Modern Management based on Big Data II and Machine Learning and Intelligent Systems III
A.J. Tallón-Ballesteros (Ed.)

doi:10.3233/FAIA210242

Assessment of National Cybersecurity Capacity for Countries in a Transitional Phase: The Spring Land Case Study

Mohamed Altaher Ben Naseir [a], Huseyin Dogan [a1], and Edward Apeh [a]
[a] Bournemouth University, Fern Barrow, Poole, Dorset, BH12 5BB, United Kingdom

Abstract. Cybersecurity capacity building has emerged as a notable matter for numerous jurisdictions. Cyber-related threats are posing an ever-greater risk to national security for all countries, irrespective of whether they are developed or in the midst of transitioning. This paper presents the results of two qualitative studies using the Cybersecurity Capacity Maturity Model (CCMM) for nations: (1) Interactive Management (IM) and (2) focus groups to analyse the current state of Spring Land's cybersecurity capacity. A total of 26 participants from government agencies and five national experts from the Spring Land National Cybersecurity Authority (NCSA) contributed to this study. The results show that Spring Land has many issues such as lack of cybersecurity culture and collaborative road-map across government sectors which results in instability within the country. The assessments feed into the requirement analysis of the National Cybersecurity Capacity Building Framework that can be utilised to organise and test the cybersecurity for nations.

Keywords: Cybersecurity capacity, Cybersecurity Maturity Models and Interactive Management.

1. Introduction

Over numerous decades, there have been several notable security failings that have defined the global security environment and resulted in governments being unable to preserve domestic security [1]. Maintaining national security (including cybersecurity) is the main responsibility of national governments and failing to do so contributes to the instability of a country [2]. Countries in a transition phase is typically characterised by civil war; political and economic upheaval; the absence of law [3, 4]. Transition phase refers to the intermediate phase in which a previous regime is replaced by a modern alternative [5]. There are a number of factors affecting the success or failure of transition stage. These factors include: the type of regime prior to the transition stage,

[1] Corresponding Author, Huseyin Dogan, Bournemouth University, Fern Barrow, Poole, Dorset, BH12 5BB, United Kingdom; Email: hdogan@bournemouth.ac.uk

the characteristics of the new leader of the transitional government and the influence of information and communication technologies (ICT) [6].

Many of these countries depend on cyberspace to provide daily services for their citizens using information and communication technologies (ICT). The growth of ICT technologies and applications provides an important vehicle for communication and interaction and has increasingly become common in low-income countries and countries that are in a transitional stage [7]. Access to a range of ICTs brings new opportunities for information exchange and communication but it also can also be seen as a technological and generational challenge to the hierarchical social order of many countries in the Middle East and North Africa (MENA) region. The current experience of democracy movements (the Arab Spring) in a number of MENA countries demonstrates how during times of public protest and turbulence, ICTs can be significant forces for organisation and mobilisation [7].

This paper aims to evaluate the capacity of cybersecurity in countries progressing through a phase of transition by taking Spring Land as an exemplar case study. The name 'Spring Land' has been selected to disguise the real name of the country in which the case study has been undertaken.

The assessment was undertaken by applying the Cybersecurity Capacity Maturity Model (CCMM) - V1.2, utilising the Interactive Management (IM) approach and focus group discussion method. The CCMM model was designed by the Global Cybersecurity Capacity Centre at the University of Oxford [8]. The CCMM model was nominated because it successfully demonstrates the effect that a Cybersecurity Capacity Building (CCB) approach can achieve at the worldwide level, including all aspects of cybersecurity to ensure that the platform remains resilient. This assessment has provided a great opportunity to illustrate the fact that in the current hyper connected world, states in a transitional phase are not operating in isolation and their failure in certain critical areas such as cyberspace is likely to have a ripple effect by destabilising stable states. Moreover, it will feed into the requirement analysis of the National Cybersecurity Capacity Building Framework and the possibility of organising and testing cybersecurity in these countries.

