Building the resilience of e-government

4.1. Introduction: Need for a resilient e-government system

Internet use has proliferated since its inception. By 2017, it was estimated that 3.7 billion people, approximately half of the world's population, have access to and continuously use the Internet.[1] With big data, machine learning, and the Internet of Things, some experts anticipate that the number of Internet connections may grow to nearly a trillion by 2035.[2] Similarly, there has been an ever increasing amount of government services that are conducted online. Egovernment development by Member States has progressed with the use of the latest tools and Internet technologies as featured in the current and past editions of the *United Nations E-Government Surveys.* Digital technologies and e-government have provided advanced tools and resources for governments to deliver public services, engage citizens in policy making, improve transparency and monitor development plans. As these tools increasingly become more essential for a dependable and smooth flow of services, threats of disruption, such as cyber-attacks or natural disasters, are never far behind.

The multiplicity of uses of these tools and resources varies across governments, whose individual departments often introduce diverse levels of coherence and consistency among the adopted ICT approaches to service delivery. A disjointed approach also results in degrees of risk, relating to technological threats across the different organizations, departments, systems, platforms and applications.

It is important, therefore, for governments to improve management of ICT-driven approaches for the sake of continuity of online services as well as to protect people's data and privacy. This requires robust platforms that are resilient to cyber-attacks, other threats and emergencies such as natural disasters, including fires, floods and earthquakes. Deployment of ICT mechanisms increases transparency, trust, security and stability in the cyber environment. There is also a tendency to connect technologies and tools to create an open-source computing platform that brings together governments, citizens and innovative companies.[3,4]

Although, constant development and deployment of resilient ICT tools indisputably boosts egovernment services, technology, by its nature, spawns threatening side effects. Rapid technological developments and globalization have brought new challenges for the protection of sensitive information and personal data. This requires a decidedly stronger and more coherent framework of protection at national and international levels, backed by effective enforcement. At the national level, creating a comprehensive cybersecurity framework implies a thorough analysis of Internet-infrastructure dependencies and vulnerabilities. Thus, Member

Photo credit: pixabay.com

In this chapter:

4.1. Introduction: Need for a resilient e-government system 67

4.2. Global view in cybersecurity 68

4.3. Designing a secure e-government system 71

4.3.1. Legal framework 72

4.3.2. Organizational framework 75

4.3.3. Technical framework 76

4.3.4. Capacity building and Cooperation 78

4.3. Conclusion 80

References 81

States should continue to adopt appropriate measures aimed at reducing the risk of cybersecurity attacks. As United Nations Secretary-General António Guterres said, governments and international organizations may not be prepared for rapid developments in the cyber environment, and existing regulations on how to address cybercrime may no longer be applicable. The growing rate of cybersecurity attacks is a vivid example of how Internet capacities are being used, not only for the benefit or empowerment of societies, but also to "degrade and enslave".[5] Considering the fast pace of cyber technology development, it is imperative to amend the existing legal frameworks so as to protect individual privacy, enhance cooperation among government bodies and address the problems stemming from cybercrime.

This chapter introduces a new concept of e-resilience modelled on the Global Cybersecurity Index (GCI) of the International Telecommunication Union (ITU), which assesses the legal, technical, organizational, capacity-building and cooperation frameworks necessary to ensure a robust and resilient e-government system. It also includes a discussion on the use of cybersecurity in improving e-government resilience.

Moreover, the chapter discusses the digital transformation of governments towards e-governance, wherein a clear vision of digital technology and the Internet is essential. It notes the importance of investing in new technologies such as cloud computing to ensure ongoing access to systems and records, and to protect data assets in case of damage to facilities, regardless of the level of e-government development. Attention to cybersecurity is important, as without it, disastrous data breaches can occur. Undoubtedly, recognizing the importance of this domain benefits the e-government system. However, this requires not only a change in existing procedures, but also in the behaviour of public servants. Civic engagement should not be overlooked, as it is critical to the system's functioning.[6] It is also crucial for agencies to create a feedback mechanism for cooperation aimed at sharing knowledge and best practices.

4.2. Global view in cybersecurity

Over the past several years, experts and policymakers have expressed increasing concerns about cyberattacks. Secretary-General Guterres, in his address to the Opening Ceremony of the Munich Security Conference, referred to the lack of response to the cybersecurity threat as an existential threat to humankind.[7]

There is a broad agreement among researchers that modern day e-government systems are susceptible to cyber threats. It is estimated that the cost of addressing cybercrime will double from $3 trillion in 2015 to $6 trillion by 2021. One reason is the increasing interdependence of ICT devices and components, where the disruption of one may cascade and affect many other services. More than a third of cybersecurity breaches are caused by "successful" exploitation of known vulnerabilities. Cyberattacks vary, but their effects can be devastating. For example, in May 2017, the "WannaCry" ransomware attack affected 150 countries, wreaking havoc on societies and resulting in financial damages. This included the United Kingdom, where the National Health Service (NHS) systems were targeted. At least 81 of the 236 NHS organizations known as "trusts" were affected, destroying key medical equipment and risking patient safety.[8] The economic impact of that cyberattack was estimated to be more than $100 million.[9]

Other types of cybercrimes are also costly and erode gross domestic product (GDP). For example, the Netherlands lost 10 billion euros to e-crime, identity and intellectual property theft, which eroded its GDP by 2 per cent. Intellectual property theft alone caused a loss of $300 billion in the United States, while Germany lost 24 billion euros.[10]

The response to the aforementioned attacks has been an increase in global spending on cybersecurity products and services. Cybersecurity Ventures predicts that worldwide, this will exceed $1 trillion cumulatively by 2021.[11] It is also predicted that global spending on security awareness training for employees will reach $10 billion by 2027, up from some $1 billion in 2014. Such investments are aimed at expanding ICT use in cybersecurity strategies and preventing future damage from cyberattacks. Long-term economic opportunity, however, lay in modernizing industrial infrastructure, the cost of which is estimated at $32 trillion.

The Global Cybersecurity Index (see Box 4.1) developed by the International Telecommunication Union can serve as reference for government officials in the process of designing secure egovernment systems. Through use of the Index, governments can assess progress in the effective deployment of ICTs and development of cybersecurity strategies. It provides governments with an assessment of the level of their cybersecurity wellness and offers solutions to addressing e-government risks. More specifically, the Index measures the type, level and evolution of cybersecurity commitment in countries,[12] which will eventually give experts an opportunity to assess the performance of those commitments from both regional and global perspectives.

