# Towards a National Cybersecurity Strategy: The Egyptian Case

**Sherif HASHEM, PhD, CISM, IEEE Senior Member**
**Visiting Professor, SUNY Polytechnic Institute, Utica, New York 13502, USA**
**(Former Chairman of the Executive Bureau, Egyptian Supreme Cybersecurity Council, Cabinet of Ministers)**
**sherif.hashem@sunypoly.edu, shashem@ieee.org**

**ABSTRACT**

This paper provides background and highlights key efforts towards establishing and implementing a national cybersecurity strategy for Egypt. We share experiences in launching national cybersecurity initiatives and developing the national cybersecurity strategy with participation from key sectors. We emphasize the importance of cooperation and knowledge exchange at the national, regional and international levels, while developing and implementing the national cybersecurity strategy.

**Keywords:** Egypt, cybersecurity, EG-CERT, national strategy, policy, norms, Supreme Cybersecurity Council.

## 1. INTRODUCTION

Cybersecurity is widely viewed, by many countries across the globe, as a key component of national security. The United States of America, being the birthplace of the Internet, developed a national strategy to secure the cyberspace in 2003 [1], then expanded its scope into an International Strategy For Cyberspace in 2011 [2], and released an updated strategy in 2018 [3].

In Europe, the European Network and Information Security Agency (ENISA) was created in 2004 to assist European Union (EU) member states in implementing relevant EU legislation, and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA developed a practical guide on the development and execution of national cybersecurity strategies for EU member states [4].

In May 2007, the International Telecommunication Union (ITU) launched a Global Cybersecurity Agenda (GCA) as a framework for international cooperation to promote cybersecurity and enhance confidence and security in the information society. The GCA has five working areas: 1) Legal measures, 2) Technical and procedural measures, 3) Organizational structures, 4) Capacity building, and 5) International Cooperation. Furthermore, the ITU invited a high level expert group (HLEG) to advise the ITU Secretary-General on the complex issues surrounding cybersecurity and to formulate proposals on long-term strategies to promote cybersecurity in the GCA five key working areas. The HLEG consisted of .more than one hundred world-renowned specialists in cybersecurity, representing expertise from across a broad range of backgrounds including the administrations of ITU Member States, industry, regional and international organizations, research and academic institutions. The HLEG produced a comprehensive report [5] that became the basis for ITU's cybersecurity efforts [6-8], including the ITU's assistance provided to member states for developing and implementing national cybersecurity strategies.

Leading intergovernmental organizations, such as the Organization for Economic Co-operation and Development (OECD) identified best practices for national strategies and policies for information security and privacy, and developed recommendations for protecting critical information infrastructure [9-10].

International as well as national cybersecurity centers of excellence have been established, in order to further enhance cyber readiness and to facilitate cooperation and coordination of efforts. For instance, NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) in Tallinn-Estonia was established in 2007, and provides support in developing and implementing cybersecurity and cyber defence strategies and policies to member states and partners [11-14].

Following the occurrence of massive cyber attacks targeting multiple critical sectors in several countries across the globe, in 2010 the United Nations established a Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, to provide policy recommendations to the General Assembly of the UN. Since 2010, several UN GGE expert groups carried forward comprehensive international conversation on cybersecurity, particularly on the applicability of international law, and on norms and confidence-building measures in cyberspace. Three UN GGE reports were developed and adopted by the UN General Assembly [15]. The author of this paper was privileged of being among the 15 international UN GGE experts in 2012/13, and he also participated in the UN GGE meetings in 2015. However, the last UN GGE group the convened in 2016/17 failed to agree on the final report, leaving a lot of speculation on the future of international cooperation and coordination efforts that are needed to face emerging cyber threats at the global level. In Dec 2018, the UN General Assembly endorsed Resolution 73/27 that establishes, an open-ended working group (OEWG) acting on a consensus basis, to continue, as a priority, to further develop the rules, norms and principles of responsible behavior of States with a view to making the United Nations negotiation process on security in the use of information and communications technologies more democratic, inclusive and transparent. The UN OEWG started its meeting in September 2019, and it aims at developing ways for the implementation of these rules and norms; and if necessary, will introduce changes to them or elaborate additional rules of behavior; and will study the possibility of establishing regular institutional dialogue with broad participation under the auspices of the United Nations; and will continue to study, with a view to promoting common understandings, existing and potential threats in the sphere of information security and

