International Journal on Advanced Science Engineering Information Technology

Vol.8 (2018) No. 6
ISSN: 2088-5334

A Model for Afghanistan's Cyber Security Incident Response Team

Islahuddin Jalal[#1], Maryati Mohd Yusof[#2], Zarina Shukur[#3], Mohd. Rosmadi Mokhtar[#4]

[#]*Center for Software Technology and Management, Faculty of Information Science and Technology*
Universiti Kebangsaan Malaysia, 43600 Bangi, Malaysia
E-mail: [1]islahuddinjalal@yahoo.com, {[2]zarinashukur, [3]Maryati.Yusof, [4]mrm}@ukm.edu.my

***Abstract*— Persistent cyber threats require effective and efficient mitigation techniques. The cyber security incident response team (CSIRT) is expected to respond to external and internal cyber threats or incidents. Various organizational, national, and international level CSIRTs have been developed for defending and protecting such kinds of threats. Developing countries like Afghanistan have also formed a Computer Emergency Response Team for handling national cyber incidents although it provides limited services to only a few constituencies and depends on funding from foreign donors. Therefore, a new organizational model was proposed to provide guidelines for a specific country, instead of a provision from a constitutional context. Five national CSIRTs were compared to identify their features and characteristics to provide basis for the proposed framework. The study presented the proposed model based on two CSIRT organizational models that incorporated a new funding strategy to achieve a Sustainable National CSIRT for developing countries. Our model combined coordinate and security teams; if consists of constituency's mission, services, resources, organizational framework, and funding strategy. This study employed qualitative method by using document analysis and interview techniques. CSIRT for Afghanistan known as AFCERT was evaluated in terms of structure, services, resources, and funding. AFCERT services level were below the standard of a national CSIRT. Therefore, a more sustainable service need to be provided based on the proposed model components. Findings showed the suitability and potential of the model in controlling and mitigating cyber-attacks, more specifically in the context of Afghanistan.**

***Keywords*—CSIRT; cyber security, cyber-attacks, cyber policy.**

I. INTRODUCTION

The Cyber Security Incident Response Team (CSIRT) plays a significant role as the backbone of a country's cybersecurity infrastructure. It manages all types of cyber incidents such as financial crime, political crime, internet fraud, and cyber pornography [1]. According to Hammond [2], more than 4000 ransomware attacks and 230000 new malware produced every day. Some national CSIRTs have been developed globally. Afghanistan's Computer Emergency Response Team (AFCERT) has been providing services to its constituencies by closely cooperating with law enforcement agencies to combat cyber crimes in the country and create awareness in the government and private sector [3], [4].

However, AFCERT is confined to law enforcement agencies and focuses mainly on legal aspects. Moreover, it does not cover constituencies as done by the national CSIRT. The current funding strategy adopted by AFCERT seems to be temporary because it relies on foreign donors, which is not sustainable. Therefore, consideration should be given to funding strategies for the national CSIRT in Afghanistan. Afghanistan faces some cyber threats, namely access to government data, threats to financial organizations and critical national information infrastructure, hacking, virus distribution, computer system tampering and data privacy issues. A CSIRT for Afghanistan is imperative in order to combat, protect and defend its cyberspace efficiently and effectively.

Numerous studies have defined CSIRT, but they all share the same theme. Ruefle et al. [5] defined it as "a concrete organizational entity or capability that has been assigned the concern of providing a portion of the incident management capability for a particular organization." According to Killcrece [6], CSIRT "is a service organization responsible for receiving, reviewing and responding to computer security incident reports and activities in its constituency." This study had defined merely CSIRT as a group of experts who can protect and mitigate cyber-attacks on critical national infrastructure, public and private sectors, as well as people.