It is crucial to protect critical information infrastructures, or CIIs, the interconnected information systems and networks, the disruption or destruction of which, would seriously impact the health, safety, security, the economic well-being of citizens, and potentially, the effective functioning of the government or economy. Also essential for a nation’s security is a well-established and protected CII framework that interacts well with the government. Thus, in designing e-government systems, it is important to consider CIIs and how these may affect online services. Given the need to protect information infrastructures from risk or threat, government officials must be made aware of the potential devastating effects of its disruption, so as to improve the effectiveness of mitigation.

The Global Cybersecurity Index 2017 reveals that 50 per cent of the surveyed countries have no cybersecurity strategy, and only 25 per cent have legislation or regulation that impose the implementation of cybersecurity measures on CIIs. It was also found that only 31 per cent of the subject countries included a section on the protection of CIIs in their cybersecurity strategy. These

Box 4.1. ITU Global Cybersecurity Index[13]

The Global Cybersecurity Index is a composite Index combining 25 indicators into one benchmark measure to monitor the cybersecurity commitments of the 193 ITU Member States in the five pillars identified by high-level experts (see Figure 4.2). It revolves around the Global Cybersecurity Agenda,[14] a framework for international cooperation launched by the International Telecommunication Union in 2007 to enhance confidence and security in the information society.[15] A first iteration of the global Index was conducted between 2013 and 2014, in partnership with ABI Research, to which 105 out of 193 ITU Member States responded. The outcome was published in 2015. Following feedback received from various communities and Member States, a second iteration with more in-depth analysis was prepared in 2016. Participants included Member States, and interested individuals, experts and representatives from contributing partners such as the World Bank, the Red Team Cyber from the Australian Strategic Policy Institute, FIRST, Indiana University, the International Criminal Police, the ITU-Arab Regional Cybersecurity Centre in Oman, Korea Internet and Security Agency, National Telecommunications Regulatory Authority of Egypt, The Potomac Institute of Policy Studies, United Nations Interregional Crime and Justice Research Institute, University of Technology Jamaica, and the United Nations Office on Drugs and Crime. As a result of the high-level attention of Member States, media and other interested bodies who believe in the vision of the Global Cybersecurity Index, ITU is compiling a third iteration with an even broader multi-stakeholder participation.

Source: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx results call for measures that will not only create awareness among governments of their position in the digitized world, but also ensure more resilient e-government systems and secure CIIs.

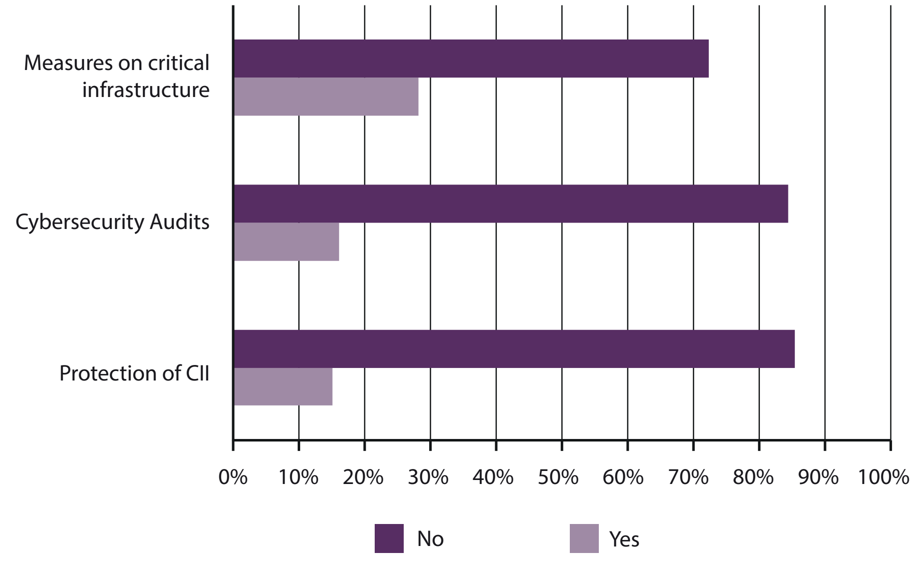
Table 4.1. Top 10 Member States with the highest commitment to cybersecurity

Country	GCI Score	Legal	Technical	Organizational	Capacity Building	Cooperation
Singapore	0.92	0.95	0.96	0.88	0.97	0.87
USA	0.91	1	0.96	0.92	1	0.73
Malaysia	0.89	0.87	0.96	0.77	1	0.87
Oman	0.87	0.98	0.82	0.85	0.95	0.75
Estonia	0.84	0.99	0.82	0.85	0.94	0.64
Mauritius	0.82	0.85	0.96	0.74	0.91	0.70
Australia	0.82	0.94	0.96	0.86	0.94	0.44
Georgia	0.81	0.91	0.77	0.82	0.90	0.70
France	0.81	0.94	0.96	0.60	1	0.61
Canada	0.81	0.94	0.93	0.71	0.82	0.70

Source: ITU, GCI Report 2017

Table 4.1. above shows the top 10 countries ranked according to their GCI score. It is clear that geographical location is irrelevant when it comes to cybersecurity commitments. These ten countries managed to establish coherent cybersecurity strategies while significantly improving their ICT mechanisms. Since these Member States are leaders in their regions, they could foster the creation and development of different forms of collaboration with neighbouring countries to improve regional cybersecurity cooperation.

Figure 4.1. Percentage of countries with CII protection included in their legislation or cybersecurity strategy



Source: ITU GCI report 2017

As seen in Figure 4.1. above, only less than one-fifth of United Nations Member States included protection of critical information structures in their legislation or cybersecurity strategy. Similarly, less than one-third conduct cybersecurity audits and have measures on critical infrastructure.