possible cooperative measures to address them and how international law applies to the use of information and communications technologies by States, as well as confidence-building measures and capacity-building. The UN OEWG is expected to submit a report on the results of the study to the General Assembly at its seventy-fifth session in 2020, and to provide the possibility of holding, from within voluntary contributions, intersessional consultative meetings with the interested parties, namely business, non-governmental organizations and academia, to share views on the issues within the group's mandate (Resolution 73/27) [16]. Furthermore, a new UN GGE will be established in 2019 on the basis of equitable geographical distribution, proceeding from the assessments and recommendations contained in the above-mentioned reports, to continue to study, with a view to promoting common understandings and effective implementation, possible cooperative measures to address existing and potential threats in the sphere of information security, including norms, rules and principles of responsible behavior of States, confidence-building measures and capacity-building, as well as how international law applies to the use of information and communications technologies by States, and will submit a report on the results of the study, including an annex containing national contributions of participating governmental experts on the subject of how international law applies to the use of information and communications technologies by States, to the General Assembly at its seventy-sixth session in 2021 (Resolution 73/266) [16].

## 2. CYBERSECURITY STRATEGY AND INTERNATIONAL NORMS

A national cybersecurity strategy needs to be developed in line with widely acceptable international rules, norms and principles of responsible behavior of States. The reports of the UN GGEs of 2013 [15] and 2015 [16] adopted at the UN General Assembly level, by consensus and recommended in UN Resolution 71/28 entitled "Developments in the field of information and telecommunications in the context of international security", adopted by the General Assembly on 5 December 2016, included some very valuable and relevant norms and principles:

- States should cooperate in developing and applying measures to increase stability and security in the use of Information and Communication Technologies (ICTs) and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security.
- States must meet their international obligations regarding internationally wrongful acts attributable to them under international law. However, the indication that an ICT activity was launched or otherwise originates from the territory or objects of the ICT infrastructure of a State may be insufficient in itself to attribute the activity to that State. Accusations of organizing and implementing wrongful acts brought against States should be substantiated. In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences.
- States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs. States must not use proxies to commit internationally wrongful acts using ICTs and should seek to ensure that their territory is not used by non-State actors to commit such acts.
- States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect.
- States, in ensuring the secure use of ICTs, should respect the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression.
- A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public.
- States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly Resolution 58/199 of 23 December 2003 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions.
- States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty.
- States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products.
- States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions.
- States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies for such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure.
- States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams CERTs or cybersecurity incident response teams CSIRTs) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.
- States should encourage the private sector and civil society to play an appropriate role to improve security of and in the use of ICTs, including supply chain security for ICT products and services. States should cooperate with the private sector and the organizations of civil society in the sphere of implementation of rules of responsible behavior in information space with regard to their potential role;
- States to promote further, at multilateral levels, the consideration of existing and potential threats in the field of information security, as well as possible strategies to address the threats emerging in this field, consistent with the need to preserve the free flow of information;

## 3. EGYPT'S INTERNATIONAL CYBERSECURITY EFFORTS

Egypt has realized early on the importance of international cooperation in addressing cybersecurity challenges. As an active member of the ITU, Egypt was part of the HLEG group and took part in various GCA activities. In addition, Egypt proposed the establishment of the ITU's Council Working Group for Child online Protection (CWG-COP) and chaired the CWG-COP from 2010 until 2017. Egypt also participates in and hosts regional cyber drills and cybersecurity conferences and workshops that are organized by the international organizations such as the ITU, OIC, and FIRST, and participates in international and regional cybersecurity studies with professional organizations such as GSMA [18]. Egypt was a member of the UN GGE from 2012 up until 2017, and has been actively participating in the OECD's Working Party on Security and Privacy in the Digital Economy since 2007.

