Contextualising the National Cyber Security Capacity in an Unstable Environment: a Spring Land Case Study

Mohamed Altaher Ben Naseir[1], Huseyin Dogan[1], Edward Apeh[1], Christopher Richardson[2], Raian Ali[1]
[1] Bournemouth University, UK
{mnaseir, hdogan, eapeh, rali}@bournemouth.ac.uk
[2] Digital Smart Solutions Limited, UK
christopher@digitalsmart.solutions

Abstract. Threats to global cyber security, including physical, personnel, and information, continue to evolve and spread across a hyper-connected world, irrespective of international borders, in both their elaboration and the scale of their impact. This cyber domain represents a constant challenge to national security, as its socio-technical components are both real and cognisant. The exacerbation of cyber-attacks undermines countries' stability, its escalation produces a landscape of genuine global threat, and the magnitude of its expanding attack mechanisms creates a '*tsunami effect'* on national cyber defenses. This paper reviews the current politically unstable state of Spring Land's cyber security capacity, utilising Interactive Management (IM) approach. It reports the findings of an IM session conducted during a workshop involving a total of 26 participants from the Spring Land National Cyber Security Authority (NCSA), other government agencies. The workshop utilised different IM techniques, such as Idea Writing (IW), Nominal Group Technique (NGT), and Interpretive Structural Modelling (ISM). Using trigger questions, based on the dimensions of the Cybersecurity Capacity Maturity Model for Nations (CCMM), a set of objectives was derived to contextualise and support identified the key initiatives for the development of national cyber security capacity in the country.

Keywords: Cyber Security, Cyber Security Maturity Models, Cyber Security in Spring Land, Interactive Management.

1 Introduction

Over the last decades the global security environment has been characterised by several security insufficiencies, which are defined as a government's inability to meet its national security onuses [1]. The security insufficiencies lead to the state instability. Unstable states are clear and often dramatic examples of unsuccessful governance and public supervision failure [2]. Generally, an unstable state is characterised by: civil war; political and economic upheaval-al; absence of law; lack of a reliable body that represents the state beyond its borders at the inter-national level [2, 3]. Global Security (Physical, Personnel and Information) threats are continuing to evolve and spread across our hyperconnected world, irrespective of any international borders, in both

their elaboration and scale of impact. The threats to any nation's infrastructure of networked information systems fluctuate from degrees of disablement to complete debility[4, 5]. Annual Global Risk reports published by the World Economic Forum (WEF) demonstrate an increased annual technological risk, such as data fraud, cyber terrorism, cyber-attacks, and Critical Information Infrastructure (CII) breakdown [6]. Therefore, it is crucial identify potential cyber threats with the potential to have a detrimental rippling effect on various aspects of society and global security.

The aim of this paper is to contextualise the state of the national cyber security capacity maturity levels within unstable environments and provides guidance on moving forward to the higher levels, employing Spring Land as an exemplar case study. Spring Land is a fictional name given to the country from which this real case study is conducted. The paper utilizes the Cybersecurity Capacity Maturity Model (CCMM) for Nations, originally proposed by the Cyber Security Capacity Centre at the University of Oxford [7], as a baseline. The ultimate aim of the paper is to provide benchmark for measuring and planning cyber security for unstable environments.

The paper is structured as follows: Section 2 discusses related research, Section 3 presents the approach of the present study, and the results of the Interactive Management (IM) sessions are presented in Section 4. Finally, Section 5 provides a discussion and conclusions.

2 Related Research

2.1 Cybersecurity at a Nation-State Level

Cyber strategic stability has become a central issue for many countries, and it is increasingly imperative that it is strategically correlated, in leading economies, such as the United Kingdom (UK), NATO and the United States (US)[4]. Cyber security was defined by the International Telecommunication Union (ITU) as: the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisations and user's assets [8]. US President Obama's (2013) Executive Order 13636 "Improving Critical Infrastructure Cybersecurity" addressed the threats the US faces in cyberspace [9]. President Obama stressed that nations must remain vigilant, and ensure the resilience of their complex critical infrastructure systems, whether physical or cyber, by mitigating the threats and fissures that can weaken them. This Executive Order altered the approach of many security practices in terms of how and where cyber issues are addressed, improving the resilience of the national critical infrastructure.