The paper is structured as follows: Section 2 discusses the related empirical research; Section 3 provides an overview on the CCMM; Section 4 presents the selected methodology and the problem of space contextualisation through the IM. The cybersecurity posture of Spring Land through the focus group discussion is presented in Section 5. Finally, Section 6 provides a conclusion and recommendations for future research in this area.

2. Cybersecurity Capacity Building (CCB)

Cybersecurity Capacity Building (CCB) is one of the greatest challenges that countries face, particularly countries in a transitional stage. These challenges are range from human resource development, institutional reform, organisational adaption, and the support provided to increase their potential to not only make use of the Internet but also realise its full potential [9, 10]. The majority of problems relate to the lack of cybersecurity culture and an inability to understand the threat posed as well as the probable consequences [11].

Furthermore, various other issues can affect decisions when building a secure cyberspace. For instance, many countries lack a legislative framework, the resources required to build what they need and secure capacities in cyberspace. Also, awareness of and education about the threats and risks associated with cyberspace are common issues in these countries. Without awareness and education, attempts to secure a system are rendered inefficient, if not useless [9, 12]. Another problem is linked to the dearth of skills among Internet users to protect themselves against rapidly emerging cyberthreats. In many developing countries and countries in a transitional period, Internet users are inexperienced and are not technically savvy.

The term 'capacity building' refers to the process of addressing an identified issue with poor governance by ensuring a suitable capability so that core functions are delivered [11]. Therefore, capacity building entails developing organisational structures (i.e. methods of management at the organisational level), human capital (i.e. addressing skills shortages and enhancing knowledge), and the frameworks that underpin legal and institutional arrangements (i.e. strategies and legislation).

However, various frameworks and guidelines have been devised by academic researchers as well as organisations operating in the country or worldwide. From these, it is apparent that five pillars support cybersecurity capacity: human, organisational, infrastructure, technology, law and regulation [13]. Such frameworks are primarily concerned with the risks to cybersecurity and the steps that can be taken to protect against them at the international level and especially in advanced economies. In addition, it is apparent from the empirical literature that there is a paucity of research focusing on emerging market countries owing to their relative shortage of human capital as well as technical capacity [14]. National governments and international organisations have recognised the threat posed by such risks but efforts to implement effective defences have not been coordinated and this disjointed approach has resulted in certain countries being much better prepared than others [15]. According to Muller [9], current efforts to address CCB have not taken a global perspective or have advocated CCB but failed to suggest how it should be implemented.

3. Cybersecurity Capacity Maturity Model for Nations (CCMM)

The CCMM was developed by the Global Cybersecurity Capacity Centre at the University of Oxford through collaboration with international stakeholders including the Organization of American States (OAS), the World Bank, the Commonwealth Telecommunications Organisation (CTO) and the International Telecommunication Union (ITU) [8]. The model offers a comprehensive analysis of cybersecurity capacity through five dimensions. These dimensions are cybersecurity strategy, Cybersecurity awareness, Cybersecurity education, training and skills, Cybersecurity legal framework and the Standards, Organisations and Technologies.

Each dimension has multiple factors which define what it means to possess a cybersecurity capacity. For each factor, there are five stages of maturity. The Start-up indicator describes a non-existent or inadequate level of capacity; the Formative level indicates that some features are formulated but poorly defined; the Established pointer shows that an element of the sub-factors are in place and defined; in the Strategic indicators level the selections of which parts of indictors are vital or less important have been made for particular institutions/nations based on certain conditions; the Dynamic indicator level is the highest level and indicates that there are clear mechanisms in

place to modify the strategy subject to the prevailing circumstance. The results of the maturity levels are graphically represented using a radar chart [8].

4. Methodology

The assessment of the national cybersecurity capacity of Spring Land utilises two qualitative approaches: Interactive Management (IM) and focus groups discussions using the CCMM for Nation states. In this study, in order to gain a more thorough understanding of the Spring Land cybersecurity posture in which the model will be applied, the authors worked alongside the Spring Land National Cybersecurity Authority (NCSA). The NCSA leads the national cybersecurity programme in Spring Land to achieve resilience in cyberspace [16]. The following sections provide more details about the methodology used in this paper and the participant's profile.

