Cyber Incident Management in Low-Income Countries - 1

PART 1: A HOLISTIC VIEW ON CSIRT DEVELOPMENT

By Hountomey, J., Bahsi, H., Tatar, U., Hashem, S., Dubois, E.

A Report Created for the Global Forum on Cyber Expertise (GFCE)

GFCE
Global Forum on Cyber Expertise

Global Affairs Canada
Affaires mondiales Canada

AfricaCERT
United Teams promoting Cybersecurity in Africa

Disclaimer

The report an output of a research project that the Global Forum on Cyber Expertise (GFCE) commissioned as part of its Global Cyber Capacity Building Research Agenda 2021. Global Affairs Canada funded the project. AfricaCERT assembled a team of Researchers: Jean-Robert Hountomey (AfricaCERT), Hayretdin Bahsi (Tallinn University of Technology), Unal Tatar (the State University of New York at Albany), Sherif Hashem (George Mason University), Elisabeth Dubois (the State University of New York at Albany).

The information, interpretation, and examples set out in this report do not constitute official or informal opinions or positions of the GFCE, its Secretariat, its members, partners, or any government. Neither the GFCE nor its members may be held responsible for the use of the information contained therein.

Through the Global Cyber Capacity Building Research Agenda mechanism, the GFCE aims to identify and address knowledge gaps relevant to ongoing GFCE work and members' capacity-building activities. For this research project, the topic was identified in 2020 by the Cyber Incident Management Task Force members under the Working Group on Cyber Incident Management and Critical Infrastructure Protection. More information about the Working Group is on the GFCE website.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

We would like to thank the Global Forum on Cyber Expertise for supporting the research resulting in this report. We would also like to thank the members of the project oversight group for their feedback to improve this report:

- Klée Aiken, Principal Pacific Partnership Advisor at CERT NZ and GFCE Research Committee Member
- Abdul-Hakeem Ajijola, Chair of GFCE Working Group B (Cyber Incident Management and Critical Infrastructure Protection)
- Richard Harris, Principal Cybersecurity Policy Engineer at MITRE Corporation and GFCE Research Committee Member
- Maarten van Horenbeeck, GFCE WG B Taskforce on Cyber Incident Management Lead

ABBREVIATIONS

AFNOG	The African Network Operators Group
APCERT	Asia Pacific CERT
APNOG	The Asia Pacific Network Operators Group
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
ENISA	European Network and Information Security Agency
FIRST	Forum of Incident Response and Security Teams
GFCE	Global Forum on Cyber Expertise
ICANN	Internet Corporation for Assigned Names and Numbers
ITU	International Telecommunication Union
LACNOG	Group of Network Operators of Latin America and the Caribbean
M3AAWG	The Messaging, Malware and Mobile Anti-Abuse Working Group (M^{3}AAWG)
NANOG	The North American Network Operators' Group
N-CSIRT	National CSIRT or CSIRT with national responsibilities
OAS	Organization of American States
OIC-CERT	The Organisation of The Islamic Cooperation Computer Emergency Response Team
PSIRT	Product Security Incident Response Team
RIR	Regional Internet Registry
SIM3	Security Incident Management Maturity Model
SOC	Security Operations Center
TLP	Traffic Light Protocol

EXECUTIVE SUMMARY

Cyber-attacks know no borders. In the digitally connected world, no region or country is secure against cyber-attacks. Preventive or reactive countermeasures require collaboration, coordination, and engagement of various organizations, government bodies, the private sector, academia, and citizens of different countries.

National Computer Security Incident Response Teams (N-CSIRTs) have been deemed active and necessary systems in defending against and preventing cyberattacks and cybercrimes, supporting a nation's cyber capacity, and limiting the harm to citizens, businesses, and governments. Although there are universal calls for establishing CSIRTs at the national level, especially toward protecting critical infrastructures and lives from cyber threats, various discrepancies exist based on a nation's resources, cultural context, capabilities, and needs. Globally many countries have established a national CSIRTs or CSIRTs with national responsibilities, referred to in this report as "N-CSIRTs." However, several low-income countries are left behind or face cyber threats and related challenges.

This report discusses the findings and recommendations of the "Cyber Incident Management in Low-Income Countries" project, funded by Global Affairs Canada. The project aims to create a tailorable guide for low-income countries to develop or improve their CSIRT capabilities in an affordable way to respond to the evolving cyber threat environment effectively. Part 1 of the report comprises a thorough desk review of academic and grey literature (e.g., reports of security vendors, independent organizations, government entities, N- CSIRTs). It lists the N-CSIRT services and identifies organizational models, applied incident handling processes, workflows, required human skill sets, training resources, applicable toolsets, maturity assessment methods, and best practices in capacity development.

This study conducted a thorough review of NSIRTs to highlight their development, successes and shortcomings, and solutions for growth. The content of this literature review is presented in five sections, to aid in identifying the maturity models of CSIRTs, review best practices, highlight the legal frameworks, and report on NSIRTs development case studies. This literature review provided significant insight into the survey development for this project.

The project team reviewed studies in academic and grey literature and white papers regarding the technological, organizational, and human resource aspects of N-CSIRTs. It is important to note that although CSIRTs may refer to various entities such as organizational CSIRTs, coordination centers, N-CSIRTs, product CSIRTs, Managed Security Service Providers, this study focuses on National CSIRTs and CSIRTs with national responsibilities (N-CSIRTs) [1]. However, we explored the various aspects of the general CSIRT structures to establish a baseline for our focus on N-CSIRTs.

The project team investigated in section 2 maturity models developed for CSIRTs, CSIRT communities, and their acceptance criteria and identifies the usable sources for understanding the maturity level of national cybersecurity efforts and their relation to N-CSIRT development. Section 3 concentrated on reviewing the documents that provide guidelines and best practices about the development of N-CSIRTs. Section 4 explores the legal frameworks regarding the establishment and operation of N-CSIRTs. In Section 5, the project team reflected on the reported case studies about the establishment and development of N-CSIRTs in some countries. The literature review provided significant insight into the survey developed for this project.

NATIONAL COMPUTER SECURITY INCIDENT RESPONSE TEAMS: A LITERATURE REVIEW

1. INTRODUCTION

The project team reviewed the studies in academic and grey literature regarding the technological, organizational, and human resource aspects of N-CSIRTs. It is important to note that although CSIRTs may refer to various entities such as organizational CSIRTs, coordination centers, N-CSIRTs, product CSIRTs, Managed Security Service Providers, this study focuses on N-CSIRTs [1]. However, we explored the various aspects of the general CSIRT structures to establish a baseline for our focus on N-CSIRTs.

The content of this literature review is as follows: Section 2 reviews the maturity models developed for CSIRTs, analyzes the main international CSIRT communities and their acceptance criteria, and identifies the sources that can be utilized for understanding the maturity level of national cybersecurity efforts and their relation to N-CSIRT development. Section 3 concentrates on reviewing the documents that provide guidelines and best practices about the development of N-CSIRTs. The legal frameworks regarding the establishment and operation of N-CSIRTs are reviewed in Section 4. In Section 5, we analyzed the reported case studies about the establishment and development of N-CSIRTs in some countries.

2. CSIRT DEVELOPMENT AND MATURITY ASSESSMENT

2.1. Maturity Models

N-CSIRTs should excel in their services to be trusted nationally and globally [2]. The maturity models are essential instruments for assessing organizational development in various domains, including incident management. In this section, we analyzed the models that evaluate the capabilities of CSIRTs.