A CSIRT has various sizes, nature, and scope. Killcrece [6] categorized it according to purpose, function, services, structure, and sector. Zajicek [7] classified CSIRT based on its internal structure, coordination and analysis center, vendor security team and incident response provider. Bradshaw [8] classify CSIRT based on the Parent organization such as National CSIRTs, Private CSIRTs, and Technical or Academic CSIRTs. According to [9] no two CSIRTs are the same. There are some similarities and differences exist in the CSIRTs. These differences may be due to the several factors such as CSIRT type, organization type (e.g., manufacturing company, university), size of the CSIRT and Kind of services they offer. CSIRT can be categorized according to its geographical circle because the cyber world has no borders or limits. For example, the category consists of organizational CSIRTs (e.g., military, community, and institutional), national CSIRTs (e.g., Malaysia, Australia, and India), and international CSIRTs (e.g. For Inspiration and Recognition of Science and Technology (FIRST), Asia Pacific Computer Emergency Response Team (APCERT), CERT@VDE which focuses on the CSIRT services to SME to address the gap in trust and capabilities in security [10] and Organization of the Islamic Conference Computer Emergency Response Team (OIC-CERT)).

A. Major Components of CSIRT

CSIRT is made up of six crucial pillars that influence each other [6], namely mission, constituency, organizational framework, resources, services, and funding.

1) Mission: One of the most critical organizational statements that indicate future direction. It should be pragmatic, flexible, concise and related to the core services that CSIRT provides to its constituencies [11].

2) Constituency: A defined group that is served by CSIRT [6], such as a parent organization, government ministry, institution, community or organization within a specific geographical boundary. A constituency can be bounded or unbounded [5], which refers to the limited service offered by CSIRT. According to [15] most of the constituency are bounded and provide services to those who are providing funding. The constituency definition for CSIRT is challenging [5]. Once the constituency is defined and understood, it will be easy to understand and determine how to protect the assets in these places [5]. This will provide an insight on the services provided by the CSIRT, mainly referring to the teamwork involved. This information will guide in determining the most suitable CSIRT organizational model [6].

3) Organizational framework: The overall structure of *the* CSIRT consist of its physical location, reporting infrastructure, job requirements, interaction with a constituency as well as within the team, authority and internal and external information flow of the CSIRT. The formation of the organizational framework depends on mission, objectives, necessity, and services of the organization in different constituency [15].

4) Resources: This comprises staff (Technical/ Non-technical) and equipment (Software/ Hardware). Killcrece and Ruefle [12] recommended various equipment for CSIRT, which included the telephone, fax machine, office computing systems, laptops, projectors, notification systems, electronic whiteboards, VPNs, SSH (Secure Shell) or digital certificates, software including operating systems, lab devices, intranet, test network, web, firewalls, servers, databases, routers, switches, monitoring tools, media and infrastructure (space, furniture, power, and transportation).

5) Services: Every CSIRT offers different services or functions based on its nature, culture, environment, expertise available, funding [5] and needs. Services are classified according to 1) reactive (alerts and warnings, incident handling, vulnerability handling and artefact handling); 2) proactive (announcements, security assessments, development of security tools, intrusion detection services and security-related information dissemination); 3) quality management (risk analysis, disaster recovery planning, security consulting, awareness building, education/ training and product evaluation) [5]; and 4) long-term resiliency (knowledge sharing for critical infrastructure guidelines, advisories), research and education, point of contact (responsible disclosure) [13].

6) Fund: This could be considered as the nucleus of the CSIRT. The fund should be obtained for start-up as well as short and long-term operations [5], which includes initial staffing, short and long-term professional development, training, equipment, tools, network infrastructure for detecting, tracking, analysing, and responding to cyber issues, as well as securing and facilitating CSIRT (data, system, staff). Different fund strategies for CSIRT have been described in the handbook [12]. Many national CSRITs do not publish the funding sources and specification because of unclear structures in the public domain [16]. Some CSIRTs are provided a fund for the services it offers by some other organization or entity [2]. Some of the examples of funding strategies for national and organizational CSIRTs are described in Table 1. Different countries have different funding strategies and models.

TABLE I
DIFFERENT FUNDING STRATEGIES FOR CSIRT

Funding strategies	**Country or Organization**
Membership Subscription	AusCERT (Australia)
Fee-based Services	MYCERT (Malaysia)
Contract Services	IBM, ISS, CISCO, Consulting firms
Government Sponsorship	US-CERT (USA)
Academic or Research Sponsorship	SURFcert, NORDUnet CERT
Parent Organizing Funding	Cisco PSIRT
Consortium Sponsorship	Group or organizations, government entities, universities
Combination of the above	CERT/CC
Funded Voluntarily	bdCERT (Bangladesh)
Domain Name Registration	CGI.br (Brazil)

B. Existing Organizational Model of CSIRT

Studies on the organizational model of CSIRT are limited. Carnegie Mellon University has been playing a leading role in the development of CSIRT guidelines, notes, and handbook. Killcerce [6] focused on CSIRT's physical location, dependence, and constituency interaction as well as

reporting infrastructure and mechanism for internal and external information flow. We analyzed five organizational models for CSIRT, as featured in the study by Killcerce [6], namely the security team model, internal distributed model, centralized model, combination of centralized and distributed model, and coordinated model [14].