4.1. Interactive management

The IM approach relates to complicated scenarios that demand collaboration among numerous knowledgeable individuals to address the matter and suggest a plan of action based on mutual agreement instead of a majority vote[17, 18]. There are three phases in IM, the first of which is the planning phase where the scenario and scope are specified. This involves creating a formal scope and context statement, defining the state of assessment, and verifying the identities of the related actors. During the workshop phase, the participants develop a shared understanding of events [17].

There are three procedures involved in IM workshops: idea writing (IW); nominal group technique (NGT); and interpretive structural modelling (ISM) [17, 18]. IW involves the participants being presented with a question so that they can develop their thoughts in writing and only then share their ideas. During the NGT, those participating assess the matter from a holistic perspective based on what occurred during the IW process. A ranking of the various ideas is compiled on the basis of their importance. The idea statements are then used as the basis for developing objectives and an Interpretive Structural Model (ISM) so that the way in which the factors associated with the problem relate to each other is recognised. In the follow-up process, the objectives and outcomes previously arrived at are acted upon to help bring about a viable solution. The authors had selected this method because IM sessions are conducted as part of an integrated approach for dealing with the situation, and each session builds on what came before and lays the foundation for what will come after [17].

In this study, a one-day workshop was hosted by NCSA for a total of 26 participants representing various stakeholders. The information details of the participants involved in the workshop are described in the participant's profile section. The results of this approach were published at the World Conference on Information Systems and Technologies (2019) [10].

4.2. Focus group

Focus group discussions aim to explore a various opinions that people have regarding particular matters and emphasising the different thoughts that groups of people have [19]. Conducting a focus group entails people collaborating about a particular subject

matter to enable the collection of relevant data [20]. Focus groups give people the opportunity to interact with each other in a way that yields useful information and a range of opinions. The decision was taken to hold focus groups because the authors believed it would generate richer data than would otherwise be possible if selecting alternative methods. [21]. In this study, five experts from the NCSA were interviewed in one session hosted in the capital city of Spring Land.

4.3. Participant's profile

Two workshops hosted by the NCSA were conducted with a national expert from Spring Land. The IM approach was conducted with a total of 26 participants from different stakeholders, 25 males and 1 female only due to lack of gender diversity involved in cybersecurity roles. The ages of those participating were within the range of 25-55 years and they had been selected because of the contribution they make to decision-making processes. They were drawn from various areas of expertise including banking, management, defence, security, oil production, immigration, digital crime and the intelligence service.

The focus group discussion was conducted with five experts (lead practitioners) from the NCSA. The participants (Ps) in this session were chosen based on their roles within the NCSA. The participants comprised senior management of the NCSA in Spring Land, a director of the NCSA (P1), a deputy director of the NCSA (P2), the head of the national cybersecurity incidents response team (CERT) (P3), the head of awareness and general relations (P4), and the head of the internal audit office (P5). For the purposes of confidentiality, the names of the participants were not disclosed.

5. Results

5.1 Problem space contextualisation through Interactive Management

5.1.1. Ideas writing (IW) results

An IW was employed to identify matters associated with a particular trigger question, thereby enabling those participating to share opinions and brainstorm in a group setting. Those participating were assigned to one of three groups where they discussed the question and offered opinions relating to the state of Spring Land's cyber security. The selected trigger question sought to identify the cybersecurity capacity issues faced by Spring Land. The trigger question employed was: *What are the current issues of cybersecurity capacity in Spring Land?*

Once the session had concluded, each of the statements that had been made were assigned a number and categorised on the basis of the CCMM dimensions. The ideas generated by the groups in response to the question are summarised and Table 1 presents examples of the challenges of cybersecurity capacity in Spring Land.