The Security Incident Management Maturity Model, recognized as SIM3, constitutes the main CSIRT maturity assessment approach in Europe [3]. The Task Force on Computer Security Incident Response Teams (TF-CSIRT), the Nippon CSIRT Association (NCA), and the GFCE have adopted this model [4]. It identifies 44 maturity parameters (criteria) classified into four quadrants; organizational, tools, human, processes. SIM3 measures the level (0-4) of each parameter. The lowest level, 0, indicates an unaddressed parameter, whereas the highest level, 4, reflects that the criteria are formally defined, applied, and assessed.

The European Union Agency for Cybersecurity (ENISA)'s maturity model mainly uses SIM3 but introduces three stages for the maturity progress: basic, intermediate, and advanced. These stages act as a characterizing and guiding instrument for the development of CSIRTs [4]. As this study addresses countries likely to be in the early stages of improving their capabilities, the research team evaluated the basic and intermediate stages of the ENISA's model. The basic stage demands a higher level (i.e., 3) for most organizational criteria, directing initial efforts in establishing CSIRT towards that quadrant. CSIRTs teams that fall into either 1, 2, or 3 categories for human resources or governance for the ENISA model are of interest to this study. CSIRTs pursuing the intermediate stage should have the highest maturity level, 4, in organizational parameters such as Mandate, Constituency, Authority, Responsibility, Service Description, and Participation in Existing CSIRT Frameworks. These CSIRTs should demonstrate improvement in most of the "tools" parameters at level 2 and progress in several "human" and "process" parameters.

ENISA has provided a peer-review methodology for SIM3 [4]. Trusted Introducer (TI) has established a certification scheme based on SIM3 and determined minimum levels for each criterion [5]. Mainly, the organizational category requires higher maturity levels, and CSIRT should achieve at least two or above in all criteria (e.g., except two criteria) in this scheme [6]. The advanced stage introduced by ENISA has higher maturity requirements than this certification demands [5].

ENISA foresees a five-year development period for reaching the advanced level for any CSIRT team, one year for the basic stage, two years for the intermediate, and two years for the advanced stage [4]. It is important to note that the above maturity frameworks apply to any CSIRT team, not specific to N-CSIRTs. However, national teams may prioritize some categories such as organizational ones or assign lesser priority to criteria associated with incident prevention as they may not directly have such responsibilities [7].

CREST, an international not-for-profit accreditation and certification body, representing and supporting the technical information security market, has also developed a framework and a maturity model assessment methodology [8]. CREST's cyber incident management framework consists of three main phases, prepare, response and follow-up, with 15 steps in total [9]. The assessment levels include five categories (0-4), foundation, emerging, established, dynamic, and optimized. Compared to CREST's framework, SIM3 presents more comprehensive evaluation criteria, especially regarding the organizational aspect. Both frameworks are relevant for self-and peer-review (i.e., Open CSIRT Foundation offers a self-assessment tool for SIM3 [10]).

Carnegie Mellon SEI built a baseline or benchmark of incident management practices for an organization [11]. A series of indicators and statements define the benchmark. An organization can use this benchmark to assess its current incident management function for process improvement. SEI also provides a form of categorization called the CSIRT Capacity development continuum that provides five capacity levels (level 0 to level 5), development stages, and outcome [12].

2.2. Trust-Building Networks

The Trusted Introducer Service (TI) has established a trust-building clearinghouse for its CSIRT community by introducing three engagement categories, listed, accredited, and certified [13]. CSIRTs provide basic information about themselves according to the RFC2380 for the listed category. Accredited members have to demonstrate that they apply best practices and conform to TI policies. Certified members pass through a rigorous assessment to justify that their maturity meets the relevant criteria set by TI [5].

The Forum of Incident Response and Security Teams (FIRST) has a CSIRT membership model [14] based on the conformance to evaluation criteria and site visit outcomes [6]. Asia Pacific CERT (APCERT) has a similar membership model and acceptance procedure [6]. AfricaCERT, as a regional CSIRT organization for Africa, has operational and associate member status for N-CSIRTs. The membership requirements include less strict conformance criteria [15]. Likewise, the Organisation of The Islamic Cooperation – Computer Emergency Response Teams (OIC-CERT) encompasses vast geography that includes predominantly Islamic countries [16]. OIC-CERT membership consists of six primary levels: Full Member, General Member, Professional Member, Affiliate Member, Commercial Member, and Fellows Member. In this, the full member status applies to national-level CSIRTs.

The Trusted Introducer Service provides the most robust membership criteria. The service differentiates teams according to their demonstrated and checked levels of maturity. It is important to note that TI is the only one that utilizes a maturity model as a baseline evaluation approach. As of March 2021, TI has 32 certified, 184 accredited, and 177 listed members [17], and FIRST has 566 team members [18].

In addition to the international communities outlined above, the countries can benefit from bilateral or multi-lateral collaborative activities [2]. A buddy nation can help a less-mature N-CSIRT enhance its capabilities [2].

2.3. Sources for National Cybersecurity Indicators

To our knowledge, the most comprehensive indicators regarding the progress of N-CSIRTs can be derived from the results of Global Cybersecurity Index studies conducted by the International Communication Union (ITU) [19]. These studies aim to evaluate the cybersecurity commitment of the countries based on their responses to the detailed questionnaires sent by ITU. CGI forms twenty indicators categorized into five pillars, legal, technical, organizational, capacity building, and cooperation. Since 2014, ITU has created a scoring system that evaluates each indicator and identifies the overall level of each country. In 2018, 155 countries submitted their reports, increasing to 194 in 2020 [20].

Although these studies address the whole national cybersecurity governance framework and capabilities, they do not directly analyze the maturity levels of N-CSIRTs. They evaluate the CSIRT ecosystem in the respective country under the technical pillar. They may help approximate comprehending the CSIRT developments. The relevant indicators from organizational measures, capacity building, and cooperation pillars could provide additional support for understanding the effectiveness of CSIRTs. One important note is that the 2017 Global cybersecurity index report gives detailed results for each country indicator, while the 2018 report listed only the overall score. The most recent report published in 2020 provides country profiles for each respondent and identifies the areas of relative strength and areas of relative growth.

Estonian e-Governance Academy (EGA) has created and maintained a database, the National Cybersecurity Index, which includes measurements about the readiness of countries for managing cyber incidents [21]. The countries send their official documents or show links to the publicly available official data to the EGA. EGA researchers also identify public resources by conducting online research. The sources must be in English. Academy collects 46 indicators under three categories, general cybersecurity indicators, baseline indicators, and incident and crisis management indicators. The indicators address various aspects of national cybersecurity governance. Similar to the ITU index, there are specific N-CSIRT indicators or related functions (i.e., 9.1 Cyber Incident Response Unit, 9.3 Single Point of Contact for International Coordination, 2.1 Cyber Threat Analysis Unit). As of March 2021, the index has data from 160 countries.

Global Cybersecurity Capacity Center (GCSCC) created the Cybersecurity Capacity Maturity Model (CMM) that evaluates the national-level capacity, similar to the efforts of ITU and EGA [22]. The model consists of five dimensions: (1) Cybersecurity policy and strategy, (2) Cybersecurity culture and society, (3) Building cybersecurity knowledge and capabilities, (4) Legal and Regulatory Frameworks, (5) Standards and Technologies. Each dimension has multiple factors formed of various aspects. Five stages (start-up, formative, established, strategic and dynamic) define the degree to which a country has progressed concerning a specific Factor. Dimension 1: “Cybersecurity Policy and Strategy” covers N-CSIRT in the “Incident Report and Crisis Management” factor. This model has the richest indicator set provided for each maturity stage compared to the models introduced above. The CMM has been deployed more than 120 times in over 87 nations around the world.[23].