C. Comparison between Four Other National CSIRTs

Some national CSIRTs have been developed since 1988 for safeguarding and protecting its critical infrastructure, financial institutions, as well as public and private sectors from cyber-attacks. According to [16] 89 countries, as well as European Union (EU), have developed national CSIRTs yet. All national CSIRTs have similar aims but with a slight difference regarding providing services, constituencies with different cultures and religions, availability of expertise and resources, as well as the type of cyber-attacks and its magnitude and intensity. Since the primary aim of this study was to support the work of proposing a new CSRIT model for Afghanistan, four national CSIRTs were reviewed to identify their relevant features based on these justifications:

- MyCERT (Malaysia): An Islamic country with similar Islamic culture, values, and attitudes as Afghanistan.
- CERT-In (India): Has a very close political relationship with Afghanistan.
- CNCERT (China): A neighboring country with Afghanistan.
- US-CERT (United States of America): the USA has signed a bilateral security agreement with Afghanistan

MyCERT and US-CERT are concerned about Internet security, while CERT-In [17] and CNCERT [18] highlighted its critical infrastructure. Exchanging information to the rest of the world is an essential aspect of US-CERT. MyCERT's primary sponsor is the government; however, since it also provides services to the public, it can provide fee-based services that help them to cater to both the public and private sectors. CERT-In is also sponsored by the government and provides services mostly to the government, academic institutions, and related industries. CNCERT is proactive and focuses more on the security of critical national infrastructure, instead of people at large as shown in MyCERT and US-CERT. International cooperation is also vital to CNCERT. US-CERT declared critical infrastructure as their stakeholders and highlighted the importance of collaboration with other parties.

In order to construct a sustainable national CSIRT, four strategic goals need to be achieved [19]:

- Plan and establish the capability to manage security incidents (engage stakeholders; understand constraints; location/ reporting; authority)
- Establish situational awareness (build trust; recognize the dual role of the CSIRT; operational capabilities; use existing national CSIRT as a resource)
- Manage cyber incidents (operational capabilities; use existing national CSIRTs as resources)
- Support the national cybersecurity strategy (in the absence of a national cybersecurity strategy; identify a sponsor for a national CSIRT).

II. Material and Method

This study employed qualitative methods via document analysis and email interviews using the purposive sampling method. Email interviews were carried out iteratively with three informants (Table 2) from the Ministry of Communication and Information Technology (MCIT) of Afghanistan. AFCERT is the only CSIRT in the country and has only two departments, namely the Cyber Awareness and Cyber Crime Forensics Departments that comprises the three informants above. They have vast experience in managing cyber-crimes in the country. The interview aimed to identify the status, infrastructure and major components required for CSIRT and how the AFCERT handles cyber incidents in Afghanistan. The interview questions were designed based on the major components of CSIRT, namely mission, constituency, services, resources, organizational framework, and fund.

TABLE II
Informant's Profile

Designation	Educational Background	Work Experience
Information Cyber Security Director	MSc in Computer Security	6yrs
General Manager (GM) of Cyber Awareness Department	BSc in Computer Science	4yrs
GM of Cyber Crimes Forensic Department	BSc in Computer Science	5yrs

Document analysis was conducted on documents related to Afghanistan's cyber threat and AFCERT including government officials report, official documents of international CSIRT, Critical Information Infrastructure Protection and Cyber Security report, and existing CSIRT model. Data were analyzed manually using the instructed content analysis technique. Field notes were examined by identifying the main elements that were categorized based on the proposed framework.