Meanwhile, in 2013, allowing for the significance of Critical Information Infrastructures (CIIs), the European Union (EU) created a practical guide concerning national cyber security strategies (NCSS), later updating it in 2016 to solidify the CIIs' status in neutralising terrorist cells [10]. This CIIs guide helped EU member states to develop their own robust national cyber resilience capability, thereby acknowledging the existence of cyber threats and their risk to national security.

Cyberspace is the 5th domain, alongside land, sea, air, and space, in modern warfare at the operational level, as soldiers are increasingly reliant on digital capacity, and also at the strategic level, since a state's weaknesses and strengths in cyberspace can be employed to deter and affect the strategic balance of power. Nation-states employ cyber weapons directly to disrupt other nation-states' critical infrastructure and computer systems[11].

Researches demonstrated that the motivation behind most cyber-attacks in 2017 was driven by cybercrime, hacktivism, cyber espionage, cyber terrorism, and cyber warfare [12]. The upsurge in cyber espionage has become a significant factor informing Diplomatic, Information, Military, and Economic in the regard to the art of war, due to the development of cyber technology, and the transformation of traditional means of intelligence into cyber espionage. Terrorists and spies can now employ Open Source Intelligence (OSINT) in the cyber domain, as a means to gather information that is not disclosed publicly, as world leaders are acutely aware of, and complain publically about, the potential damage to intellectual property posed by cyber espionage [13]. With regards to cyber-attacks we differentiate: 'cyber terrorism' which uses computers as weapons, or targets, by politically motivated international, or sub-national groups who cause violence and fear in order to influence an audience, or cause a government to change its policies [14]; and cyber warfare, which references attacks conducted by nation-state actors [15].

2.2 Cyber Security in Spring Land

To date, Spring Land authorities have been unable to reinforce their security position, or to enhance their cyber security to meet this demand and its associated criminal, malicious, or state-inspired risks of increased online activity. In 2013, the Spring Land government officially established the National Cyber Security Authority (NCSA), the primary mission of which was to encourage and sustain the secure use of digital services, together with preventing, detecting, and responding effectively to the associated cyber risks [16] . In the same year, with the support of (ITU), Spring Land Computer Emergency Response Team (CERT) was established with national-level responsibilities, and is in charge of prevention, detection, and mitigation of cyber threats. Due to the current political conflict and austerity measures, NCSA faces a lack of funding, which hinders its attempts to advance cyber security [17]. Thus, its ability to address cyber security concerns at any level does not inspire sufficient public confidence. The onus is now on the Spring Land Homeland Security apparatus to prevent any possible terrorist threats, and to preserve and protect the country's critical infrastructure through applying coherent strategy shared by all the relevant departments.

2.3 Cybersecurity Capacity Maturity Model for Nations (CCMM)

Assessing the risk of national critical infrastructure has gained increasing attention. The assessment and detection of cyber threats is conducted though CCMMs [18].

Various types of CCMM exist, such as the International Organisation for Standardisation's Systems Security Engineering Capability Maturity Model (SSE-CMM), the National Institute of Standards and Technology (NIST) Cybersecurity framework, and the US Department of Energy's Cybersecurity Capability Maturity Model (C2M2) [18].The majority of these frameworks are employed at an organisational level; whereas the CCMM proposed by the Cyber Security Capacity Centre at the University of Oxford is employed at a national level, and has been deployed to review cyber security capacity in over 40 countries [7]. Developed through collaboration with international stakeholders, this academic model is politically neutral, offering a comprehensive analysis of cybersecurity capacity through five different dimensions: (i) Cyber Security Policy and Strategy; (ii) Cyber Culture and Society; (iii) Cyber Security Education, Training, and Skills; (iv) Legal and Regulatory Frameworks; and (v) Standards, Organisations, and Technologies. Each dimension includes multiple factors and attributes, each making a significant contribution to capacity building. Meanwhile, each factor, involves five stages of maturity, with the lowest indicator implying a non-existent, or inadequate, level of capacity, and the highest indicating both a strategic approach, and ability to dynamically enhance against environmental considerations, including operational, socio-technical, and political threats [7]. These dimensions were employed when establishing the trigger questions in the present study's IM workshop, in order to capture feedback from the participants, and to contextualise the problem space, centred on the Spring Land case study.