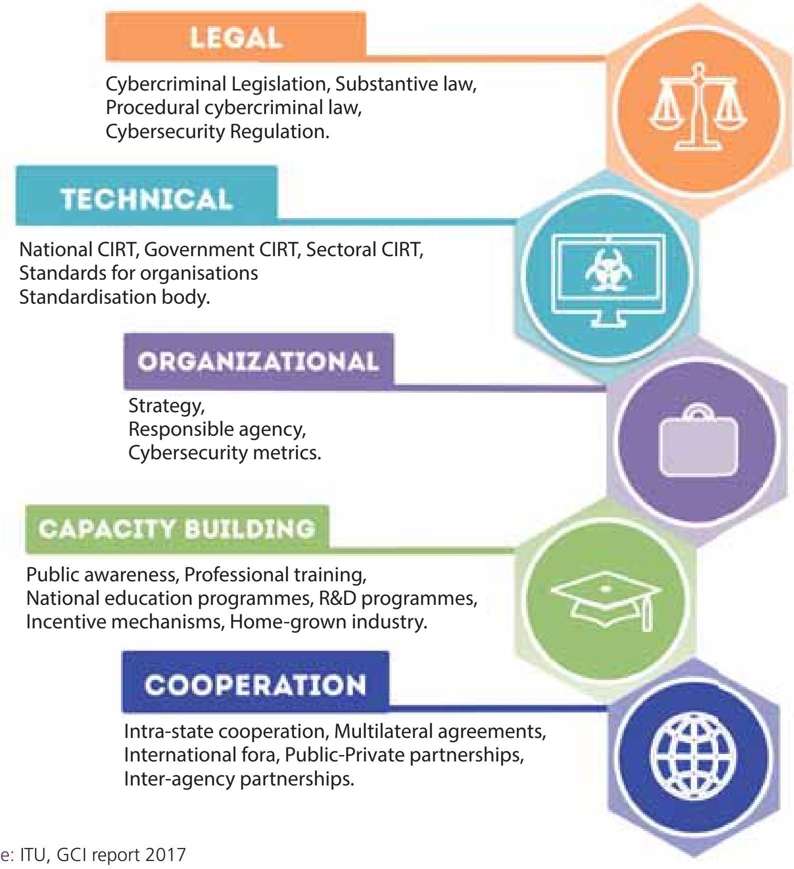
Critical information protection secures communications or information services that are essential to the functioning of a modern economy.[16] For example, the Australian Privacy Principle Act posits that all eligible entities "must take reasonable steps to protect personal information it holds from misuse, interference and loss, as well as unauthorized access, modification or disclosure."[17]

National protection of critical information infrastructures presents an organized view of strategic information services and available infrastructure resources. This requires an assessment of potential risks, threats and information components supporting critical infrastructures. It also defines risk management protocols essential to the health of the national economy and mitigates possible risks. Protection protocols overall have positive long-term stabilizing effects[18], whereas insufficient protection provides criminals with opportunities to exploit online vulnerabilities and conduct cyberattacks.

4.3. Designing a secure e-government system

There are five main pillars in ITU's Global Cybersecurity Agenda (see Figure 4.2) that lay a solid foundation for the creation of a secure e-government system – legal, technical, organizational, capacity building and cooperation. These measure different aspects of government cybersecurity

Figure 4.2. Five Pillars of ITU's Global Cybersecurity Agenda


LEGAL
Cybercriminal Legislation, Substantive law,
Procedural cybercriminal law,
Cybersecurity Regulation.
TECHNICAL
National CIRT, Government CIRT, Sectoral CIRT,
Standards for organisations
Standardisation body.
ORGANIZATIONAL
Strategy,
Responsible agency,
Cybersecurity metrics.
CAPACITY BUILDING
Public awareness, Professional training,
National education programmes, R&D programmes,
Incentive mechanisms, Home-grown industry.
COOPERATION
Intra-state cooperation, Multilateral agreements,
International fora, Public-Private partnerships,
Inter-agency partnerships.

Source: ITU, GCI report 2017

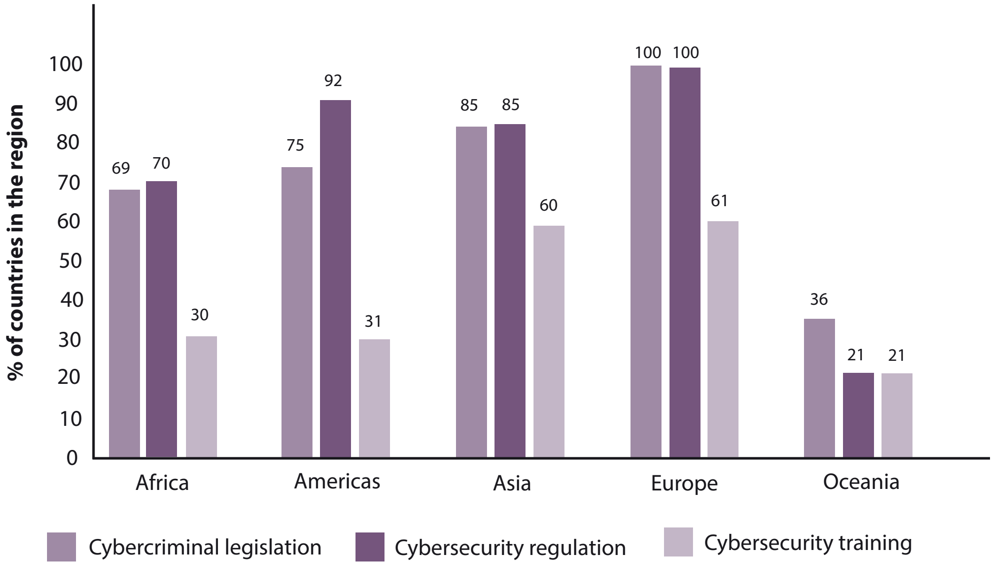
commitment as well as the progress with which governments ensure the confidentiality, integrity and availability of online information. The legal pillar seeks to develop advice on how criminal activities committed over ICTs could be dealt with through legislation in an internationally compatible manner. The technical pillar focuses on key measures for addressing vulnerabilities in software products, including accreditation schemes, protocols and standards. The organizational pillar considers generic frameworks and response strategies for the prevention, detection, response to and crisis management of cyberattacks, including the protection of countries' critical information infrastructure systems. The capacity-building pillar elaborates strategies for raising awareness, transferring know-how and boosting cybersecurity on the national policy agenda. The cooperation pillar aims to develop a strategy for international cooperation, dialogue and coordination in dealing with cyberthreats. All five foundational components work synergistically to ensure cybersecurity.