III. Results and Discussion

A. AFCERT

AFCERT has been actively functioning since 2009 as a first responder for combating and mitigating cybercrimes in the country. It is centrally located and under the auspices of the Information and Cyber Security Directorate of the Ministry of Communication and Information Technology (MCIT). It works round the clock to provide services to its constituencies, closely cooperating with law enforcement agencies and creating awareness in the government and private sectors. When cyber incidents occur, the constituencies report to the AFCERT through a formal letter or email. Then the AFCERT provides feedback to the constituencies and files the report for future investigation. AFCERT works closely with law enforcement agencies, and most of its cases are confidential. Therefore, it does not publish nor possess a formal mechanism for periodically publishing official reports on threats, crimes, or vulnerabilities for the public. So, the cybersecurity challenges across all areas of human life are in such magnitude and complexity that the current policy responses

are closed and led only by governments are not sufficient and may increase the number of collateral damage. [20]

1) The constituency of AFCERT: AFCERT provides services to law enforcement agencies and creates awareness for the government and private sectors. AFCERT does not include constituencies like other national CSIRTs. Therefore, it is necessary for Afghanistan to develop a national CSIRT to combat and defend its cyberspace effectively and efficiently.

2) Services by AFCERT: AFCERT provides the following services to its constituencies (Table 3).

TABLE III
AFCERT SERVICES

Reactive Services	Proactive Services	Security Quality Management Services
Response on-site	• Vulnerability assessment • Penetration testing	• Information Security Audit • Support entities by writing security policies and procedures

"AFCERT services are mainly in response to the crime scene, conduct information security audit, vulnerability assessment of networks, penetration testing, and support entities by specifying their security policies and procedures" (ICSD Director). AFCERT does not share its cybersecurity information with its constituencies or other national CSIRTs due to unavailable connection meant for coordination and cooperation – "due to political instability we are not able to connect our NOC with international partners, but for now we are using online information to obtain the latest updates on cyber alerts" (GM CAD).

Information sharing, coordination, and cooperation with other local and national CSIRTs are the core services of a national CSIRT, but these services are lacking in the AFCERT. Compared to other national CSIRTs, the services provided by the AFCERT are not up to the standard of a national CSIRT. This calls for the enhancement of sustainable services that fulfill the requirements of a national CSIRT for Afghanistan.

3) Resources of AFCERT: AFCERT has limited resources comprising:

- Staff (ICSD director, 4 CCFD members, and 3 CCAD members)
- Equipment (e.g., Furniture, Computers/ laptops, Internet, Telephone, OS, DNS, Web Server, Workstation, Antivirus software, forensic lab)
- Infrastructure (e.g.: CCFD, CCAD, Power, Transportation)

4) Fund of AFCERT: Similar to other national CSIRTs, Afghanistan also receives funding from the government and the United States Agency for International Development (USAID), which is one of the donors working towards the rebuilding and rehabilitation of Afghanistan. According to the ICSD Director, "AFCERT is using the government budget for its sustainability and improvement. Every year we estimate the budget and send the proposal to the Ministry of Finance. There is no other source available for AFCERT except one from the e-Government resource center funded by USAID".

The current funding strategy for AFCERT is not sustainable due to the reliance on foreign donors. A national CSIRT should be fully funded by its government or other means to fulfill its requirements. Therefore, a focused consideration should be given towards funding strategies for a sustainable national CSIRT for Afghanistan.

B. CSRIT

This study proposed a Central Coordinate Contributed-CSRIT (3C-CSIRT) model that combined coordinate and security teams (Figure 1). The respective constituency's role is highly engaged by sharing its expertise and budget. This study attempted to improve the sustainable funding issue and limited technical expertise. As 3C-CSIRT is a national CSIRT so, therefore, should not be part of either Intelligence institution or law enforcement agencies and do not report directly to either of them [16]. The significant components of 3C-CSIRT are the constituency's mission, services, resources, organizational framework, and funding strategy. The components were identified from the literature and validated through interviews and document analysis.