It is important to note that index studies, ITU and EGA, do not evaluate the maturity levels. They are more oriented to assess whether relevant cybersecurity organizations, frameworks, and programs are effective in the corresponding country. However, they can provide systematic and comparable information about the cybersecurity practices of the countries and enable us to derive some insights, especially about the indicators at lower maturity levels, as those levels are more focused on the existence of building blocks rather than their effectiveness. On the other side, the model of GCSCC has more clear indicators based on the five maturity levels.

The Organisation for Economic Co-operation and Development has published guidance for improving the comparability of statistics produced by Computer Security Incident Response Teams [24]. The report explored the challenge of collecting relevant statistics for an informed policy decision. The report addresses two aspects of measurement: CSIRT capacity resourcing to effectively mitigate security incidents and the security incidents that CSIRT handles. In addition, the report explores future work areas such as risk conditions, capacity, and incident data.

N-CSIRTs and regional CSIRTS organizations produce monthly and annual reports, including various statistics. Organizations such as CyberGreen have developed and applied statistical methods to measure indicators of malicious activity and risk conditions. In addition, Organizations such as “The Shadowserver Foundation”, “Team-Cymru”, and “The Anti-Phishing Working Group (APWG)” provide reports that can help CSIRTs enhance their incident response coordination.

3. N-CSIRT GUIDELINES & BEST PRACTICES

Maturity models indicate areas of organizational settings improvement, but they do not answer how to improve [25]. Although the upper maturity levels indicate some process characteristics such as documentation, upper management approval, or feedback cycles, they do not guide service assignment and management. On the other side, various organizations such as ENISA, CERT/CC, FIRST, GFCE (including Cybil), and others have published many guidelines and best practice documents about CSIRTs and N-CSIRTs. Many academic or non-academic resources present main challenges in maturity development. N-CSIRTs in low-income countries (and CSIRTs with few resources) need more help transitioning their maturity assessments into actionable programs. Navigating through the maturity curve requires prioritization, management, and utilization of respected guidelines and best practices.

3.1. CSIRT Services

Many CSIRTs have adopted the RFC 2350 best current practice and the outline for CSIRT template for publishing their capabilities and services [26]. FIRST published a comprehensive framework document that presents a potential service portfolio for CSIRTs [27]. The CSIRT services framework classifies the services into five categories: information security incident management, vulnerability management, information security event management, situational awareness, and knowledge transfer. FIRST extended the usual incident handling services with a new category, Product Security Incident Response Team (PSIRT), and published a service framework document [28]. The PSIRT services framework addresses product development companies by framing the security teams that conduct vulnerability management throughout the secure development life cycles. Although CSIRTs depend on information published by PSIRTs to address security issues, N-CSIRTs can promote the establishment of PSIRTs in the national framework. However, these services are out of their scope.

Carnegie Mellon University Software Engineering Institute (CMU-SEI) grouped the CSIRT services into reactive, proactive, and security quality management services [29]. The services such as incident and vulnerability handling are reactive. Proactive services include broad content ranging from intrusion detection services to security assessments and maintenance of security infrastructures. The quality management service category covers the efforts related to training, awareness, consulting, risk analysis, and product evaluation. Although CMU-SEI's document provides a comprehensive service list, this list includes various operational security services, attributing a broad meaning to the CSIRT notion.

In CMU-SEI's publication, reactive services such as alerts and warnings, incident handling, vulnerability handling, announcement as a proactive service, and quality management services such as awareness building and security consulting are the core services of CSIRTs [30]. Incident management, communication with the constituency, and situational awareness are considered the minimum service or operation areas of N-CSIRTs in GFCE's guideline [2].

Although some well-developed N-CSIRTs or similar national cybersecurity centers have also established situational awareness and event management services [31], they commonly deliver knowledge transfer and incident management services. Achieving high quality in a few services rather than many degraded or unassigned services is prescribed for trustworthiness as a core principle in local and international CSIRT communities [32].

Extending the responsibilities of N-CSIRTs beyond the commonly known services, a noteworthy service category proposal named "long-term resiliency services" is provided by Clark et al. [33]. This category lists key strategic responsibilities such as creating knowledge-sharing platforms and frameworks for sectors (e.g., critical infrastructures), establishing public-private participation networks, and initiating and supporting national cybersecurity research activities. In countries where an initial national framework is well-established, the N-CSIRTs could carry those responsibilities. Nevertheless, N-CSIRTs can trigger or support national cybersecurity framework development efforts in countries with less mature cybersecurity frameworks.

N-CSIRTs can also stimulate efforts to develop sectoral CSIRTs that aim to foster a sector's cybersecurity capabilities. CMU-SEI has published a sector CSIRT framework for developing sector-based incident response capabilities. SEI [34].

3.2. Organizational Values, Models, and Processes

An N-CSIRT should build its values around cooperation, trust, and transparency [2]. The ideas of information sharing and working together should be the core part of the organizational value system so that the other parties and constituencies would trust the CSIRT as a coordination point. The mission and activities should be transparent to society as any hidden goals have been detrimental to trust. On the other side, N-CSIRTs should respect its constituencies' and partners' confidentiality and privacy requirements. They should take necessary physical and cybersecurity countermeasures to protect the relevant information.

According to Nyre-Yu et al., organizational structure and policies significantly impact the performance of CSIRT teams [35]. The GFCE Global Good Practices indicates (1) N-CSIRTs should have a clear and officially approved mandate to fulfill a national responsibility; reflecting the highest level of political and legislative support(2). The responsibilities and constituencies need to be clarified. N-CSIRTs should be equipped with the necessary authority to fulfill their tasks, (3) N-CSIRTs should consult legal experts about the legal boundaries of their operations, and (4) N-CSIRTs should also be part of the national crisis management structure [2].

The CSIRT builds its service portfolio, identifies and allocates resources. Securing relevant funds is essential for sustaining the organizational structure of the N-CSIRTs. As governments start to include cybersecurity in their agendas and publish national-level strategies, CSIRTs often receive continuous and solid funding. However, less-developed countries have had fewer funding alternatives when compared to developed ones [36]. Jalal et al. of the Afghanistan CSIRT indicate that government sponsorship, fee-based services, in-kind supports, or a combination of these could be funding alternatives for N-CSIRTs [37].

Many CSIRTs operate lists of tools and implement processes aimed at helping build capacity or improve their effectiveness. The National Cybersecurity Centre in the Netherlands guides and other CSIRT guides discuss the importance of proper tools and how their lack can affect operation excellence. Organizational learning from the incidents requires a well-established lessons-learned procedure. [38].

CSIRTs maintain an IT resource list to keep track of the physical and virtual tools and IT assets vital for business operation. The tools include centralized and accurate asset management systems, team cooperation tools, consolidated email and incident tracking systems, forensics and malware analysis tools, monitoring and detection tools, cyber threat intelligence systems as well as feeds. As incident loads increase and cyber threats grow, using automation tools helps improve incident response and influence the meantime to acknowledge (MTTA) and mean time to remediate (MTTR) that measure how well security operations can reduce organizational risk.

FIRST developed Traffic Light Protocol (TLP) to classify information exchanged among the security communities [14]. Many CSIRT communities adopted TLP. FIRST introduced a framework for exchanging information among the relevant partners in CSIRT and security ecosystems [39].