3 Research Method

The aim of this case study was to review the current state of Spring Land's cyber security capacity utilizing an approach called Interactive Management (IM). This case study is an example of a Socio-Technical System (STS) of unstable environment. According to Baxter and Sommerville [19], the STS considers human, social and structural factors, as well as technical factors in the design of organisational systems. This is supported by Appelbaum and Trist [20] by claiming that STS design functions on the presumption that an organisation is a combination of social and technical parts open to its environments. IM was chosen for this reason for the present study, and is discussed further in the following section.

3.1 Interactive Management (IM)

The IM technique concerns complex situations requiring a group of people, who are knowledgeable in terms of the situation, to collaborate in tackling the main aspects of an issue, to develop a deep understanding of the situation under analysis, and to detail the basis for effective action [21]. The concept was developed by Warfield and Christakis[22] in 1980. IM involves three phases; the planning phase: in this phase, the situation is defined, and the scope of the issue clarified [21].The workshop phase: this phase involves uniting a group of participants in an understanding of the issue, or situation. According to Ward, et al. [23], the IM workshop involves three procedures: Idea Writing (IW), Nominal Group Technique (NGT), and Interpretive Structural

Modelling (IS) [21, 24]. In IW, a trigger question is provided to the participants, about which they are invited to silently compose their ideas in a written form. This is followed by the NGT, in which the participants generate further ideas, based on the more holistic view of the problem gained from the IW. The final part of the workshop involves transforming the idea statements into objectives, and then building an Interpretive Structural Model (ISM) to identify the relationships between the various items surrounding the problem. The follow-up phase: in this phase, the outcome and the objectives derived from the previous phase are initiated, commencing the implementation plan towards a solution.

3.2 Participant's profile

In this present study, a one-day workshop hosted by NCSA was conducted with a total of 26 participants (25 male, 1 female) from different stakeholders. The age of participants was between 25 – 55 years old. NCSA issued an invitation letter to all of the stakeholders to help the researcher to contextualise the problem space, which featured the current state of Spring Land's homeland security. The participants were selected due to their contributions in their decision making roles, and included government officials, managers, and general employees participating in security development from areas such as Defence, e-services, Private Sector, Banking, Digital Crime Unit, Oil and Gas sector and Intelligence agency.

4 Results

4.1 Idea Writing (IW) Results

IW was employed to reveal the issues relating to a given a trigger question, providing the participants with a forum to brainstorm and exchange ideas. The participants were divided randomly into three groups to discuss the question, and to provide their views concerning the issues relating to cyber security in Spring Land. The trigger question employed was: What are the current issues of cyber security in Spring Land? After the session, the statements produced were numbered, merged and organised, then sorted into categories, according to each of the CCMM dimensions. Table 1, below, presents the list of shortcomings to face in unstable environments taking Spring Land as a case study.

Table 1. Unstable Environments Vs CCMM Dimensions

D1 - Cyber Security Policy and Strategy
D1.1. Lack of a national cyber security strategy;
D1.2. Unavailability of a national risk management plan, and threat of cyberspace, has not been identified on the national or sector-specific level;
D1.3. Deficiency of a national roadmap for a cyber defence strategy;
D1.4. Difficulty in implementing the cyber security strategy, due to political issues, and scarcity of resources;
D1.5. Absence of a public and private partnerships for sharing information;
D1.6. Miss of a national crisis management protocol and incident response plan for