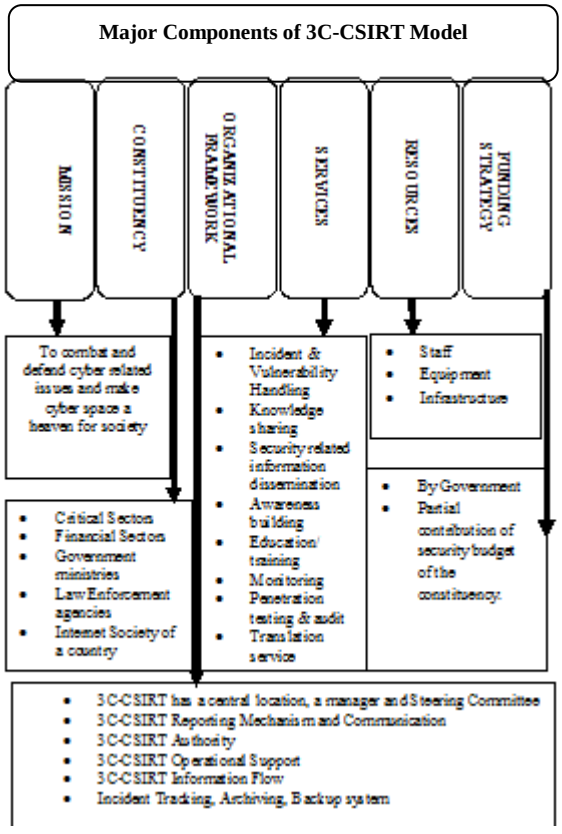

Fig.1. Proposed CSIRT Model

1) 3C-CSIRT Constituency: The constituencies in this model follow the critical sectors in Afghanistan [21], they include financial sectors, government ministries, law enforcement agencies and the Internet Society of Afghanistan.

2) 3C-CSIRT Organizational Framework: As the 3C-CSIRT is a combination of the central coordinate model and security team, it has both a dedicated as well as an ad hoc team for its parent constituency. The dedicated team works for all the constituencies of the 3C-CSIRT, while the ad hoc team works only for its parent organization and handles cyber incidents on-site while sharing the incidents with the central 3C-CSIRT. 3C-CSIRT has a central location, a manager, and a steering committee (SC). SC comprises the head of ISO, CIO, IT and CSO in the constituencies. The constituencies must be large enough with branches or offices covering more than half of all the Afghanistan provinces. The 3C-CSIRT involves staff with skills and expertise in all systems and platforms supported by the constituency. However, 3C-CSIRT is a national team that covers the entire cyber society in the country and runs its operations round the clock. Therefore, its role is to advise and support the constituencies that do not have security teams. It is authoritative to some extent in the presence of security teams from the respective constituencies. The 3C-CSIRT should act neutral and be impartial to all constituencies. It is obvious that large, geographically dispersed constituencies cannot reasonably provide an appropriate direct incident response at the site [6]. Therefore, the function of the security team would be to fill this gap in the proposed model.

3) 3C-CSIRT Reporting Mechanism and Communication: The focal point in this model should be the office of the 3C-CSIRT manager for internal and external entities to coordinate and render support since the manager is responsible for controlling and managing the 3C-CSIRT technical staff and provide reports to the steering committee. The 3C-CSIRT should have a proper reporting mechanism for its constituencies in order to respond and support them without delay. There should be a helpdesk centrally located in 3C-CSIRT, which is responsible for collecting incident reports from its constituencies through multiple modes of communication such as mobile phones, email, Internet, fax, fixed line and secure communication channels (for internal reporting). The security team will report security incidents using their secure communication channel to the 3C-CSIRT helpdesk to keep track of incidents occurring in the country for further investigation. This will help to prevent recurring incidents in other constituencies and also help in publishing annual, quarterly or monthly incidents or reports for the public.

4) 3C-CSIRT Authority: As discussed earlier, the 3C-CSIRT's role is to advise and support constituencies without security teams while being authoritative to some extent in the presence of security teams from the respective constituencies. 3C-CSIRT has temporary operational authority over all constituencies in the case of emergency, risky, or critical incidents.

5) 3C-CSIRT Operational Support: 3C-CSIRT is responsible for providing operational support to the security team in the constituencies and also those who do not have a security team. 3C-CSIRT provides technical and practical guidance [5] throughout an incident's life cycle, from identification, analysis, containment, eradication, and recovery in order to defend and protect assets from cyber incidents efficiently and effectively.

6) 3C-CSIRT Information Flow: Incoming information might include situational awareness and incident detection [12], while outgoing information might involve the relative responses. The source and destination of both flows need to be considered. The incoming information might specifically comprise reports received, data from network logging or monitoring devices such as IDS, or secret information from other organizations including National Defence Services (NDS) and law enforcement sectors and sharing information with other CSIRTs and security organizations within and outside the 3C-CSRIT constituency. Examples of outgoing information include alerts, advisories, security guidance and documentation, awareness information, or formal briefings and reports going to management and business lines [5].