Table 1. Examples of national cybersecurity capacity challenges of countries in transitional stage vs CCMM Dimensions[10]

D1 - Cybersecurity policy and strategy	D2 - Cyber culture and society
D1.1. Absence of a national cybersecurity strategy.	D2.1. Lack of a cybersecurity culture and the absence of an understanding of cyber-risk and its consequences in the public and private sectors as
D1.2. Unavailability of a national risk management plan and threat of cyberspace has not been identi-	

fied at the national or sector-specific level. D1.3. Deficiency of a national roadmap for a cyber defence strategy.	well as among decision-makers. D2.2. Lack of awareness-raising programmes at the governmental level. D2.3. Citizens' confidence in the use of e-government services is weak.

5.1.2. Nominal group technique (NGT) results.

The purpose of using the NGT was to produce, simplify and amend ratings for a series of objectives. Those participating chose what they believed to be the three main objectives for the various dimensions (where 1 indicates the lowest importance and 3 indicates the greatest importance). 19 of the participants cast their vote but 7 did not because of external commitments or other reasons. Figure 1 illustrates the objectives of greatest importance for the various dimensions as well as indicating how they interrelate.

5.1.3. Interpretive structural modelling (ISM) for countries in transitional stage.

The ISM approach enabled those participating to analyse how the elements resulting from the NGT process are inter-related, providing the means to address the associated complexities [22, 23]. So as to ensure that the ISM is clear, the objectives of the NGT stage were categorised on the basis of their similarities to help identify the most notable objectives of the respective dimensions. Figure 1 illustrates the ISM resulting from the objective statements and how they interact on the basis of the CCMM's dimensions.

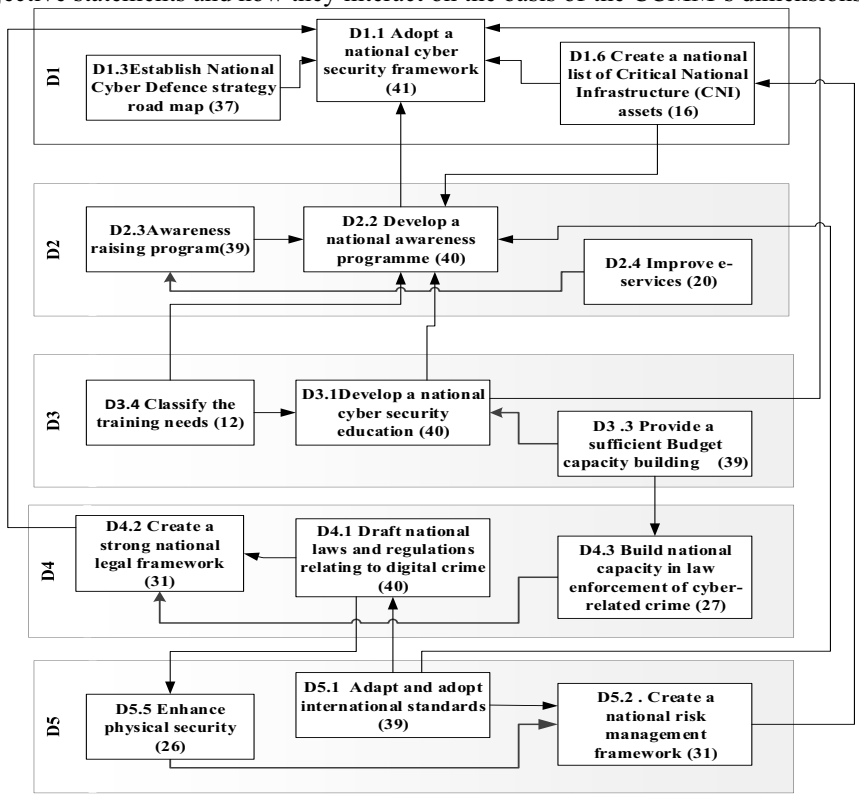

Figure 1. Interpretive structural modelling for countries in a transitional phase

It is apparent from Figure 1 that there is a need for a national blueprint owing to the fact that the existing state cyberspace interactions make clear the insufficient capacity of national cybersecurity. It can also be seen that the group believed providing a comprehensive programme to boost awareness throughout the country would help to enhance the capacity of cybersecurity at the national level. It was the group's belief that establishing a national strategy would help to initiate a process that would result in a national legal framework to enhance the sharing of information, the disclosure of susceptibilities and reporting among public sector bodies. Furthermore, it was recommended by the group that international standards (e.g., ISO27000) be adopted by government bodies so as to bolster efforts to ensure effective technical controls. In addition, it was claimed that the capacity to tackle threats (both internal and external) would benefit from improvements to physical security.