4.3.1. Legal framework

Legal measures allow governments and other stakeholders to define basic response mechanisms to cyberattacks, including within e-government systems. These mechanisms may involve investigation and prosecution of crimes and violation of norms, leading to the imposition of sanctions for non-compliance and legal breaches by nefarious agents or entities. A legislative framework sets the minimum standards of behaviour across the board, applicable to all, upon which further cybersecurity capabilities can be built. Ultimately, the goal is to enable all nations to have adequate legislation to harmonize practices and offer a setting for interoperable measures that facilitate international combat against cybercrime.

As Figure 4.3. shows, all European countries have cybersecurity legislation and regulations in place. However, only 60 per cent provide training in cybersecurity. The majority of countries in the Americas and Asia have both legislation and regulations. Oceania has the lowest indicators in all three categories. Notably, all regions have relatively low cybersecurity training indicators.

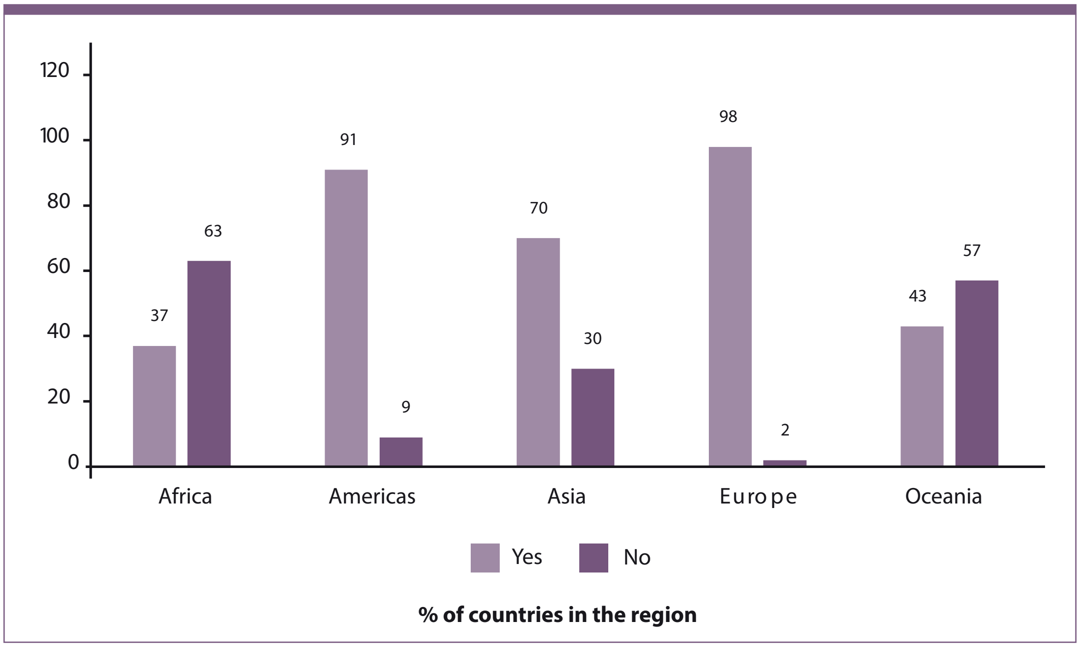
Figure 4.3. Total number of Member States with laws related to cybercrime in 2017



Source: ITU, GCI report 2017

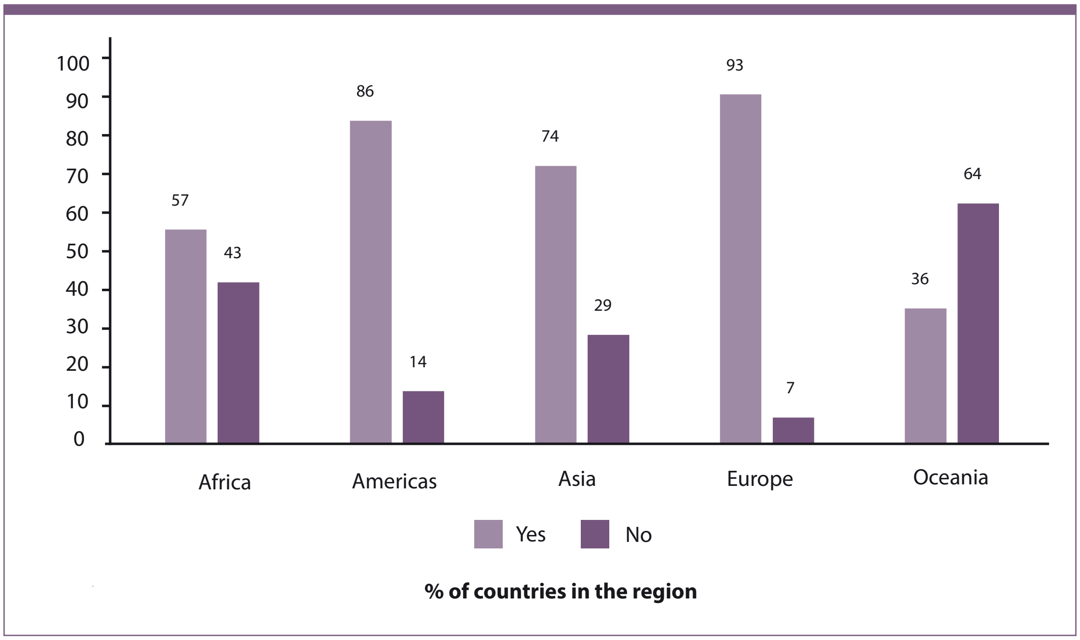
Figure 4.4. shows that 133 out of 193 United Nations Member States, or about 69 per cent, have laws pertaining to citizens' rights to access government information online. Of these countries, 20 are in Africa, 32 are in the Americas, 33 are in Asia, 42 are in Europe and 6 are in Oceania. As many as 34 African countries do not have government information or laws on citizens' rights to access it online. It is also absent in Cuba, Cyprus, Haiti, Monaco and Suriname.

Figure 4.4. Percentage of countries with Access to Information Act



As seen in Figure 4.5., the *United Nations E-Government Survey* highlights that 141 Member States, or 73 per cent, have legislation on personal data protection online. While the legislation may be available in the remaining 52 countries, this information is not accessible online.

Figure 4.5. Personal data protection legislation available online



Data protection is vital since it ensures the privacy of individuals, communities, and specific groups, and protects them from unauthorized surveillance and discriminatory monitoring. Personal data protection is regulated differently in every country. In Europe, the law protects personal data regardless of the technology used for processing that data.[19] In fact, the European Union is considered to have the strongest legal privacy provisions.[20] General Data Protection Regulation will be enacted in the Union in 2018, which will significantly affect data collection and analysis procedures.