TF-CSIRT proposes a code of conduct to its members [40]. FIRST, APCERT, OIC-CERT, and AfricaCERT have similar documents [41], [42]. FIRST's Ethics Special Interest Group has developed EthicsfIRST [43] aimed to guide the ethical conduct of all team members, including current and potential practitioners, instructors, students, influencers, and anyone who uses computing technology in an impactful way. While an N-CSIRT may receive, process, or generate information about zero-day vulnerabilities, it should apply a clear responsible disclosure policy [44]. A document by the Dutch National Cybersecurity Center, "Coordinated Vulnerability Disclosure: The Guideline," provides an example of a responsible disclosure policy [45].

Although the SIM3 model identifies maturity levels, the model does not provide any guidance about the key performance indicators or metrics for gap analysis and evaluation of the team's effectiveness. A systematic mapping describes several key indicators and metrics related to the cost, quality, and service (time) involved in incident management [46]. However, the study does not present a comprehensive synthesis of the findings, and most of the indicators are related to more operational security aspects.

CMU-SEI published assessment questions and indicators regarding the incident management processes of an organization, which apply to any CSIRT, not necessarily an N-CSIRT [47].

3.3. Human Resources and Required Skills

The allocation and development of relevant human resources are tightly connected to organizational goals [35]. N-CSIRTs should have enough technical experts and at least one policy expert to handle policy and regulatory-related tasks, including information sharing with other state and non-state actors [44]. In the relevant CMU-SEI publication, CSIRT staff members require two skills categories: personal skills and technical skills [48]. Communication, presentation, diplomacy, ability to follow policies and procedures, teaming, critical thinking, problem-solving, time management, integrity, and coping with stress are personal skills. Technical skills make two categories: technical foundation and incident handling skills. The former covers the topics of common understanding. The list includes the knowledge of security principles, fundamentals of vulnerabilities and attacks, risks and risk management, network protocols/applications/services, network and host security issues and malicious code. It is recommended that some team members have programming experience, especially if the N-CSIRT uses open-source tools. Incident handling skills address the operational knowledge that encompasses technical problems such as possible intrusion methods, organizational policies and processes regarding the incident analysis.

3.4. Communication and Information Exchange Channels

3.4.1. Communication with National Entities

According to GFCE Global CSIRT Best Practices, an N-CSIRT should have well-established information exchange channels national entities such as: (1) law enforcement bodies, (2) national crisis management organizations, (3) public policymakers (i.e., especially the policymakers in the area of cyberspace), (4) national intelligence/security agencies, (5) academics/ researchers, and (6) province and territorial governments[2]. Communication with critical infrastructure organizations and their regulators should be added to the list.

3.4.2. N-CSIRT Development Programs

ITU has established various levels of N-CSIRT capacity building and assessment programs for countries. ITU assessed the N-CSIRTs of 79 countries and contributed to the development of 14 N-CSIRTs.

The Member States of the Inter-American Committee against Terrorism (CICTE) of the Organization of American States (OAS) developed a cybersecurity program that includes policy development, capacity building, and cybersecurity research. This program has contributed to the establishment of 17 national CERTs in the region.

Several organizations and delivery partners such as Worldbank, ITU, SEI, Cyber4Dev, the Home Office National Cyber Risk Assessment Team (UK), APNIC, and many others, deliver cyber risk assessments and support N-CSIRT capacity building worldwide.

3.4.3. Conferences and Events Regarding CSIRTs

FIRST organizes annual gatherings, various trainings, workshops, and other events [49]. Regional CSIRT organizations such as TF-CSIRT [50], APCERT [51], OIC-CERT [52], AfricaCERT [15], [53], and OAS [54] have similar event and training activities. Cybersecurity events and technical discussions are organized globally by countries' cybersecurity agencies, RSA, BlackHat, etc. [55]. ISC2, Offensive Security, EC-Council, CompTIA, and PECB are all organizations that provide training courses relevant for CSIRTs. SANS is another significant training organization that holds various technical trainings in different regions [56]. Similarly, security researchers exchange the latest attack techniques at Defcon [57].

SEI organizes an Annual Technical Meeting for CSIRTs with National Responsibility for technical and managerial staff members of National CSIRTs to share information, tools, techniques, and strategies that address problems unique to CSIRTs that are responsible for a nation or economy.

Network Operators groups such as NANOG, LACNOG, AfNOG, APNOG, and Internet players such as M3AAWG, RIRs, ICANN, Internet Society, Top-level domain (TLD) registry operators also facilitated workshops for incident responders.

3.4.4. National & International Cybersecurity Exercises

N-CSIRTs participate in various cybersecurity exercises organized by various international and regional organizations. ITU organizes global and regional cybersecurity exercises (cyber drills) to develop the readiness and incident handling capabilities of CSIRTs [58]. Lock Shields, conducted by NATO Cooperative Cyber Defence Excellence Center (NATO CCDCOE), is an annual technical cybersecurity exercise for NATO countries [59]. ENISA conducts EU-level cyber incident and crisis management exercises [60]. Numerous resources are available for conducting exercises such as the guideline for developing cyber exercises published by MITRE [61].

Regional CSIRT organizations organise various cybersecurity exercises within their constituencies. As example, 25 CSIRTs from 19 economies joined the 2021 annual cyber drills of the Asia Pacific Computer Emergency Response Team (APCERT) [62]. OIC-CERT organizes drills each year [63]. Likewise, Singapore hosts annual cyber incident exercises for ASEAN Member States (AMS) and Dialogue Partners [64].

IMPROVING CAPABILITY WITH CYBER DRILLS

Regional incident response and security teams use Cyber Drills to test their members' communication and response capability with scenarios to test members' preparedness for various cyber issues. The exercises also provide opportunities for regional collaboration, trust, and confidence-building.

AfricaCERT

AfricaCERT organized its first Cyber Drill: "Testing the Waters," in 2021. The Drill aimed to test the response capability of participating teams facing the following scenarios: Phishing, Defacement, REM, Ransomware investigation. These exercises were designed to put participants into live conditions and tested their communication and technical capabilities. 32 Computer Security Incident Response Teams from 24 countries, including APCERT and OICCERT economies teams, participated in the Drill.

APCERT

APCERT organized every year a Cyber Drill for APCERT Region and partners. The theme of the 2021 APCERT Drill was "Supply Chain Attack through Spear-Phishing - Beware of Working from Home -." The exercise reflected real incidents and issues reflected the collaboration amongst the economies in mitigating cyber threats and validates the enhanced communication protocols, technical capabilities, and quality of incident responses that APCERT fosters in assuring Internet security and safety. 25 CSIRTs from 19 economies of APCERT and 2 economies of OIC-CERT and AfricaCERT participated.

The ITU

The ITU organizes annual Cyber Drills designed with a dual purpose: as a platform for cooperation, information sharing, and discussions on current cybersecurity issues, as well as to provide hands-on exercise for national Computer Incident Response Teams (CIRTs) / Computer Security Incident Response Teams (CSIRTs).

OAS

OAS (Organization of American States) and INCIBE (Spanish National Cybersecurity Institute) organizes every year International CyberEx that seeks to strengthen the ability to respond to cyber incidents and improve collaboration and cooperation. International CyberEx 2020 had 80 teams and 320 team members representing 39 countries.

OICCERT

The Organization of the Islamic Cooperation - Computer Emergency Response Teams (OIC-CERT) organizes an annual Cyber Drill with the objectives to:

- Test the communication capabilities of the members' points of contact.
- Check the processes and procedures in managing contingencies.
- Test the technical competencies of participating teams.
- Simulate cross-border cooperation in mitigating information security incidents.