5.2 Spring Land's cybersecurity posture through focus group discussion

This section discusses the results of applying the CCMM model to assess Spring Land's cybersecurity posture using a focus group discussion approach. Five experts (lead practitioners) from the NCSA participated in this discussion, as mentioned in the participant's profile section. The cybersecurity posture of a nation state of the five dimensions of the CCMM model is presented in Figure 2 which shows the overall capacity level results using the radar chart.

5.2.1. Cybersecurity policy and strategy indicators (D1).

This dimension explores the capacity of the government to design, create, organise and implement the cybersecurity strategy. Through the discussion, this dimension was classified to be at the start-up stage in Spring Land because no national cybersecurity strategy currently exists. Therefore, NCSA has been assigned to be in charge of the cybersecurity programme.

"NCSA leads the security of information as there is no single body or group related to cybersecurity in Spring Land. In general, we can say that we are at a strategic level with a total lack of financial support because of the political situation" (P1).

NCSA created a national computer emergency response team (Spring Land - CERT) which is working only at the level of NCSA departments due to a lack of co-operation, trust, national strategy and poor awareness at the state level. *"In general, we have national accreditation to represent Spring Land in the world but there is no national plan and poor communication channels due to the fear of dealing with one another. In contrast, there is good cooperation at an international level as Spring Land is a member of different international organisations such as ITU" (P3).*

Regarding the critical national infrastructure (CNI) protection, most of the Spring Land critical systems have been destroyed and the government has not issued a list of CNI.

"*In general, physical security has a negative impact on CNI and there are no clear processes to reveal who is in charge of protecting all sectors, except the telecommunications sector" (P5).*

Furthermore, the difficult economic situation and scarcity of means in the country prevents the NCSA from raising awareness and improving national infrastructure protection.

5.2.2. Cyber culture and society indicators (D2)

Cyber culture and society at both the individual and government level are at the start-up stage in Spring Land. In the meantime, the NCSA has tried to improve the knowledge base and raise awareness of cybersecurity issues through campaigns and programmes targeted at children, their parents and university students.

"NCSA has conducted awareness activities for the government sector. As a result of these activities, NCSA reported a lack of awareness programmes in all government sectors and society" (P4).

Additionally, the NCSA has a plan to change the cybersecurity mind-set and raise awareness of the Spring Land public and national sector regarding spam, scams, phishing, information security, wireless network security and cloud computing security. The NCSA team pointed out that a lack of skilled people and cybersecurity awareness leads to more cybersecurity threats and increased cyber vulnerabilities. Despite the fact that some e-government services in Spring Land have been developed and implemented, a lack of trust and confidence in online security prevails due to there being no online protection across the majority of the government sector.

"*Spring Land has been considered as a target for e-hunting; these are hackers from inside and outside the state. These hackers are creating fake social media pages to commit frauds. There are no public key infrastructures or digital certificates to protect it" (P5*).

Due to political issues and the absence of a legislative body in Spring Land, the maturity of privacy online is considered to be at a start-up stage because no official initiatives have been issued. The exception is a certain unofficial initiative to issue laws for electronic transactions.

5.2.3. Cybersecurity education, training and skills indicators (D3)

Throughout the discussion, it has been noted that cybersecurity education, training, and skills capacity in Spring Land is at a start-up level. There are no plans at the national level to increase the efficiency of education in the field of cybersecurity.

"There are no plans at the state level to define the required educational curricula in cybersecurity" (P4).

Additionally, there are no current or future financial allocations, co-ordination or training plans between universities and the private sector regarding cybersecurity training at the state level due to a lack of interest.