Box 4.2. Data Protection Act of Switzerland

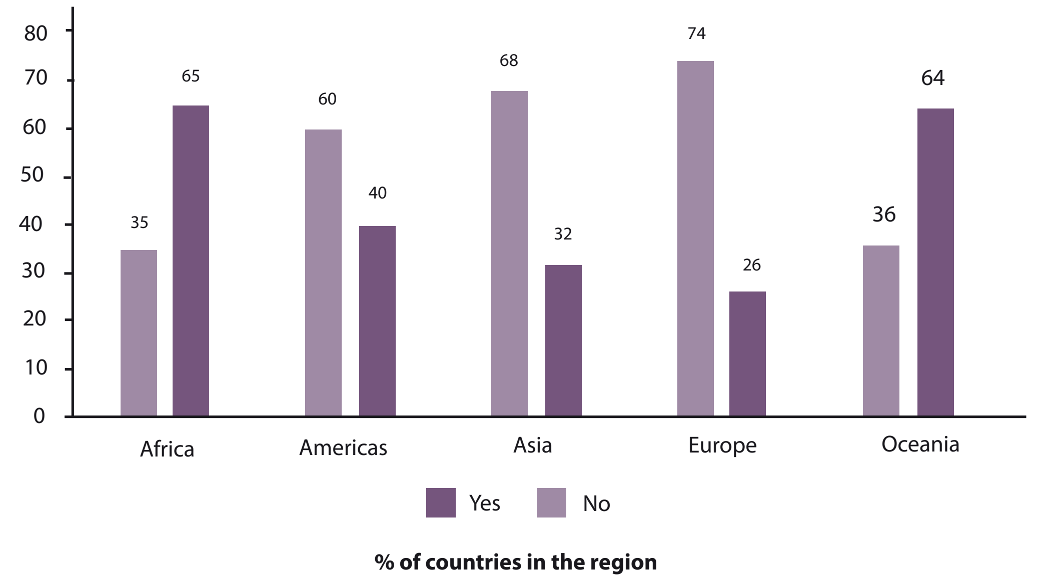
In 2017, the Swiss government issued a preliminary draft of a new Data Protection Act intended to amend existing provisions on digital technology and strengthen personal data protection. It was also crafted to maintain the European Commission knowledge of ways of securinf the free flow of personal data between the European Union countries and Switzerland.

Source: https://www.swlegal.ch/files/media/filer_public/68/68/6868d658-d977-41f0-948f-7468edcb8931 news_alert_september_2017_english.pdf

There are multiple ways of reducing the risks of breaches and unauthorized data retrieval. For starters, personal and sensitive data should be kept at minimum. All personal data could be encrypted and stored during a specific relevant period and destroyed thereafter. The number of actors involved in data collection and storage should be minimized with the assistance of trustworthy and reliable organizations. In order to mitigate risks to the integrity and continuity of available data, replications could be produced and stored off-site, domestically or abroad. The United States State Department and the Estonian Government have already implemented this strategy to ensure data security and the smooth operation of their e-government services.[21]

Figure 4.6. below shows that only 109 Member States have cybersecurity legislation, compared to the information in Figure 4.5., which highlights those with laws on access rights. Majority of the Member States in Asia and Europe have cybersecurity legislation online, while only 13 countries in Africa, 12 in the Americas and 4 in Oceania have it online.

Figure 4.6. Countries with cybersecurity legislation online



4.3.2. Organizational framework

It is important for Member States to have a cybersecurity strategy, a coordinating agency and a compilation of indicators for tracking cybercrime.

Governments should design and execute a robust cybersecurity strategy so as to secure its E-government system. An effective strategy should include the protection of critical information infrastructure and a national resiliency plan. Box 4.3. highlights the United Kingdom organizational framework for cybersecurity. The strategy's formulation should also be open for consultation with all the relevant stakeholders to create trust and transparency in the government and ensure that all reap the benefit. Ideally, cybersecurity strategies should be aligned with the national e-government strategy.

Governments also should consider establishing national agencies responsible for ensuring coherence in putting cybersecurity strategies into action and assessing their efficacy. This needs to be complemented by a commitment to human resource development and leadership. Without a national cybersecurity strategy, a governance model and a supervisory body, the efforts of various sectors and industries can become disparate and disconnected, which could thwart efforts to attain national harmonization and increase e-government resilience in the event of a cyberattack.

Equally important is the compilation of indicators for tracking cyber incidents. Measuring progress is vital, as is observing current and past trends, and putting in place appropriate future actions to implement a secure e-government system and develop further cyber strategies. The Netherlands uses metrics to measure its cybersecurity development, the result of which is summarized in the Cyber Security Assessment Netherlands report.[22] Their National Cyber Security Centre compiles disclosure reports, security advisories and incidents using a registration system. The metrics allow trends to be observed and addressed.

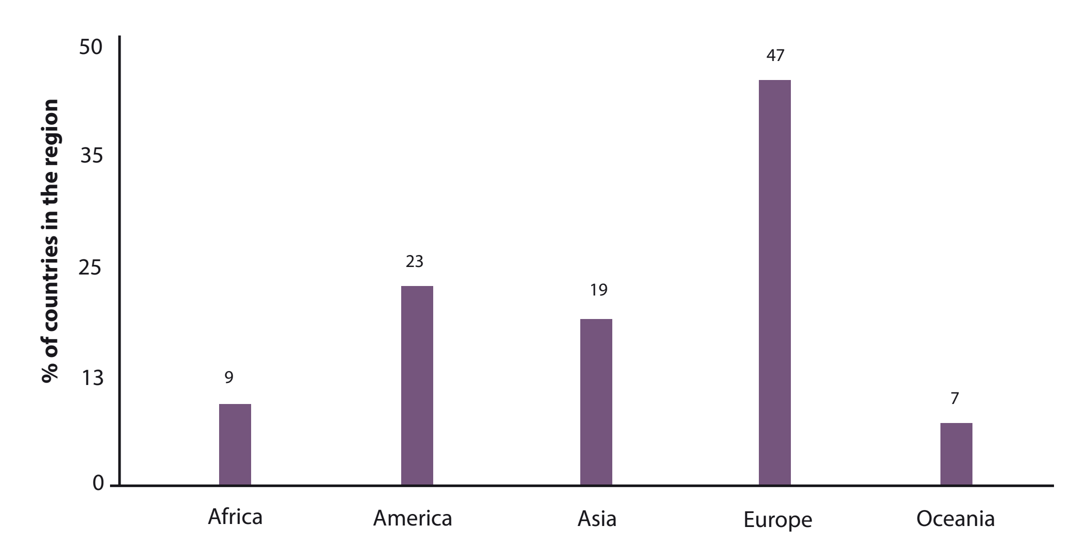
The presence of cybersecurity metrics is an indication that a country has a legally recognized set of measures to provide balanced and unbiased data on the performance of cybersecurity development. Such measures provide crucial data that better equip both the private and public sectors for further administrative decisions regarding e-government system upgrades. Figure 4.7. illustrates the relationship between the high presence of cybersecurity metrics in Europe and the region's advanced level of ICT mechanisms implementation.