3.4.5. Policy and Governance Events

The Internet Governance Forum's annual and regional gatherings are significant venues for discussing Internet policy, governance, and technical issues [65]. Africa Internet Summit and related regional events covers various technical and governance topics related to the ICT area [66].

Discussion such as those arising from the United Nations Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, as well as the United Nations [67] Open-Ended Working Group (OEWG) [68], and their most recent reports in 2021 [69], [70], emphasize the importance of capacity building and highlight possible roles and responsibilities of N-CSIRTs in supporting the implementation of cyber norms and confidence-building measures in manage cyberspace risks [69]–[71].

3.5. Partnerships and Collaborations

Some donor countries have invested resources to support the cybersecurity capacity-building efforts of other less-developed countries. Such efforts, which do not solely focus on CSIRT development, have been classified into four categories: (1) Methodological, (2) Technical, (3) Infrastructural, (4) Budgetary [72]. Methodological studies refer to research regarding national governance models or policy options, e.g., Cybersecurity Capacity Maturity Model [73], National Cybersecurity Framework Manual [74]. Technical studies are mostly based on the trainings given to CSIRTs or community-based support.

The Japan Computer Emergency Response Team Coordination Center (JPCERT/CC), CERT/CC, Estonia, ANSSI France, the UK Home office support other nations in capacity building [75]. JPCERT/CC supported Tanzania and Fiji with training and workshops [72]. South Korea's Korea's KISA, the mother organization of KrCERT/CC, has dispatched skilled KrCERT/CC staff to Rwanda to provide training activities. Cyber threat intelligence organizations such as "The Shadowserver Foundation", "Team-Cymru", and "The Anti-Phishing Working Group (APWG)" are part of community-based technical assistance. Telecommunication infrastructure projects cover various training, including cybersecurity options. [72]. In the budgetary support option, the donor country directly sponsors operational expenses.

4. LEGAL FRAMEWORKS

It is highly recommended that the status and the responsibilities of the N-CSIRT are defined in national-level legislation, regulation, policy, or a strategy [2]. In various countries, a locally established CSIRT first assumes an N-CSIRT or fulfills that role without formal approval. At this stage, while this organization starts building trust in the related ecosystem by carrying out some vital CSIRT services, it may promote cybersecurity awareness among the high-level policy circles and aim to have a formal status (e.g., Tunisian case [76]). Even such an achievement can indicate a milestone in establishing a national governance structure.

The EU Network and Information Security Directive (NIS Directive) urges member states to establish CSIRT units equipped with incident coordination responsibilities, emphasizing participation in the international cooperation networks [77].

5. SPECIFIC NATIONAL PRACTICES

The experience of the Netherlands exemplifies how initial CSIRT efforts have evolved into a well-established National Cybersecurity Center (NCSC-NL) with nationwide key operational, tactical, and strategic responsibilities [33]. The Netherlands has a mature cybersecurity framework and has published three national strategy documents. NCSC-NL is TI certified and ranked 12 in the ITU Global Cybersecurity

Index of ITU. GOVCERT.NL's initial service portfolio includes incident management, publishing alerts and advisories, and conducting awareness and training activities for government networks. It became a national coordinator for cyber incidents and acted as a national contact point. The organisation has then transitioned into NCSC-NL, extended its scope with critical infrastructures, and launched strategic services to establish private-public partnerships and initiate research and education activities. Other N-CSIRTs in Europe have transitioned through similar phases [33].

Tunisian N-CSIRT, tunCERT, was launched in 1999 [71]. The initial challenges have been identified as a lack of awareness, experts, and money. The team first approached politicians and policy-makers and increased their awareness, in turn, obtained short-term budget and assistance. Information sharing events have been established with the cybersecurity communities, including CISOs and security professionals. The open-source tools have been promoted due to budget constraints. This CSIRT has engaged in various awareness campaigns addressing the whole population.

Columbian N-CSIRT, colCERT, differs from similar CSIRTs as it constitutes one umbrella organization covering cyber defense, cybercrime fighting, and usual CSIRT units [73]. CSIRT of Afghanistan, AFCERT, mainly gives support to cybercrime investigations but does not fulfill basic N-CSIRT functions such as incident coordination, information sharing, and cooperation with other countries [37]. It is important to note that a significant function of an N-CSIRT is to engage with the citizens, different sectors, and CSIRTs of other countries and promote sharing of incidents and other relevant domain knowledge. Although these organizations usually work closely with other law enforcement agencies when needed,

Three CSIRTs selected from the government, academia, and private sector in Ecuador have been assessed based on the SIM3 model and found to be lower than the basic level [74]. The lack of clear organizational objectives and experienced security professionals were the main reasons for not having a successful implementation of the CSIRT in the country.

Cambodia launched its N-CSIRT in 2007. A study, published in 2009, provides a guideline for improving the capabilities of Cambodian N-CSIRT and gives a special emphasis on the development of the technical capability and also hiring policy experts [75]. It is recommended that CSIRT should not only rely on government funds but seek other sources as well. Another noteworthy proposal given in this document is that a bureaucratic government entity should take the lead in cybersecurity policy development efforts, and N-CSIRT should support this organization in technical matters. The establishment of sectoral CSIRTs is considered a service by some N-CSIRTs. For example, South African N-CSIRT [76] provides services for ICT, Financial, and Retails sectors [77].

EG-CERT EXPERIENCE

Background

Egyptian national Computer Emergency Readiness Team (EG-CERT) was launched in April 2009. EG-CERT is affiliated with the Egyptian National Telecom Regulatory Authority (NTRA), and provides support to the ICT sector, the financial sector as well as the governmental sector, in order to help them tackle Cybersecurity threats and deal with significant cyber incidents such as distributed denial of services (DDOS) attacks. EG-CERT provides both reactive as well as proactive services, including incident handling, cyber forensics, malware analysis, vulnerability assessment, and penetration testing.

Currently, EG-CERT employs over 60 professionals (45+ are full-time cybersecurity professionals). EG-CERT prepares over 250 penetration testing reports annually for its constituents and for relevant authorities and key organizations [78].

Initial Capacity Building Efforts to Jump-Start EG-CERT and its Constitutes

As soon as EG-CERT assumed its national responsibilities, providing support to key critical information infrastructure (CII) entities, it was immediately realized that empowering those responsible for CIIP in the critical sectors, and enhancing their technical skills, should be of upmost priority. Hence, a pilot national cybersecurity training program was organized and sponsored by the NTRA between 2009-2010, for training 220 professionals in 38 organizations within the governmental/public sector, banking sector, education sector, as well as from ICT private sector companies (Telecom companies, mobile operators, CSPs, banks, etc.). The program covered key cybersecurity topics: security essential, incident handling, penetration testing and ethical hacking, perimeter security, advanced wireless penetration testing and ethical hacking. As an outcome of the program, 179 of those professionals obtained international certificates from SANS, some of them obtained up to 4 different advanced cybersecurity certificates within the program. The launch of the pilot training program had an immediate positive impact in creating awareness, enhancing readiness, and establishing a network of trust and enhanced cooperation spirit among participating entities as well as among professionals. The financial sponsorship from the NTRA was also a strong message of commitment, partnership and support from a leading public entity, a message that extended beyond professionals from public sector to partners from the private sector, and even beyond the telecom sector to other critical sectors. The success of the pilot training program inspired several programs among various sectors, and was recognized by the ITU in its Global Cybersecurity Index & Cyber wellness Profiles published in 2015 [79], where Egypt was one of two countries worldwide to receive a perfect score of (1.0) in Capacity Building. Successful Egyptian cybersecurity initiatives and activities has led to the advanced cybersecurity rank that Egypt has achieved in 2020 (23rd among 194 countries) as reported by the International Telecommunications Union (ITU) Global Cybersecurity Index [20].