5.2.4. Legal and regulatory framework indicators (D4)

This dimension looks at the government's capacity to design and develop national legislation and accompanying by-laws that directly and indirectly relate to cybersecurity. In Spring Land, the level of maturity for this dimension is considered to be at the start-up phase. There is no cyber- or ICT security-related legislation or regulations except for some initiatives by the e-Commerce Chamber of the Ministry of Economy. These initiatives face many problems, but the crucial problem is jurisdictional fragmentation due to political instability. Moreover, there is a digital crime unit in the Ministry of the Interior that deals with this type of crime by applying traditional laws relating to ordinary crimes, not cyber-related laws. Spring Land does not have any regulations or laws specifically relating to privacy, data protection or human rights.

"There are no laws related to protect systems and data" NCSA team.

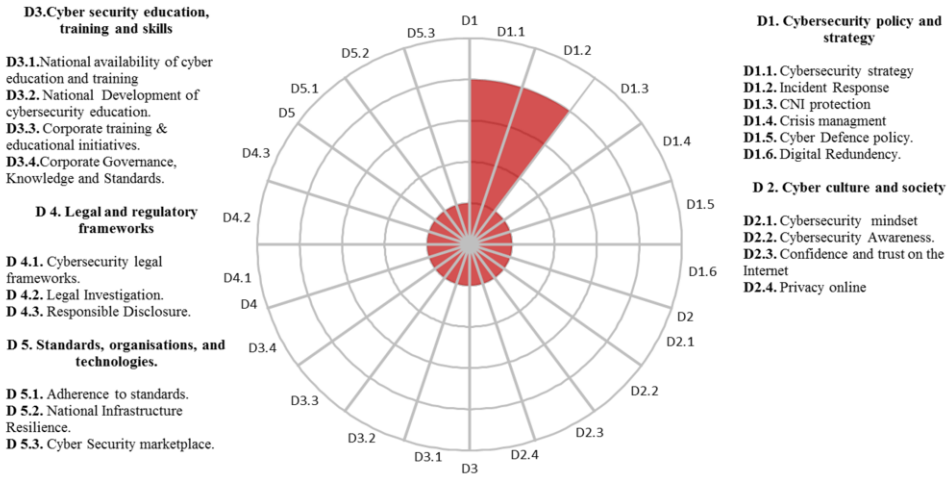

Figure 2. Results of all CCMM dimensions.

In addition, law enforcement along with the investigation and prosecution of cybercrime services in Spring Land face a shortage of skills to handle cybercrime cases. Moreover, there is no national mechanism to report or disclose cyber related crime or vulnerabilities. Also, there are no specific courts dealing with digital crime and no training is provided to build capacity in this particular dimension.

5.2.5. Standards, organisations and technology indicators (D5)

Throughout the discussion, all of the participants agreed that Spring Land is at the start-up stage in terms of this dimension. There are no cybersecurity standards that have been adapted to procurement and software development in the government sector. As explained by the NCSA team, there has been an attempt to start the process of implementing international standards but there is a shortage of skilled people and financial resources. There is no national agency or framework to monitor the implementation of standards and minimal acceptable practices in the government sector.

In addition, there is a lack of research centres in this field and poor co-operation between the public and private sectors in terms of training and the development of skills. As mentioned by the participants in the discussion of Dimension 1, not all sectors have a disaster recovery plan or a business continuity plan. All of the participants pointed out that the government does not have a plan to manage, monitor or evaluate national infrastructure resilience.

6. Conclusion and future work

The current paper has examined the core features of Spring Land's cybersecurity to demonstrate the typical situation faced by countries in transition phase and how best to address such matters. The observations help to improve our grasp of the capacity of cybersecurity in Spring Land and provide a foundation for a National Cybersecurity Capacity Framework (NCCBF) in countries that are transitioning stages. The IM approach yielded a series of problem statements and objectives that can be applied to

enhance management processes in similar cases. Be that as it may, it is apparent that additional validation is needed for the results obtained and future research should select data that will enable the results to be generalised. In addition, future research should apply the UML and IDEF0 modelling methods so that the ISM can be decomposed into functional models to develop the NCCBF. Using data from advanced countries in which the CCMM is already operational in addition to a range of practices and standards, the framework will make it possible for transitioning countries to overhaul their existing cybersecurity arrangements by initiating strategies capable of realising a desirable outcome.