Box 4.3. National Cybersecurity Strategy of the United Kingdom

The **United Kingdom** issued its second five-year National Cyber Security Strategy in 2016. The Strategy, established by the Cabinet Office, aims to make the country one of the safest places in the world for online business. Compared to its first Strategy, the new one has doubled its investment in cybersecurity. Some of its main objectives is to make United Kingdom more resilient to cyberattacks, enhance stable cyberspace in support of open societies, and create a stable and secure place for conducting business in cyberspace. All of these goals are directly related to the further development of e-government and cybersecurity, involving both private and public sectors.[23]

Source: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

Figure 4.7. Countries with cybersecurity legislation online

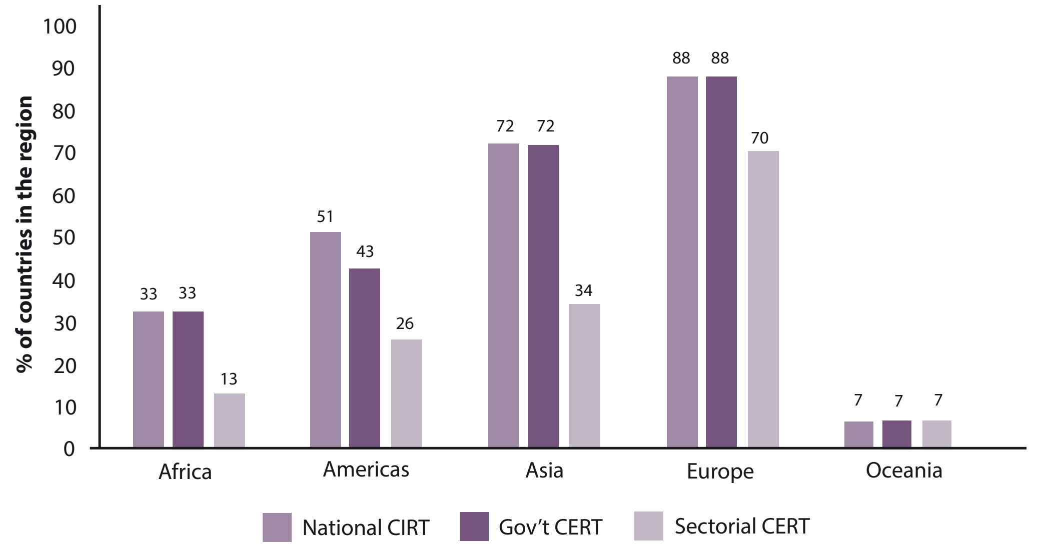


4.3.3. Technical framework

Establishing strong security features in communication networks and increasing resilience against network attacks involving access, modification or service denial, are prerequisites for successful e-government development. Threats to network security such as cyber terrorism, cyber espionage, advanced persistent threats, blended threats and others, are the result of the fast and continuous evolution in technology. Firewalls, antivirus software, Internet security software suites, antimalware, encryption and security fencing are among the measures used to prevent network security from being compromised. To ensure a more reliable and secure e-government system, governments must put in place a computer emergency response team (CERT) or a computer security incident response team (CSIRT) that responds to computer or cybersecurity incidents solely affecting government institutions. Also wise is to have specific government institutions, which protect the nation's entire infrastructure, including that of academia and the civil sector. Box 4.4. and Box 4.5. illustrate cases from United Arab Emirates and Georgia.

Figure 4.8. illustrates the presence of CSIRT as well as government and sectoral CERTs. The highest presence of these teams is in Europe followed by Asia, while Africa and Oceania have the lowest presence.

Figure 4.8. Regional view of CERT/CIRT/CSIRT



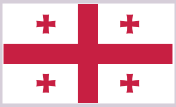
Box 4.4. The National Computer Emergency Response Team of the United Arab Emirates

The United Arab Emirates develops actionable intelligence from analysis of threat, incident and vulnerability data. It also provides constituents with proactive services in the form of preliminary alerts, remediation and recovery from security incidents, and advisories to improve the infrastructure as well as related security processes of their clients or citizens before an event occurs. The national CERT acts as the central point in disseminating information and advises all affected entities during high-profile targeted cyberattacks against critical national infrastructure. It also provides forensics services, including digital forensics investigations, computer forensics and mobile device forensics, data recovery and data wiping.

Source: https://www.tra.gov.ae

Box 4.5. Information Security Policy in Georgia

Georgia has established the Legal Entity of Public Law Data Exchange Agency as part of its Ministry of Justice. The Agency is tasked with establishing an infrastructure for data exchange for both public and private sectors and to implement its information security policy. Moreover, the national CERT of Georgia operates under the Agency and is responsible for handling critical incidents that occur within Georgian governmental networks and critical infrastructures. Georgia also established the Cyber Security Bureau, under its Minister of Defence. It is responsible for cybersecurity in the defence sector. The Council for State Security and Crisis Management acts on the national level as a coordinating body and operates directly under the Prime Minister.



Source: Government of Georgia, 2017

A well-designed cloud computing strategy can be made cost-effective by sharing platforms across various e-government applications, increasing resource utilization and providing scalability. Cloud computing can further increase the capacity for integration and interoperability across egovernment systems. In addition, by analyzing huge volumes of data, cloud computing allows for accelerated fraud detection capabilities, which provides opportunities to address corruption in the public sector.[24] While a proactive cloud computing strategy improves services, optimizes processes and gives more opportunities for citizens to interact with the government, it comes with certain challenges. Hence, regular security audits should be performed to ensure proper functionality and system security. Furthermore, backups and restoration features should be in place to prevent data loss or absence of connection during natural disasters or similar events.