EG-CERT and the National Cybersecurity Strategy

EG-CERT participated in developing the first Egyptian National Cybersecurity Strategy in 2017 [80], and has taken the role of the "Technical Arm" of the Egyptian Supreme Cybersecurity Council (ESCC) that was established at the Cabinet of Ministers level in 2014. EG-CERT is also assisting in the implementation of the national cybersecurity strategy, especially in developing and empowering CERT teams in critical sectors, with a special focus on the financial, energy, and transportation sectors. In parallel, plans are being implemented for developing a national security operations center (SOC) and national cybersecurity certification center.

Regional and International Cooperation

EG-CERT has broad regional and international cooperation, including the participation in annual international cyber drills with Asia Pacific – APCERT annual cyber drill (since 2012), Organization of Islamic Countries - OIC-CERT annual cyber drills (since 2012), and ITU Arab region cyber drill (since 2012). EG-CERT is a member of the international Forum of Incident Response and Security Teams (FIRST), and is a founding member of the Organization of Islamic Countries CERT (OIC-CERT) and Africa CERT.

EG-CERT has also organized several regional and international events, including an ITU Arab Regional Cybersecurity Workshop (2011), the ITU Arab regional cyber drill (2015), the ITU ARCC Regional Cybersecurity Summit (2016) and the FIRST Regional Cybersecurity Symposium for the Arab and African Region (2016).EG-CERT has cooperation agreements with Cybersecurity Malaysia, US-CERT, Uganda, Tanzania, Team Cymru, and Indian CERT. It also has strong relationships with many CERTs in the Arab region, in Africa, and across the Globe.

REFERENCES

[1] R. Ruefle, A. Dorofee, D. Mundie, A. D. Householder, M. Murray, and S. J. Perl, “Computer Security Incident Response Team Development and Evolution,” *IEEE Secur. Priv.*, vol. 12, no. 5, pp. 16–26, Sep. 2014, doi: 10.1109/MSP.2014.89.

[2] Global Forum on Cyber Expertise, “GFCE Global Good Practices - National Computer Security Incident Response Teams (CSIRTs),” 2017. [Online]. Available: https://thegfce.org/wp-content/uploads/2020/06/NationalComputerSecurityIncidentResponseTeamsCSIRTs-1.pdf

[3] D. Stikvoort, “Incident Classification/Incident Taxonomy according to eCSIRT.net – adapted.” 2015. [Online]. Available: https://www.trusted-introducer.org/Incident-Classification-Taxonomy.pdf

[4] European Union Agency for Network and Information Security, “ENISA Maturity Evaluation Methodology for CSIRTs,” ENISA, Apr. 2019. [Online]. Available: https://www.enisa.europa.eu/publications/study-on-csirt-maturity-evaluation-process

[5] Trusted Introducer, “Processes: Certification.” https://www.trusted-introducer.org/processes/certification.html (accessed Sep. 13, 2021).

[6] Trusted Introducer, “SIM3 Trusted Introducer Certification Standard,” May 2010. [Online]. Available: https://www.trusted-introducer.org/TI-Certification-Profile.pdf

[7] H. Duijnhoven, T. van Schie, and D. Stikvoort, “Global CSIRT Maturity Framework - Stimulating the Development and Maturity Enhancement of National CSIRTs Version 1.0,” Global Forum on Cyber Expertise, Jun. 2019. [Online]. Available: https://thegfce.org/wp-content/uploads/2020/05/MaturityFrameworkfornationalCSIRTsv1.0_GFCE.pdf

[8] CREST, “CREST Representing the Technical Information Security Industry.” Jan. 2019. [Online]. Available: https://www.crestapproved.org/wp-content/uploads/2019_What-is-CREST.pdf

[9] CREST, “CREST Cyber Security Incident Response Guide Version 1,” 2013. [Online]. Available: https://www.crest-approved.org/wp-content/uploads/CSIR-Procurement-Guide-1.pdf

[10] Open CSIRT Foundation, “SIM3 Self-Assessment Tool.” https://sim3-check.opencsirt.org//#/ (accessed Sep. 13, 2021).

[11] A. Dorofee *et al.*, “Incident Management Capability Assessment,” Carnegie-Mellon University Software Engineering Institute, CMU/SEI-2018-TR-007, Dec. 2018. [Online]. Available: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=538848

[12] Carnegie Mellon University Software Engineering Institute, “Security Operations Overview,” 2018. [Online]. Available: https://apps.dtic.mil/sti/pdfs/AD1068341.pdf

[13] Trusted Introducer, “Processes: Overview of TI Processes.” https://www.trusted-introducer.org/processes/overview.html (accessed Sep. 13, 2021).

[14] Trusted Introducer, “Traffic Light Protocol (TLP) — Version 1.0,” FIRST. [Online]. Available: https://www.trusted-introducer.org/ISTLP.pdf

[15] “How to become a member?,” *AfricaCERT*. https://www.africacert.org/how-to-become-a-member/ (accessed Sep. 12, 2021).

[16] Organisation of The Islamic Cooperation - Computer Emergency Response Team, “OIC-CERT All Members.” https://www.oic-cert.org/en/allmembers.html#.YT6q851KhMs (accessed Sep. 12, 2021).

[17] Trusted Introducer, “Directory : Team Database.” https://www.trusted-introducer.org/directory/teams.html (accessed Sep. 12, 2021).

[18] Forum of Incident Response and Security Teams, Inc., “FIRST - Teams,” *FIRST*. https://www.first.org/members/teams (accessed Sep. 12, 2021).

[19] “Global Cybersecurity Index,” *ITU*. https://www.itu.int:443/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx (accessed Sep. 12, 2021).

[20] International Telecommunication Union, “Global Cybersecurity Index 2020,” 2020. [Online]. Available: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

[21] “National Cyber Security Index,” *e-Governance Academy Foundation*. https://ncsi.ega.ee/ncsi-index/ (accessed Sep. 12, 2021).

[22] Global Cyber Security Capacity Centre, “Cybersecurity Capacity Maturity Model for Nations (CMM) Revised Edition,” *SSRN Electron. J.*, 2016, doi: 10.2139/ssrn.3657116.

[23] “CMM Reviews around the World,” *Global Cyber Security Capacity Centre*, Jun. 2021. https://gcscc.ox.ac.uk/cmm-reviews (accessed Sep. 12, 2021).

[24] Working Party on Security and Privacy in the Digital Economy, “Guidance for Improving the Comparability of Statistics Produced by Computer Security Incident Response Teams (CSIRTs),” OECD, DSTI/ICCP/REG(2013)9/FINAL, 2015. [Online]. Available: https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG(2013)9/FINAL&doclanguage=en

[25] C. Acartürk, M. Ulubay, and E. Erdur, “Continuous improvement on maturity and capability of Security Operation Centres,” *IET Inf. Secur.*, vol. 15, no. 1, pp. 59–75, 2021, doi: 10.1049/ise2.12005.