national critical infrastructure assets, and this has not been prioritised; **D1.7**. Lack of a national cyber security framework for monitoring the adoption of international cybersecurity standards in the government sectors.
D2 - Cyber Culture and Society **D2.1**. Lack of a cyber security culture, and the absence of an understanding of cyber-risk and its consequences in public and private sectors, and decision makers; **D2.2**. Lack of awareness-raising programmes on the governmental level; **D2.3**. Citizens' confidence in the use of e-government services is weak.
D3 - Cyber Security Education, Training, and Skills **D3.1**. Dearth of experienced people to train and teach cyber security programmes, and migration of experiences, due to the security situation in the country; **D3.2**. Lack of a national plan or curriculum in the education system that meets the needs of the cyber security environment; **D3.3**. Education outputs in the cyber security domain are weak, and focus only on technical issues; **D3.4**. Absence of training collaboration between the public and private sector; **D3.5**. Lack of a strategic view of cybersecurity capacity building.
D4 - Legal and Regulatory Frameworks **D4.1**. Non-existence of cybersecurity legislation or regulations to protect personal, commercial, and governmental data. In addition, the initiatives to issue laws related to cyber security face difficulties, resulting from the political situation; **D4.2**. Lack of legislation or regulations for reporting breaches and abuses of cyber-space; **D4.3.** Absence of a legislative system, due to unrest in the political situation; **D4.4.** Poor cooperation between the authorities in the Ministries of Justice and Interior, especially in the field of digital criminal investigation; **D4.5**. Absence of human rights law concerning cyberspace; **D4.6.** Lack of an official national framework for the reporting or sharing of technical vulnerabilities; **D4.7.** Insufficiency of specific legislation concerning cybercrime, and lack of courts to handle cybercrime cases; **D4.8.** Shortage of resources and expertise for digital crime investigation.
D5 - Standards, Organisations, and Technologies **D5.1**. Lack of use of the information security management systems (ISMS), in all governmental sectors, except for a telecommunications provider **D5.2**. Most government sectors use technologies and applications provided by third parties and international companies, without heeding the need to review the security vulnerabilities in the systems; **D5.3**. Lack of a national agency for digital certification; **D5.4**. Absence of national benchmarking, auditing, and risk assessment policy; **D5.5**. Lack of a national infrastructure resilience plan. Military and political conflicts have severely affected the resilience of the infrastructure, and exposed the telecommunications, electricity, and water sectors to destruction or theft.

4.2 Nominal Group Technique (NGT) Results

The NGT technique was employed to generate and obtain an initial rating of a set of objectives. Following the organising and numbering of the IW, the participants were required to transform their ideas into a set of objectives, which were used to create an interpretive structural model (ISM), and to summaries the interactions between them. The final part of the workshop employed the NGT, requiring the participants to select their top three objectives from the list for each dimension, with one being the least important, and three the most important. A total of 19 of the participants then voted on the objectives, although seven of the participants failed to vote, owing to external commitments or issues. Table 2 shows the three most important objectives from each CCMM dimension.

Table 2. CCMM Vs Three Top Priority Objectives

Dimension	Objective	Total
D1	**D1.1.** Adopt a national cyber security framework.	41
	D1.3. Establish a central committee to design a national roadmap for a cyber defence strategy.	37
	D1.6. Create a national list of CNI assets, and identify the risk priorities.	13
D2	**D2.2**. Develop a national awareness program that is compatible with the current situation, targeting all of society.	40
	D2.3. Encourage all stakeholders to run regular awareness-raising campaigns.	39
	D2.4. Improve e-services, in order to promote the required level of trust, and improve the application of security measures.	20
D3	**D3.1**. Develop national cyber security education and cyber security modules.	40
	D3.2. Provide a sufficient budget for capacity building.	39
	D3.4. Classify training needs, and develop cyber exercises and drills.	12
D4	**D4.1**. Draft national laws and regulations relating to digital crime.	40
	D4.2. Create a strong national legal framework for the sharing of information incidents, vulnerability disclosure, and report-ing.	31
	D4.3. Build and strengthen national capacity in law enforce-	27

	ment.	
D5	**D5.1**. All stakeholders to adapt and adopt international standards, such as ISO27000.	39
	D5.2. Create a national risk assessment, crisis management, and auditing framework.	31
	D5.5.Enhance physical security.	26

4.3 Interpretive Structural Modelling (ISM)

The ISM technique helped the participants to examine the inter-relationships between the elements gained through the NGT process, and provided a structure for tackling its complexity [25]. The ISM is an acknowledged methodology for classifying relationships among a set of interconnected criteria, which define a problem or an issue [26]. In order to create a clear ISM, the objectives were grouped by similarity, to facilitate the identification of the three most important objectives from each dimension, which are presented in Table 2. The ISM, derived from the objective statements and their interactions based on the dimensions of the CCMM, is represented in Fig.1.