7) 3C-CSIRT Services: Some of the services include incident and vulnerability handling, knowledge sharing (guidance, advisories), security-related information dissemination, awareness building, education/ training, monitoring, penetration testing and audit, as well as translation services. Incident handling means the response to cyber incidents or events requested or reported by constituencies [6]. Incident handling includes protecting, defending, mitigating, and controlling the risk of cyber incidents that affect the system or network. The advancement and production of more and smarter devices for the internet of Things (IoT) will pose more risks alongside new attack surfaces is going to be exposed in autonomous systems such as self-driving vehicles [22]. The incident handling activities are categorized as follows [6]:

- Incident and Vulnerability Analysis. The 3C-CSIRT analyses the reported incident to determine the origin, the tool used in the attack, the scope of the attack, the vulnerability that was exploited, provide a strategy for incident recovery and mitigating as well as performing an in-depth analysis on the affected system with the help of the security team from the 3C-CSIRT constituencies. The analysis is performed in order to understand the overall security position of the constituencies.
- Incident and Vulnerability Response Support. Response on sites, such as answering questions through the telephone, mobile phones, email or other communication tools, provides results by researching incidents and vulnerabilities, tracking and maintaining the history of incidents and vulnerabilities that could be accessed by the constituencies and provide technical reports.
- Incident and Vulnerability Response Coordination. A dedicated team provides comprehensive tracking, recording, and dissemination of information for the constituency, consolidates the collected information to identify similar attacks, artifacts, vulnerability exploits, trends, and patterns; develop a mitigation strategy for potential threats; bring constituents together to act as a unit against the cyber threats or crimes.

This component covers the whole incidence's life cycle (Figure 2) [5].

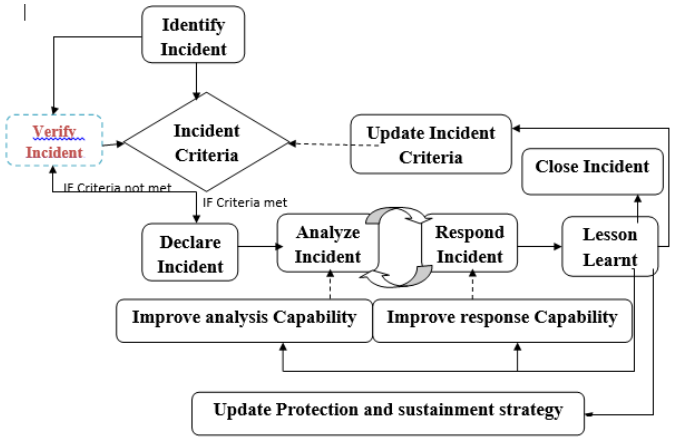

Fig. 2. Incident Handling Life Cycle (adapted from Ruefle et al. [5])

8) Knowledge Sharing (guidance, advisories): 3C-CSIRT shares technical guidance and advisories that form a precautionary step for the constituency's systems or networks from cyber intrusion activities. A CSIRT is not something like operating in a vacuum, but it must operate in the context of a complex sociotechnical environment or system [9]. Therefore, 3C-CSIRT should share its practical experience regarding cyber incidents, vulnerabilities or other security issues with its constituencies as well as with other external CSIRTs, either locally or internationally, for better cooperation and coordination. However, sharing or exchanging information and cooperation depends on the available trust models they may have with each other [9].

*9) Security Related Information Dissemination:*3C-CSIRT has a website through which all the constituencies can share security-related information such as recommended tools, security patches, software updates, best practices, vulnerabilities, and incidents in English as well as in their native language for better understanding.

10) Awareness Building: 3C-CSIRT provides awareness programs for all constituencies by arranging seminars, briefings on the definition of security issues, effects on society and economy as well as precautionary measures for prevention purposes. The 3C-CSIRT uses media broadcasting and social media for security awareness purposes.

