security must be reassessed regularly to make modifications to security policies, practices and procedures to make provision for new and changing threats and vulnerabilities that are continuously discovered. Measurements must also be updated accordingly and the baseline should be reviewed and updated.

4.3 Execution Phase

Step i: Run Awareness and Educational Campaigns

In addition to technical, administrative and procedural measures to protect computer systems, education and awareness for force members are essential elements for a cybersecurity culture. Educational campaigns for targeted groups as identified in the design phase must be organised to raise awareness on cybersecurity issues (Usmani & Appayya, 2017). Deliver these campaigns in a timely and efficient manner, using a communication medium that is appropriate to the target group.

Step ii: Run Cybersecurity Exercises

The focus of these exercises is to evaluate the preparedness of military units and support structures to deal with cyber-attacks. They can be online exercises for individuals or in the form of cybersecurity drills. Exercises are also an effective way to measure the level collaboration and information sharing between the different military units and will contribute to capacity building. They should ideally run annually.

Step iii: Measure the success of the exercises

For example, if an activity's aim was to make participants aware of the importance of logging out of workstations when they leave an office, the baseline will be the number of workstations that were open in the absence of the user (physical inspection) before the activity. The current behaviour can be determined by a similar count after the activity was run.

Step iv: Return to Step 6.

5. Conclusion

An organisational cybersecurity culture is crucial for any organisation to ensure a cyber-secure environment. Although there are some guidelines and best practices for cultivating national and organisational cybersecurity cultures, limited attention is paid to the cultivation of military cybersecurity culture in the literature. The military environment differs markedly from a business environment in terms of the nature of their work and traditional military culture. The paper proposes a framework for a military force to cultivate and foster a cybersecurity culture within the traditional military culture. This framework has to be tested in a military environment.

6. References

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.

ENISA. (2017). *Cyber Security Culture in Organisations.* European Agency for Network and Information Security.

Gcaza, N., & von Solms, R. (2017). Cybersecurity Culture: An ill-defined problem. *IFIP World Conference on Information Security Education (WISE 2017)*, pp. 98-109.

Gcaza, N., von Solms, R., & Jansen van Vuuren, J. (2015). An Ontology for a National Cybersceurity Culture Environment. *The Nineth International Symposium on Human Aspects of Information Security and Assurance (HAISA 201)*, pp. 1-10.

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 , 50* (1), pp. 1-10.

International Telecommunication Union. (2008). *Global Security Report.* https://www.itu.int/osg/csd/stratplan/AR2008_web.pdf.

Kortjan, N., & von Solms, R. (2012). Fostering a cyber security culture: a case of South Africa. In A. Koch, & P. van Brakel (Ed.), *14th Annual Conference on World Wide Web Applications.*

Leenen, L., Aschmann, M., Grobler, M., & van Heerden, A. (2018). Facing the Culture Gap in Operationalising Cyber within a Military Context. *The 13-th International Conference on Cyber Warfare and Security (ICCWS 2018).* Washington D.C., USA.

Mlamedal, B., & Roislien, H. (2016). *The Norwegian Cyber Security Culture.* Norwegian Centre for Information Security (NorSIS).

OECD. (2015). Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity.

PCI Security Standards Council. (2014). *Best Practices for Implementing a Security Awareness Program.* Security Standars Council (PCI), Security Awareness Program Special Interest Group.

Ponemon Institute. (2012). *The Human Factor in Data Protection.*

Reid, R., & van Niekerk, J. (2014). Towards an Education Campaign for Forstering a Societal Cyber Secure Culture. *The Eighth International Symposium in Human Aspects of Information Security and Assurance (HAISA)*, pp. 174-184.

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

Schein, E. (1985). *Organizational Culture and Leadership. A dynamic view.* San Francisco: :Jossey-Bass.
Harris, R. (2016, January a). *Army Braces for a Culture Clash*. From Signal: https://www.afcea.org/content/?q=Article-army-braces-culture-clash

Schlienger, T., & Teufel, S. (2002). Information Security Culture - from analysis to change. In *In Security in the Information Society* pp. 191-201.

Snyder, D., Powers, J., Bodine-Baron, W., Fox, B., Kendrick, L., & Powell, M. (2015). *Improving the Cybersecurity Of U.S. Air Force Military Systems throughout their Life Cycles.* RAND Corportaion.

Soeters, J. (1997). Value Orientations in Military Academies: A Thirteen Country Study. *Armed Forces & Society, 24* (1), pp. 7-32.

US DOD. (2015). *Department of Defense: Cybersecurity Culture and Compliance Initiative (DC3I).* Office of the Secretary of Defense.

Usmani, K. A., & Appayya, J. A. (2017, November 4). Capacity Building is the Key to Fight Against Cybercrime: The Mauritian Perspective. *Global Cyber Expertise Magazine*.

Veltsos, C. (2017, March 6). *Building a Cybersecurity Culture Around Layer 8*. From Security Intelligence: https://securityintelligence.com/building-a-cybersecurity-culture-around-layer-8/