As can be observed from Fig.1, the development of a national blueprint is deemed to be important because current state interactions in cyberspace manifest the lack of national cyber frameworks. The results in Fig.1 also show that the group considered that the provision of a robust national awareness programme, which targets the whole society, would be a significant factor in improving national cyber security. The group believed that the creation of a national strategy framework would drive the creation of an effective national legal framework, which would assist in the improvement of information sharing, incident vulnerability disclosure, and reporting between governmental sectors. Furthermore, the group decided that enhancing physical security would also help to increase the national and organisational capability to resist and react to internal and external threats.

5 Conclusion and Future Work

In this paper we explored the main characteristics of Spring Land cyber security as an example of unstable STS. We used IM-based approach. IM provided a rational grounding in the current cyber security challenges in Spring Land, and how they should be addressed. The set of problem statements and objectives derived from the IM approach can be employed to support the management of a national cyber security capacity in an unstable environment, similar to the case study exemplar presented herein. However, these results require further validation and generalisable data, which will be addressed in a future study. The relationships between objectives from ISM will be analysing using the adjacency matrix and create a reachability matrix. In addition, development of a meta-model based on the Interpretive Structural Model (ISM)

developed for an unstable environment. The modelling approaches such as IDEF0, UML, SysML, Data Flow Diagrams and Flow Charts can be used to decompose the ISM into further applied functional models.