4.3.4. Capacity building and Cooperation

The cybersecurity of e-government systems requires inputs from all sectors and disciplines, given the rising interdependence of big data, machine learning and the Internet of things that are incorporated within the system. This includes cooperation at the intergovernmental level, among agencies at the national level, with the private sector, civil society and academia. Constant dialogue and sharing of best practices are necessary in responding to or defending against a cyberattack. Greater cooperation initiatives can enable the development of much stronger cybersecurity capabilities, help deter persistent online threats, and enable better investigation, apprehension and prosecution of malicious agents.

A good example for cooperation is taking place in Australia where the Government, business and the research communities are working closely to advance the country's cybersecurity agenda. The Government has directed resources towards increasing the number of cybersecurity professionals, and it has invested in tertiary education competitions. Beyond this, it is partnering with various sectors to improve and share cybersecurity information. This is further facilitated through the convening of annual cybersecurity leaders' meetings.[25]

Similarly, Azerbaijan has established an Electronic Security Centre, or CERT, which identifies cyber security threats and raises national awareness of existing and emerging threats. In collaboration with the national operator, the Ministry of Communications and Information Technologies and other authorities, this CERT conducts preventive measures to counter cyber threats and secure cyberspace.

The table below lists various international networks on e-government and cybersecurity providing platforms for hosting dialogues among governments concerning digitization. As egovernment cannot operate effectively without collaborating with organizational structures, it is essential for governments in transition to actively participate in these networks.

Table 4.2. Global cybersecurity activities

- The **United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE)** was established with the aim of examining existing and potential threats from cybersphere and possible cooperative measures to address them. The mandate of the Group was reconfirmed in 2009, 2011, 2013 and 2015. The main outcome of the UN GGE 2013 Report was the reconfirmation of the principle that existing international law(s) apply to the use of ICT by States. In addition, the 2015 Report contained new provisions on norms and principles of responsible State behaviour in cyberspace, specifying, for example, that a State should not conduct or knowingly support ICT activity that intentionally damages or otherwise impairs the use and operation of critical infrastructure. The fifth UN GGE ended its fourth and final session in June 2017 without a consensus on a final report, leaving the dialogue on the conduct of States in cyberspace open.

- Cybersecurity has been very prominent in the agenda of the **Internet Governance Forum (IGF)** since its first meeting in 2006. The 2017 Best Practices Forum on Cybersecurity examined how a well-developed cybersecurity strategy helps to create an enabling environment for ICTs and Internet technologies to contribute towards achieving the SDGs.

- A fundamental role of ITU, based on the guidance of the World Summit on the Information Society and the ITU Plenipotentiary Conference, is to build confidence and security in the use of information and communication technologies. At the World Summit, world leaders entrusted ITU to be the Facilitator of Action Line C5, "Building confidence and security in the use of ICTs", in response to which, in 2017, ITU launched the Global Cybersecurity Agenda as a framework for international cooperation in this area.

- **The Global Forum on Cyber Expertise** has emerged as a series of conferences discussing principles related to governing behaviour in cyberspace. The first conference was held in London in 2011, followed by Budapest in 2012; Seoul in 2013; The Hague in 2015; and New Delhi in 2017.

- **The Global Commission on the Stability of Cyberspace** was inaugurated in 2017, with the mission to develop proposals for norms and policies to enhance international security and stability and to guide responsible State behaviour in cyberspace. It is composed of 27 Commissioners representing a wide range of geographic regions, as well as representatives from governments, the private sector, technical and civil society stakeholders.

4.4. Conclusion

The main conclusions of this Chapter are as follows:

- First and foremost, the adoption of a regionally and internationally harmonized set of legislation against the misuse of ICTs for criminal or other nefarious purposes is critical to providing a common regulatory basis, whether on prohibiting criminal conduct or establishing minimum regulatory requirements. Legal measures should allow each State to establish the basic response mechanisms to data or system breaches. Ultimately, the goal is to enable all States to have adequate legislation in place to harmonize practices internationally and to offer a setting for interoperable measures, thus, facilitating international combat against cybercrime.

- Organizational measures are necessary for the proper implementation of any national initiative. At the initial phase of transformation, a government should incorporate cybersecurity and risk management as an essential component of the e-government systems. A sub-section on the implementation of cybersecurity should be constituted to enhance security and protection in e-government. A national cybersecurity strategy, governance model and supervisory body should be created parallel to the e-government strategy to overcome attempts by various sectors to foil efforts to attain national harmonization in e-government development. A broad strategic objective should be set along with a comprehensive plan for implementation, delivery and measurement.

- Technology is the first line of defense against cyber threats and malicious online agents. Without adequate technical measures and the capabilities to detect and respond to cyberattacks, e-government systems and their respective entities are vulnerable. The emergence and success of ICTs can only truly prosper in a climate of trust and security. Governments therefore need to be capable of developing strategies to establish accepted minimum security criteria and accreditation schemes for software applications and systems. Moreover, governments must regularly assess systems to ensure that security precautions are being implemented by establishing a CIRT/CERT/CSIRT with a national responsibility capable of identifying, defending, responding to and managing cyber threats. Alongside these efforts, a national entity focused on dealing with cyber incidents should be created, or, at the very least, a responsible government agency be mandated to watch, warn and respond to incidents. The same agency could also provide support for the development of an organizational structure needed for coordinating responses to cyberattacks.

- With the increasing interest in knowledge-sharing and transfer in organizations, cooperation through collaboration and communication among relevant stakeholders such as central governments, local public authorities, the private sector, academia, civil society and international organizations, are crucial. The Internet is a highly interdependent system, and no single actor can adopt a fix-all solution to overcome threats that arise from its use. Without Internet, regardless of its obstacles and shortcomings, there can be no egovernment services. However, a secure e-government system requires collaboration among all stakeholders including vendors, industries, manufacturers, academia, government and civil society.

References

1 ITU, (2017). ICT Facts and Figures 2017. [online] Available at: https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx [Accessed 25 Jun. 2018].

2 Nye, J. (2018) How will new cybersecutiry norms develop?. [online] Project Syndicate. Available at: https://www.project-syndicate.org/commentary/origin-of-new-cybersecurity-norms-by-joseph-s--nye-2018-03 [Accessed 25 Jun. 2018].