Successful Egyptian cybersecurity initiatives and activities has led to the **advanced cybersecurity rank that Egypt has achieved in 2015 (27th among 193 countries) and further advanced in 2017 (14th among 194 countries)** as reported by the International Telecommunications Union **(ITU) Global Cybersecurity Index [8]**.

## 4. EGYPT'S NATIONAL CERT (EG-CERT)

The idea to develop an Egyptian cybersecurity and Critical Information Infrastructure Protection (CIIP) framework was initiated in 2007, within a working group at the Egyptian Ministry of Communications and Information Technology. The first implementation step was the establishment of the Egyptian national Computer Emergency Readiness Team (EG-CERT) in April 2009. EG-CERT is affiliated with the National Telecom Regulatory Authority (NTRA), and provides support to several entities in the ICT sector, the financial sector as well as the governmental sector, in order to help them tackle Cybersecurity threats and deal with cyber incidents and denial of service (DDOS) attacks. EG-CERT provides both re-active as well as proactive services, including incident handling, cyber forensics, malware analysis, vulnerability assessment, and penetration testing.

It is worth noting that EG-CERT started as an ICT sector specific CERT. However, a few weeks after its establishment, it was called upon to provide support and services to entities in other critical sectors, especially in the financial and governmental sectors. Furthermore, in Oct 2009, EG-CERT was contacted to assist the prosecutors in investigating an international cybercrime case "Operation Phish Phry" that involved a phishing ring of about 100 alleged criminals from Egypt and the USA, targeting thousands of victims in US Banks. That phishing ring was considered one of the largest worldwide at that time [20]. EG-CERT professionals spent over 1600 man hours on the cyber forensics analysis, and produced a report in excess of 500 pages. EG-CERT's efforts were timely, professional, and instrumental in the successful prosecution of such a challenging case, and was recognized nationally as well as by the US officials. By the end of 2009, EG-CERT had emerged as the National CERT.

Currently, EG-CERT produces over 150 reports annually for its constituents and for relevant authorities and key organizations. EG-CERT leads and coordinates efforts to confront distributed denial of services (DDOS) attacks on critical infrastructure by local and international "cyber hacktivist" groups, such as Anonymous. EG-CERT assists in dealing with web defacement attacks on several governmental and strategic websites in the financial sector. EG-CERT's support and services are provided, whether to governmental or private entities, free of charge, in full confidence and discretion. EG-CERT's engagement is generally based on the criticality of the threat and/or the severity of the incident. The breakdown of the cyber incidents handled by EG-CERT shown by sector during the last four years is shown in Fig. 1.

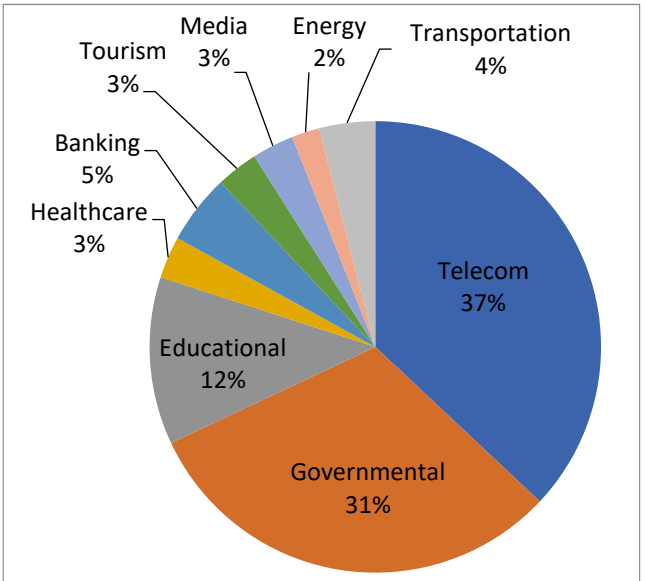


**Fig 1: Cyber incidents handled by EG-CERT 2015-18 (by sector)**

As soon as EG-CERT assumed its national responsibilities, providing support to key CII entities, it became evident that empowering those responsible for CIIP in 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, 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.