11) Education/Training: The lack of technical expertise and talent for a long time within the constituent's organization may severely damage the respective organizations' ability to develop and implement the policy [23] and combat the cybercrimes effectively and efficiently. Therefore, the 3C-CSIRT provides training programs to members in the constituency. This includes training classes on security issues, incident response issues, tutorials on the type of attacks and its solution strategies, and vulnerability trends. The 3C-CSIRT also trains its technical staff by sending them to foreign countries for international certification courses.

12) Penetration Testing and Audit: 3C-CSIRT provides Penetration Testing and Audit services on the request of constituencies. These services include simulation tests on systems and networks to identify flaws in the systems or networks. Before conducting penetration tests, both the 3C-CSIRT and constituency, sign service level agreements for legal purposes. The 3C-CSIRT can conduct security audits in constituencies based on international (e.g., ISO, COBIT) or local security standards. 3C-CSIRT provides an audit report to the constituency in order to identify the weak points or violations of standards. A security audit is compulsory for all constituencies of 3C-CSIRT and should be conducted once a year. The audit can identify risk level of systems, networks, and applications in order to assist in reducing, preventing or mitigating risks.

13) Monitoring: 3C-CSIRT monitors the constituency's networks by ensuring that the operational security of its data system is adequately monitored for security anomalies. It monitors all websites in the .af domain for defacement, collects information from internet traffic entering the constituency's network for gaining situational awareness of intruders by analyzing the traffic of the constituencies through the distributed network intrusion detection system based on the open source tool called "SNORT."

14) Translation Service: As a non-English speaking country, Afghanistan can benefit from translation services meant for dissemination, awareness and knowledge sharing (guidance, advisories) purposes.

15 3C-CSIRT Resources: Resources such as staff, equipment, and infrastructure need to be considered. Standard Operating Procedures (SOPs) for emergency communication, handling media interactions, incident reporting, sensitive data storage, and record keeping/incident tracking can support 3C-CSIRT's incident handling policies. *Staff* includes the steering committee, manager, technical staff and non-technical staff. The steering committee consists of heads of ISO, CIO, IT and CSO in the constituencies. The constituencies must be large enough and have branches or offices that cover more than half of Afghanistan. The 3C-CSIRT comprises staff with skills and expertise in all types of systems and platforms supported by the constituency. The manager should control and manage 3C-CSIRT operations and report to the Steering Committee. The role and responsibility of each staff in the 3C-CSRIT should be clearly defined.

16 Equipment: equipment includes furniture, computer equipment (hardware, software), stationary, test lab, transportation, and communication equipment (telephone, cell phone, and fax).

17) Infrastructure: infrastructure provides a secure environment for routine work, which includes office, physical security, digital security systems (CCTV), universal power supply (UPS) system, power generator, secure communication mechanism, tracking system, repository system, web services, backup system, monitoring system (IDS, IPS, Firewall), System and Network protection as well as Scanning software, which the 3C-CSIRT security team can utilize the infrastructure of the respective constituencies.

18) Funding strategy: a funding strategy is based on compulsory and non-compulsory constituencies contributing some part of their annual security budget to the national CSIRT. The government should take the initiative and encourage ministries, financial institutions and other public and private organizations by defining or explaining the role, responsibilities and importance of national CSIRTs to participate and contribute some part of their security budget to the national CSIRT in order to combat and defend the cyberspace of Afghanistan in an effective and efficient manner. Compulsory constituencies including critical sectors, the national bank, and the government must provide funds to the national CSIRT at any cost. The non-compulsory entities are the remaining sectors that need the services of the national CSIRT. According to this strategy, the steering committee and the security team members should be paid by the respective constituencies.

IV. Conclusion

This study attempted to overcome the shortcomings in the constituency as well as the services and funding strategy of Afghanistan's computer emergency response team by proposing the 3C-CSIRT organizational model to accomplish a Sustainable National Cyber Security Incident Response Team. Results showed the model's suitability and potential in managing cybersecurity activities, specifically from the Afghanistan context. For future research, some data collection methods, such as on-site observations, face-to-face interviews, and a detailed content analysis could be conducted to validate the proposed model further. Investigations on other components of CSIRT could provide a deeper insight into cybersecurity operations.

Acknowledgment

Universiti Kebangsaan Malaysia grant AP-2017-003/2 partly sponsors this work.