3 Note: Lathrop et al. define "Government 2.0" as the use of technology—especially the collaborative technologies at the heart of Web 2.0—to better solve collective problems at a city, state, national and international level.

4 Ferenstein, G. (2013). Road to Government 2.0: Technological Problems and Solutions for Transparency, Efficiency and Participation. [online] Queenstown: The Aspen Institute, p.7. Available at: http://csreports.aspeninstitute.org/documents/RoadtoGovrnmt_Final_text.pdf [Accessed 25 Jun. 2018].

5 United Nations, (2017). Secretary-General's Address to the General Assembly. [online] Available at: https://www.un.org/sg/en/content/sg/statement/2017-09-19/secretary-generals-address-general-assembly [Accessed 25 Jun. 2018].

6 InfoDev, (2012). The E-Government Handbook for Developing Countries: A Project of InfoDev and The Center for Democracy & Technology. [online] Available at: http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan007462.pdf [Accessed 25 Jun. 2018].

7 United Nations, (2018). Address at the Opening Ceremony of the Munich Security Conference. [online] Available at: https://www.un.org/sg/en/content/sg/speeches/2018-02-16/address-opening-ceremony-munich-security-conference [Accessed 25 Jun. 2018].

8 National Audit Office, (2018). Auditor Guidance Note 3 (AGN 03) Supporting Information: Local Authorities. [online] Available at: https://www.nao.org.uk/code-audit-practice/wp-content/uploads/sites/29/2015/03/Local-Authority-VFM-2017-18-FINAL-16-April-2018.pdf [Accessed 26 Jun. 2018].

9 Goldman, R. (2017). What We Know and Don't Know About the International Cyberattack. New York Times, [online] Available at: https://www.nytimes.com/2017/05/12/world/europe/international-cyberattack-ransomware.html [Accessed 26 Jun. 2018].

10 Deloitte, (2016). Cyber crime costs Dutch organisations 10 billion euros each year. [online] Available at: https://www2.deloitte.com/nl/nl/pages/over-deloitte/articles/cyber-crime-costs-dutch-organisations-10-billion-euros-each-year.html [Accessed 26 Jun. 2018].

11 Morgan, S. (2017) 2017 Cybercrime Report: Cybercrime damages will cost the world $6 trillion annually by 2021. [online] Available at: https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf [Accessed 26 Jun. 2018].

12 ITU. Global Cybersecurity Agenda (GCA). [online] Available at: https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx [Accessed 26 Jun. 2018].

13 ITU. Global Cybersecurity Index. [online] Available at: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx [Accessed 26 Jun. 2018].

14 ITU. Global Cybersecurity Agenda (GCA). [online] Available at: https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx [Accessed 26 Jun. 2018].

15 UNTERM. Global Cybersecurity Agenda. [online] Available at: https://unterm.un.org/UNTERM/Display/Record/UNOV/NA/1467a520-29e5-405d-b76e-216198de6961 [Accessed 26 Jun. 2018].

16 Cukier, K. (2005). Ensuring (and Insuring?) Critical Information Infrastructure Protection: A Report of the 2005 Rueschlikon Conference on Information Policy. [online] Available at: http://www.rueschlikon-conference.org/pressdocs/56_R_05_Report_Online.pdf [Accessed 26 Jun. 2018].

17 Australian Government Federal Register of Legislation. Privacy Act 1988. [online] Available at: https://www.legislation.gov.au/Series/C2004A03712 [Accessed 26 Jun. 2018].

18 OECD, (2008). Recommendation of the Council on the Protection of Critical Information Infrastructures. Available at: https://legalinstruments.oecd.org/instruments/ShowInstrumentView.aspx?InstrumentID=121&Lang=en&Book=False [Accessed 26 Jun. 2018].

19 European Commission. What is personal data?. [online] Available at: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en [Accessed 26 Jun. 2018].

20 Jacobson, R., Höne, K. E. and Kurbalija, J. (2018). Data Diplomacy: Updating diplomacy to the big data era. [online] Available at: https://www.diplomacy.edu/sites/default/files/Data_Diplomacy_Report_2018.pdf [Accessed 26 Jun. 2018].

21 Hocking, B.and Melissen, J. (2015). Diplomacy in the Digital Age. [online] Available at: https://www.clingendael.org/sites/default/files/pdfs/Digital_Diplomacy_in_the_Digital%20Age_Clingendael_July2015.pdf [Accessed 26 Jun. 2018].

22 NCSC, (2016). Cyber Security Assessment Netherlands 2016: Professional criminals are an ever greater danger to digital security in the Netherlands. [online] Available at: https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands/cyber-security-assessment-netherlands-2016.html [Accessed 26 Jun. 2018].

23 Cabinet Office, (2016). The UK Cyber Security Strategy 2011-2016 Annual Report. [online] Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf [Accessed 26 Jun. 2018].

24 SIIA, (2011). SIIA White Paper: Guide to Cloud Computing for Policymakers. [online] Available at: https://www.siia.net/Admin/FileManagement.aspx/LinkClick.aspx?fileticket=PJv7cHdxGTw%3D&portalid=0 [Accessed 26 Jun. 2018].

25 UNDESA. Member States Questionnaire (MSQ) Analysis.

26 UNODA. Developments in the field of information and telecommunications in the context of international security. [online] Available at: https://www.un.org/disarmament/topics/informationsecurity/ [Accessed 26 Jun. 2018].

27 United Nations, (2013). Developments in the field of information and telecommunications in the context of international security. [online] Available at: http://undocs.org/A/68/156 [Accessed 26 Jun. 2018].

28 United Nations, (2013). Developments in the field of information and telecommunications in the context of international security. [online] Available at: http://undocs.org/A/68/172 [Accessed 26 Jun. 2018].

29 IGF. BPF Cybersecurity. [online] Available at: https://www.intgovforum.org/multilingual/content/bpf-cybersecurity-1 [Accessed 26 Jun. 2018].

30 ITU. ITU Cybersecurity Activities. [online] Available at: https://www.itu.int/en/action/cybersecurity/Pages/default.aspx [Accessed 26 Jun. 2018].

31 GFCE. Global Forum on Cyber Expertise. [online] Available at: https://www.thegfce.com/ [Accessed 26 Jun. 2018].

32 GCSC. Global Commission on the Stability of Cyberspace. [online] Available at: https://cyberstability.org/ [Accessed 26 Jun. 2018].