[26] N. Brownlee and E. Guttman, “Expectations for Computer Security Incident Response.” 1998. [Online]. Available: https://www.hjp.at/doc/rfc/rfc2350.html

[27] Forum of Incident Response and Security Teams, Inc., “Computer Security Incident Response Team (CSIRT) Services Framework Version 2.1,” FIRST, Nov. 2019. [Online]. Available: https://www.first.org/standards/frameworks/csirts/FIRST_CSIRT_Services_Framework_v2.1.0.pdf

[28] Forum of Incident Response and Security Teams, Inc., “Product Security Incident Response Team (PSIRT) Services Framework Version 1.1,” FIRST, 2020. [Online]. Available: https://www.first.org/standards/frameworks/psirts/FIRST_PSIRT_Services_Framework_v1.1.pdf

[29] M. West-Brown, D. Stikvoort, K.-P. Kossakowski, G. Killcrece, R. Ruefle, and M. Zajicek, “Handbook for Computer Security Incident Response Teams (CSIRTs),” Carnegie-Mellon University Software Engineering Institute, CMU/SEI-2003-HB-002, Apr. 2003. Accessed: Sep. 12, 2021. [Online]. Available: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6305

[30] G. Killcrece, K.-P. Kossakowski, R. Ruefle, and M. Zajicek, “Organizational Models for Computer Security Incident Response Teams (CSIRTs),” Carnegie-Mellon University Software Engineering Institute, Pittsburgh, PA, Dec. 2003. Accessed: Sep. 12, 2021. [Online]. Available: https://apps.dtic.mil/sti/citations/ADA421684

[31] H. Bahsi, “Analysis of National Cyber Situational Awareness Practices,” in *Strategic Cyber Defense: A Multidisciplinary Perspective*, vol. 48, IOS Press, 2017, pp. 31–41.

[32] National Cyber Security Centre, “CSIRT Maturity Kit - A step-by-step guide towards enhancing CSIRT Maturity,” GCCS, Apr. 2015.

[33] K. Clark, D. Stikvoort, E. Stofbergen, and E. van den Heuvel, “A Dutch Approach to Cybersecurity through Participation,” *IEEE Secur. Priv.*, vol. 12, no. 5, pp. 27–34, Sep. 2014, doi: 10.1109/MSP.2014.83.

[34] J. Novak, B. A. Manley, D. Mcintire, S. Mudd, A. L. Hueca, and T. A. Bills, “The Sector CSIRT Framework: Developing Sector-Based Incident Response Capabilities,” CMU/SEI-2021-TR-002, Jun. 2021. [Online]. Available: https://resources.sei.cmu.edu/asset_files/TechnicalReport/2021_005_001_734796.pdf

[35] M. Nyre-Yu, R. S. Gutzwiller, and B. S. Caldwell, “Observing Cyber Security Incident Response: Qualitative Themes From Field Research,” *Proc. Hum. Factors Ergon. Soc. Annu. Meet.*, vol. 63, no. 1, pp. 437–441, Nov. 2019, doi: 10.1177/1071181319631016.

[36] I. Skierka, R. Morgus, M. Hohmann, and T. Maurer, “CSIRT basics for policy-makers,” *Hist. Types Cult. Comput. Secur. Incid. Response Teams*, 2015.

[37] I. Jalal, M. Mohd Yusof, Z. Shukur, and Mohd. R. Mokhtar, “A Model for Afghanistan’s Cyber Security Incident Response Team,” *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 8, no. 6, p. 2620, Dec. 2018, doi: 10.18517/ijaseit.8.6.6692.

[38] R. Van der Kleij, G. Kleinhuis, and H. Young, “Computer Security Incident Response Team Effectiveness: A Needs Assessment,” *Front. Psychol.*, vol. 8, p. 2179, 2017, doi: 10.3389/fpsyg.2017.02179.

[39] Forum of Incident Response and Security Teams, Inc., “Information Exchange Policy 2.0 Framework Definition,” FIRST, Nov. 2019. [Online]. Available: https://www.first.org/iep/FIRST_IEP_Framework_v2.0.pdf

[40] A. Cormack, K.-P. Kossakowski, M. Miroslaw, D. Parker, and D. Stikvoort, “CCoP - CSIRT Code of Practice v.2.4,” 2017. [Online]. Available: https://www.trusted-introducer.org/TI-CCoP.pdf

[41] Asia Pacific Computer Emergency Response Team, “Code of Conduct for APCERT.” APCERT, 2011. [Online]. Available: http://www.apcert.org/documents/pdf/CODE_OF_CONDUCT_FOR_APCERT_v1.0.pdf

[42] Forum of Incident Response and Security Teams, Inc., “FIRST Code of Conduct,” *FIRST*. https://www.first.org/about/policies/code-of-conduct (accessed Sep. 13, 2021).

[43] “EthicsfIRST: Ethics for Incident Response and Security Teams,” *FIRST — Forum of Incident Response and Security Teams*. https://www.first.org/global/sigs/ethics/ethics-first (accessed Sep. 12, 2021).

[44] R. Morgus, I. Skierka, M. Hohmann, and T. Maurer, “National CSIRTs and their Role in Computer Security Incident Response,” New America, Nov. 2015. [Online]. Available: http://na-production.s3.amazonaws.com/documents/CSIRTs-incident-response.pdf

[45] National Cyber Security Centre, “Coordinated Vulnerability Disclosure: the Guideline,” Ministry of Justice and Security, publicatie, Oct. 2018. Accessed: Sep. 12, 2021. [Online]. Available: https://english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline

[46] A. Cadena *et al.*, “Metrics and Indicators of Information Security Incident Management: A Systematic Mapping Study,” in *Developments and Advances in Defense and Security*, Singapore, 2020, pp. 507–519. doi: 10.1007/978-981-13-9155-2_40.

[47] A. Dorofee, G. Killcrece, R. Ruefle, and M. Zajicek, “Incident Management Capability Metrics Version 0.1,” Office of the Project Manager Radar Systems Intel and C3CM Systems, Apr. 2007. Accessed: Sep. 13, 2021. [Online]. Available: https://apps.dtic.mil/sti/citations/ADA468688

[48] Carnegie Mellon University Software Engineering Institute, “What Skills Are Needed When Staffing Your CSIRT?,” 2017. [Online]. Available: https://resources.sei.cmu.edu/asset_files/WhitePaper/2017_019_001_485684.pdf

[49] Forum of Incident Response and Security Teams, Inc., “FIRST Events,” *FIRST*. https://www.first.org/events (accessed Sep. 13, 2021).

[50] Trusted Introducer, “TF-CSIRT Trusted Introducer : Events,” Mar. 28, 2013. https://www.trusted-introducer.org/events.html (accessed Sep. 13, 2021).

[51] Asia Pacific Computer Emergency Response Team, “Events / APCERT.” https://www.apcert.org/events/index.html (accessed Sep. 13, 2021).

[52] Organisation of The Islamic Cooperation - Computer Emergency Response Team, “OIC-CERT Events.” https://www.oic-cert.org/en/events/conference/2020.html#.YT9lZ51KhMs (accessed Sep. 13, 2021).

[53] Forum of Incident Response and Security Teams, Inc., “2020 FIRST & AfricaCERT Virtual Symposium for Africa and Arab Regions,” *FIRST*. https://www.first.org/events/symposium/africa-arab-regions2020 (accessed Nov. 12, 2021).

[54] Organization of American States, “OAS Cybersecurity Program,” Aug. 01, 2009. http://www.oas.org/en/sms/cicte/prog-cybersecurity.asp (accessed Sep. 13, 2021).

[55] “Black Hat.” https://blackhat.com/ (accessed Sep. 13, 2021).

[56] SANS Institute, “Cyber Security Training | SANS Courses, Certifications & Research.” https://www.sans.org/ (accessed Sep. 13, 2021).

[57] DEF CON, “defcon.org.” https://defcon.org/ (accessed Sep. 13, 2021).

[58] “CyberDrills,” *ITU*, 2021. https://www.itu.int:443/en/ITU-D/Cybersecurity/Pages/cyberdrills.aspx (accessed Sep. 13, 2021).