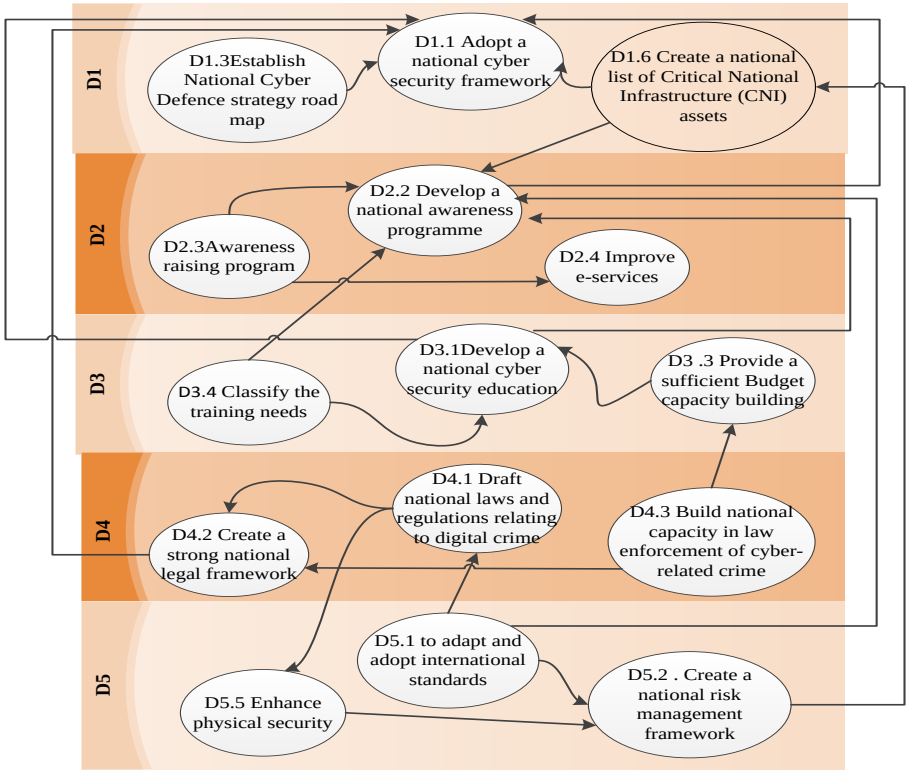

Fig 1. Interpretive structural modelling for unstable ennviroment

References

1. M. McCrabb, "Rough Waters," Naval War College Review, vol. 70, pp. 141-145, (2017).
2. K. DeRouen Jr and S. Goldfinch, "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).
3. 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).
4. H. Nissenbaum, "Where computer security meets national security," Ethics and Information Technology, vol. 7, pp. 61-73,(2005).
5. G. W. Bush, President George W. Bush: The National Strategy to Secure Cyberspace: Morgan James Pub, (2003).

6. W. E. F. Weforum.. The Global Risks Report 2018 (13th ed.). Available: http://www3.weforum.org/docs/WEF_GRR18_Report.pdf, (2018).
7. GCSCC. Cybersecurity Capacity Maturity Model for Nations (CMM). (2017). https://www.sbs.ox.ac.uk/cybersecuritycapacity/system/files/CMM%20Version%201_2_0.pdf
8. ITU. Definition of Cybersecurity. Available: http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/Pages/cybersecurity.aspx, (2016).
9. E. Orded, "Executive Order--Improving Critical Infrastructure Cybersecurity," (2013).
10. J. Argomaniz, "The European Union Policies on the Protection of Infrastructure from Terrorist Attacks: A Critical Assessment," Intelligence and National Security, vol. 30, pp. 259-280, (2015).
11. M. Hjortdal, "China's use of cyber warfare: Espionage meets strategic deterrence," Journal of Strategic Security, vol. 4, p. 1, (2011).
12. P. Passeri, "Cyber Attacks Statistics," in Cyber Attacks Statistics, ed, (2017).
13. K. Geers, "The cyber threat to national critical infrastructures: Beyond theory," Information Security Journal: A Global Perspective, vol. 18, pp. 1-7, (2009).
14. C. Wilson, "Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. CRS Report for Congress. Congressional Research Service-The Library of Congress," ed, (2005).
15. J. J. Prichard and L. E. MacDonald, "Cyber Terrorism: A Study of the Extent of Coverage in Computer Science Textbooks," Journal of Information Technology Education: Research, vol. 3, pp. 279-289, (2004).
16. NCSA. The National Cyber Security Authority (NCSA), (2013).
17. Symantec, "Cyber crime and cyber security trends in Africa Report," Symantec (2016).
18. W. Miron and K. Muita, "Cybersecurity capability maturity models for providers of critical infrastructure," Technology Innovation Management Review, vol. 4, p. 33, (2014).
19. G. Baxter and I. Sommerville, "Socio-technical systems: From design methods to systems engineering," Interacting with Computers, vol. 23, pp. 4-17, (2011).
20. S. H. Appelbaum, "Socio-technical systems theory: an intervention strategy for organizational development," Management decision, vol. 35, pp. 452-463, (1997).
21. Warfield, John N, and A. R. Cárdenas, A handbook of interactive management: Iowa State Press, (2002).
22. B. A. Banathy, "Information-based design of social systems," Systems Research and Behavioral Science, vol. 41, pp. 104-123, (1996).
23. J. Ward, H. Dogan, E. Apeh, A. Mylonas, and V. Katos, "Using Human Factor Approaches to an Organisation's Bring Your Own Device scheme," in International Conference on Human Aspects of Information Security, Privacy, and Trust, pp. 396-413, (2017).
24. F. R. Janes, "Interactive Management: Framework, Practice, and Complexity,", pp. 51-60, (1995).
25. H. Dogan, S. A. Pilfold, and M. Henshaw, "The role of human factors in addressing Systems of Systems complexity," in 2011 IEEE International Conference on Systems, Man, and Cybernetics, pp. 1244-1249, (2011).
26. P. Shahabadkar, "Deployment of interpretive structural modelling methodology in supply chain management–an overview," International Journal of Industrial Engineering & Production Research, vol. 23, pp. 195-205, (2012).