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 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, IMPACT, and Indian CERT. It also has strong relationships with many CERTs in the Arab region, in Africa, and across the Globe.

## 5. EGYPT'S NATIONAL CYBERSECURITY STRATEGY

In 2014, a new Egyptian constitution was adopted. Article (31) of the new constitution recognizes that: "*a safe and secure cyberspace is essential for the Egyptian economy and is a main pillar of Egypt's national security*."

Later in December 2014, and in light of Article (31) of the new Egyptian constitution and motivated by the recommendations of the ITU's HLEG report, a Supreme Council for Critical Information Infrastructure Protection and Cybersecurity (namely the Egyptian Supreme Cybersecurity Council ESCC), was established at the Cabinet of Ministers level. ESCC is chaired by the Minister of Communications and Information Technology, and has members from the critical sectors as well as the key security agencies.

ESCC began its work in 2015, and was initially mandated to develop a national cybersecurity strategy for Egypt, with EG-CERT being recognized as the technical arm for the newly founded ESCC. The development of the proposed five years national cybersecurity strategy was finalized by the ESCC in May 2017 [21]. The strategy document was forwarded to the Cabinet of Ministers, and the implementation of the strategy started later in the fall of 2017.

The key goal of the national strategy is to:

*"To confront cyberthreats and enhance confidence and security of the ICT infrastructure, and its applications and services in various critical sectors, in order to create a safe, reliable, and trusted digital environment for the Egyptian society."*

The national cybersecurity strategy aims at developing and implementing a comprehensive framework for enhancing the security of and the trust in the ICT infrastructure, applications and services in Egypt, while protecting the privacy of various users. It follows the international norms and best practices discussed in the previous sections, especially the UN GGE's recommendations and ITU's GCA five working areas (legal/regulatory, technical, organizational, capacity building, international cooperation).

**Primary Strategic Objectives**

i. Boost the comprehensive awareness of the importance of cybersecurity and Critical Informnation Infrastructure Protection (CIIP) as **a National Priority**, essential for Egypt to be an attractive destination in the information age and an active participant in the Global Digital Economy.

ii. Establish the Egyptian Supreme Cybsecuirty Council as the national focal point for cybersecurity and for CIIP

iii. Develop comprehensive **legal, institutional, and operational frameworks** for cybersecurity and for ciip

iv. Empower cybersecurity industry development

v. Enhance and further develop the **skill pool and human resources** in cybersecurity, at all levels and in various sectors

vi. Support and promote the development of domestic trustworthy cybersecurity technology

**Secondary Strategic Objectives:**

i. Empower and sustain trust in ICT infrastructure, applications and services across all sectors.

ii. Develop/promote models and best practices that reduce the risks and secure the benefits of a trusted digital environment for government, businesses and individuals

iii. Encourage and empower research and development efforts and activities in cybersecurity and CIIP domains

iv. Encourage the deployment of revolutionary and state-of-the-art ICT technologies, such as of cloud computing and artificial intelligence, to provide innovative solutions that tackle major cyber threats and challenges.

v. Develop the environment for digital privacy protection

vi. Enhance child online protection (COP)

vii. Provide directions to protect against common cybercrimes such as identity theft and on line fraud.

The national cybersecurity strategy document highlighted the main cyberthreats, and the key "critical" sectors that may be affected the most by these cyberthreats, including the ICT sector, the financial sector, the energy sector, the government services sector, transportation, and healthcare. Seven strategic pillars were identified (Fig. 2) and six national programs were proposed to be implemented over a period of five years.