[59] “Locked Shields,” *CCDCOE*. https://ccdcoe.org/exercises/locked-shields/ (accessed Sep. 13, 2021).

[60] “Cyber Europe,” *ENISA - European Union Agency for Network and Information Security*. https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme (accessed Sep. 13, 2021).

[61] J. Kick, “Cyber Exercise Playbook,” MITRE Corp, Bedford, MA, Nov. 2014. Accessed: Sep. 13, 2021. [Online]. Available: https://apps.dtic.mil/sti/citations/ADA624910

[62] Asia Pacific Computer Emergency Response Team, “Apcert Cyber Drill 2021 ‘Supply Chain Attack Through Spear-Phishing - Beware of Working from Home -.’” APCERT, Aug. 25, 2021. [Online]. Available: http://www.apcert.org/documents/pdf/APCERT_Drill2021_Press Release.pdf

[63] Organisation of The Islamic Cooperation - Computer Emergency Response Team, "OIC-CERT Cyber Drill." https://www.oic-cert.org/en/events/cyber_drill/index.html#.YT9ykJ1KiUk (accessed Sep. 13, 2021).

[64] Cyber Security Agency - Singapore, "15th iteration of ASEAN CERT Incident Drill tests CERTs' preparedness against opportunistic COVID-19-related campaigns," *CSA Singapore*, Oct. 08, 2020. https://www.csa.gov.sg/news/news-articles/15th-asean-cert-incident-drill (accessed Sep. 13, 2021).

[65] "Internet Governance Forum," *Internet Governance Forum*. https://www.intgovforum.org/multilingual/ (accessed Sep. 13, 2021).

[66] "AIS'21 Online," *Africa Internet Summit*. https://2021.internetsummit.africa/ (accessed Sep. 13, 2021).

[67] United Nations, "Group of Governmental Experts – UNODA," 2021. https://www.un.org/disarmament/group-of-governmental-experts/ (accessed Oct. 22, 2021).

[68] United Nations, "Open-ended Working Group – UNODA," 2021. https://www.un.org/disarmament/open-ended-working-group/ (accessed Oct. 22, 2021).

[69] United Nations, "Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security," A/76/135, Jul. 2021. Accessed: Oct. 22, 2021. [Online]. Available: https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf

[70] United Nations, "Open-ended working group on developments in the field of information and telecommunications in the context of international security," A/AC.290/2021/CRP.2, Mar. 2021. [Online]. Available: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

[71] M. V. Horenbeeck, Ed., "Cybersecurity Culture, Norms and Values." Internet Governance Forum, 2018. [Online]. Available: https://www.intgovforum.org/multilingual/system/files/filedepot/13/igf_2018_-_bpf_on_cybersecurity_background_paper_-_culture_norms_and_values_0.pdf

[72] A. Klimburg and H. Zylberberg, "Cyber Security Capacity Building: Developing Access," Norwegian Institute of International Affairs, Report no. 6, 2015, 2015. [Online]. Available: https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/301986/NUPI_Report_6_15.pdf?sequence=3

[73] Global Cyber Security Capacity Centre and University of Oxford, "Cybersecurity Capacity Maturity Model for Nations (CMM) 2021 Edition," 2021. [Online]. Available: https://cybilportal.org/wp-content/uploads/2021/03/CMM2021-Edition-March-2021.pdf

[74] "National Cyber Security Framework Manual," NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, 2012.

[75] K. Komiyama, "Challenges and Next Steps for the Global CSIRT Community." International Centre for Defence and Security, 2021. [Online]. Available: https://icds.ee/wp-content/uploads/2021/05/ICDS_Report_So_Far_Yet_So_Close_chapter_IV.pdf

[76] Carnegie Mellon University Software Engineering Institute, "Tunisia CSIRT Case Study," Jan. 2013. [Online]. Available: https://resources.sei.cmu.edu/asset_files/WhitePaper/2013_019_001_484987.pdf

[77] *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*. 2016, pp. 1–30. Accessed: Sep. 13, 2021. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2016/1148/oj

[78] S. Hashem, "Establishing a National CERT/CISRT in Egypt," in *The Proceedings of the 23rd World Multi-Conference on Systemics, Cybernetics and Informatics: WMSCI 2019*, 2019, vol. II, pp. 38–43.

[79] International Telecommunication Union and ABI Research, "Global Cybersecurity Index & Cyberwellness Profiles," Apr. 2015. [Online]. Available: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf

[80] S. Hashem, "Towards a National Cybersecurity Strategy: The Egyptian Case," *J. Syst. Cybern. Inform.*, vol. 17, no. 3, pp. 88–94, 2019.

AUTHORS

Jean-Robert Hountomey is an Internet pioneer in West Africa. He is also a founding member of the Africa Forum of computer security and incident response team (AfricaCERT) and the African Anti Abuse Working Group. He is member of the African Union Cybersecurity Expert Group. He has worked on Internet policy issues, capacity building, information security, product security, secure software development life cycle, and privacy risk management for two decades. He has contributed to many organizations and many publications. Jean-Robert's research focuses on law, technology, and Internet governance issues.

Prof. Hayretdin Bahsi is a research professor at the Centre for Digital Forensics and Cyber Security at Tallinn University of Technology in Estonia. He received his PhD and MSc degrees in Computer Engineering from Sabanci University and Bilkent University respectively. He was involved in many R&D and consultancy projects on cyber security as a researcher, consultant, and program coordinator at the Information Security Research Centre of the Scientific and Technological Research Council of Turkey between 2000 and 2014. He acted as the founding director of the National Cyber Security Research Institute. His research interests include cyber-physical system security and the application of machine learning methods to cyber security problems.

Dr. Unal Tatar is an assistant professor of cybersecurity in the College of Emergency Preparedness, Homeland Security, and Cybersecurity at the University at Albany. Dr. Tatar worked as a principal cybersecurity researcher in government, industry, and academia for over 15 years. He is the former coordinator of the National Computer Emergency Response Team of Turkey. Dr. Tatar’s research is funded by the National Science Foundation, National Security Agency, Department of Defense, NATO, and Society of Actuaries. His main topics of interest are cybersecurity risk management, economics of cybersecurity, cyber insurance, privacy, cybersecurity education, supply-chain security, and blockchain. Dr. Tatar holds a BS in Computer Engineering, an MS in Cryptography, and a Ph.D. in Engineering Management and Systems Engineering.

Dr. Sherif Hashem is a Full Professor of Information Sciences and Technology at George Mason University-USA. He is currently a member of the Board of Directors of FIRST (Forum of Incident Response and Security Teams), and a member of the African Union's Cybersecurity Expert Group (AUCSEG). He is a **Senior IEEE** member and an ISACA Certified Information Security Manager (CISM). Dr. Hashem received a Ph.D. in Industrial Engineering from Purdue University-USA, a M.Sc. in Engineering Mathematics and a B.Sc. in Communication & Electronic Engineering from Cairo University-Egypt. He completed the Senior Executive Program at Harvard Business School-USA. He received several awards and recognition including: the *Global Bangemann Challenge Award* from the *King of Sweden* (Stockholm – 1999).

Ms. Elisabeth Dubois is a Ph.D. Candidate in Information Science with specializations in crisis communication and information assurance. She holds a BS in Digital Forensics and MBA degree from the University at Albany. Elisabeth's research is interdisciplinary focusing on various aspects of crisis and risk management including cybersecurity, decision making, communication, and education. She has been involved in many academic, research, community-based, and professional projects and experiences in related topics.