References

[1] J.Govil (2007) Ramifications of Cyber Crime and Suggestive Preventive Measures. The 2007 IEEE EIT Proceeding, 610-615

[2] A. Hammond. (2018). February 16, 2018. Three Issues to Address. The Data Center Journal Cybersecurity 2018 http://www.datacenterjournal.com/cybersecurity-2018-three-issues-address.

[3] Profile, I. C. (n.d.). ITU. Retrieved 2014, from ITU [Online]. Available: http://www.itu.int/en/ITU-D/Cybersecurity/Pages/default.aspx

[4] Information and Cyber Security Directorate Director Interview.

[5] R. Ruefle, K.v. Wyk and L. Tosic (2013). New Zealand Security Incident Management Guide for Computer Security Incident Response Teams (CSIRTs). New Zealand National Cyber Security Centre Government Communication Security Bureau, Developed in cooperation with the CERT® Division of the Software Engineering Institute at Carnegie Mellon University.

[6] G. Killcerce (2003). Organizational Models for Computer Security incident response Team (CSIRT). CMU/SEI-2003-HB-001.

[7] M. Zajicek (2004). Creating and Managing: CSIRTs-notes. Creating and Managing Computer security incident response teams (CSIRTs) . United States of America: CERT/CC.

[8] S. Bradshaw. (2015) Combatting Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity. Published by the Center for International Governance Innovation and Chatham House. Ourinternet.org.

[9] Rick Van der Kleij, Geert Kleinhuis and Heather Young Computer Security Incident Response Team Effectiveness: A Needs AssessmentFrontiers in Psychology, Front. Psychol., 12 December 2017 https://doi.org/10.3389/fpsyg.2017.02179

[10] FIRST/TF-CSIRT: The Changing Face of Cybersecurity By Kevin Meynell Published by Internet Society [Online]. Available: https://www.internetsociety.org/blog/2018/02/first-tf-csirt-changing-face-cybersecurity

[11] N. Brownlee (1998). ietf.org. Retrieved 2014, ISOC [Online]. Available: https://www.ietf.org/rfc/rfc2350.txt

[12] G. Killcrece and R. Ruefle (2008). Creating and Managing Computer Security Incident Response Teams (CSIRTs). Carnegie Mellon University.

[13] Kas Clark, D. S. (2014). A Dutch Approach to Cybersecurity through participation. Copublished by the IEEE Computer and Reliability Societies , 27-34.

[14] I. Jalal, Z. Shukur and M.R. Mokhtar. (2017) 3C-CSIRT Model: A Sustainable National CSIRT For Afghanistan. The 2017 6th International Conference on Electrical Engineering and Informatics (ICEEI), 25-27 Nov 2017. Langkawi.

[15] Y.M. Wara and D.Sing. (2015) A Guide to Establishing Computer Security Incident Response Team (CSIRT) For National Research and Education Network (NREN). The 2015 African Journal of Computing & ICT.

[16] I.S.M.H.a.T.M Rober Morgus, "National CSIRTs and Their Role In Computer Security Incident Response, " GPPi, 2015

[17] CERT-In. http://www.cert-india.com/(2014). Retrieved 2014, from CERT-In website.

[18] CNCERT. About us: CNCERT website. Retrieved 12 23, 2014, from CNCERT website: http://www.cert.org.cn/

[19] J. Carpenter and J. Haller (2010). Establishing a National Computer Security Incident Response Team (CSIRT) . (J. Allen, Interviewer)

[20] European CyberSecurity Journal : Strategic Perspective on CyberSecurity Management and Public Policies A Multistakeholder Approach To Cybersecurity Policy Development Lea Kaspar and Matthew Shears Volume 3 (2017)▪ ISSUE 3

[21] K. Salamzada. Z. Shukur and M. Abu Bakar (2015). A Framework for Cybersecurity Strategy for Developing Countries: Case Study of Afghanistan. Asia-Pacific Journal of Infrmation Technology and Multimedia, Vol(4), No 1 (2015)

[22] CERT Australia (website). Retrieved 21 Feb, 2018 [Online]. Available: https://www.cert.gov.au/news/cyber-security-challenges-2018

[23] Benjamin Dean and Rose McDermott, A Research Agenda to Improve Decision Making in Cyber Security Policy, 5 Penn. St. J.L. & Int'l Aff. 29. Available at: http://elibrary.law.psu.edu/jlia/vol5/iss1/4