References

[1] M. McCrabb, "Rough Waters," *Naval War College Review,* vol. 70, pp. 141-145, 2017.
[2] M. L. Cook, R. H. Dorff, D. Jablonsky, M. G. Roskin, R. C. Nation, G. Marcella*, et al.*, *US Army War College Guide to Strategy*: Strategic Studies Institute, 2001.
[3] DeRouen Jr, Karl Goldfinch, and Shaun, "What makes a state stable and peaceful? good governance, legitimacy and legal-rationality matter even more for low-income countries," *Civil Wars,* vol. 14, pp. 499-520, 2012.
[4] D. W. Brinkerhoff, "Rebuilding governance in failed states and post-conflict societies: core concepts and cross-cutting themes," *Public Administration and Development: The International Journal of Management Research and Practice,* vol. 25, pp. 3-14, 2005.
[5] S. Guo and G. A. Stradiotto, *Democratic transitions: Modes and outcomes*: Routledge, 2014.
[6] Strachan and Anna, "Factors affecting success or failure of political transitions," Institute of Development Studies, K4D Helpdesk Report. Brighton, UK2017.
[7] M. I. Wilson and K. E. Corey, "The role of ICT in Arab spring movements," *Netcom. Réseaux, communication et territoires,* pp. 343-356, 2012.
[8] GCSCC. (2017, 25/10/2016). *Cybersecurity Capacity Maturity Model for Nations (CMM)* Available: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20Version%201_2_0.pdf
[9] L. P. Muller, "Cyber security capacity building in developing countries: challenges and opportunities," 2015.
[10] M. A. B. Naseir, H. Dogan, E. Apeh, C. Richardson, and R. Ali, "Contextualising the National Cyber Security Capacity in an Unstable Environment: A Spring Land Case Study," in *World Conference on Information Systems and Technologies*, 2019, pp. 373-382.
[11] P. Pawlak, "Capacity building in cyberspace as an instrument of foreign policy," *Global Policy,* vol. 7, pp. 83-92, 2016.
[12] E. Tamarkin, "The AU's cybercrime response: A positive start, but substantial challenges ahead," 2015.
[13] R. Azmi, W. Tibben, and K. T. Win, "Review of cybersecurity frameworks: context and shared concepts," *Journal of Cyber Policy,* vol. 3, pp. 258-283, 2018.
[14] A. C. Tagert, "Cybersecurity challenges in developing nations," 2010.
[15] I. Atoum, A. Otoom, and A. A. Ali, "A holistic cyber security implementation framework," *Information Management & Computer Security,* 2014.
[16] NCSA. (2013). *The National Cyber Security Authority (NCSA)*
[17] Warfield, John N, and A. R. Cárdenas, *A handbook of interactive management*: Iowa State Press, 2002.
[18] F. R. Janes, "Interactive Management: Framework, Practice, and Complexity," 1995, pp. 51-60.
[19] A. Tong, P. Sainsbury, and J. Craig, "Consolidated criteria for reporting qualitative research (COREQ): a 32-item checklist for interviews and focus groups," *International journal for quality in health care,* vol. 19, pp. 349-357, 2007.
[20] O. Doody, E. Slevin, and L. Taggart, "Focus group interviews. Part 3: analysis," *British Journal of Nursing,* vol. 22, pp. 266-269 4p, 2013.
[21] J. Kitzinger, "Qualitative research: introducing focus groups," *Bmj,* vol. 311, pp. 299-302, 1995.
[22] P. Checkland, *Soft systems methodology : a 30-year retrospective ; Systems thinking, systems practice*: Chichester : John Wiley, c1999., 1999.
[23] E. Trist, "The socio-technical perspective: The evolution of socio-technical systems as a conceptual framework and as an action research paradigm," ed: New York: Wiley & Sons, 1981.