**Fig. 2:** Pillars of the National Cybersecurity Strategy

The main cyberthreats highlighted in the strategy are:

1. **Penetrating critical ICT infrastructure,**
2. **Cyber terrorism and cyber warfare,**
3. **Theft of digital identity and personal data.**

Thus, the scope and structure of the strategy and its objectives are in line with the national requirements and follow the international norms, rules and principles that are discussed in Section 2 above. Likewise, the implementation of the strategy must follow the same spirit.

**Strategic Programs:**

1. Program to develop the appropriate legislative framework to secure the cyberspace, combat cybercrimes and protect privacy and digital identity,
2. Program to develop an integrated national system for cyber readiness and incidents response,
3. Program to enhance the protection of digital identity (Digital Citizenship Program), and to improve the infrastructure necessary to establish trust in e-transactions in general, and in e-government services in particular,
4. Program for capacity building to empower the human calibers and develop the required expertise in various sectors,
5. Program to support scientific research and development and for cybersecurity industry development,
6. Program to raise awareness of the opportunities and benefits offered by e-services to individuals, institutions and government agencies, and of the importance of cybersecurity to protect these services from cyber risks and challenges.

**Implementation Started:**

At the operational level, guided by the experience of establishing and operating EG-CERT, and with the leadership and support of EG-CERT professionals, the ground work for developing and empowering CERT teams in critical sectors has started, with a special focus on the financial, energy, and transportation sectors. The financial CERT (Fin-CERT) is expected to be fully operational by end of 2019.

In parallel, plans are being implemented for developing a national security operations center (SOC) and national cybersecurity certification center.

A new national capacity building and advanced skills development program is being launched, with participation from the Information Technology Institute (ITI), the National Telecommunication Institute (NTI), the Information Technology Industry Development Agency (ITIDA), as well as several academic institutions and technology providers.

In order to further enhance the legal cybersecurity framework, a new cybercrime law was developed and adopted in August 2018. A new private data protection draft law has been finalized , approved by the Cabinet of Ministers, and is being discussed at the Egyptian parliament.

## 6. LESSONS LEARNED

- **Start small, then grow.** In 2009, EG-CERT started with a team of 6 professionals, divided between incident management and cyber forensics. As the demand for its services grow, EG-CERT grew to employ over 50 professionals. It expanded its scope of services to include proactive services, such as penetration testing, malware analysis, and reverse engineering. It also developed research and development capabilities [22-32].
- **The human factor is central**. When it comes to cybersecurity, humans often are the weakest link. Cybersecurity readiness starts and flourishes with empowered and skilled workforce. The launch of EG-CERT was supported by recruiting talented professionals and an advanced training and skill development program, targeting not only EG-CERT professionals, but also professionals from 38 key entities, including government, academia and private sector.
- **Stay focused and avoid turf fights.** It is important, especially for a national CERT, to stay focused on its mission, and on enhancing its services and empowering its staff. Any distractions, especially internal and external organizational politics, conflicts, and turf fights, should be avoided. CERTs should be viewed as "***professional cyber peace keepers and guardians of safety and security in cyberspace for all.***".
- **Cybersecurity and physical security are highly interdependent.** When called upon to investigate a cyber incident or assess cyber-related vulnerabilities of an ICT system, EG-CERT professionals often realize that the more evident root cause or vulnerability is actually more fundamental and physical, such as lack of proper access control, absent or expired staff certification and clearance, unclear work flow, missing data and information classification, or improper authorizations. Thus, cyber risk needs to be addresses as a part of a holistic approach for overall operational risk management, rather than an isolated technical or technological risk.
- **Security-by-Design is key to successful cybersecurity.** Attempting to "fix" serious vulnerabilities or shortcomings in critical systems can be both costly, time consuming, and sometimes impossible, once the system has been designed or deployed. Cybersecurity need to be addressed from the very early phases of system design and incorporated in the design from the beginning.
- **Build and strengthen partnerships.** Cybersecurity professionals should be open to share knowledge and expertise with their peers. EG-CERT professionals often provide seminars, workshops, and training to professionals working in key entities and organizations, nationally, regionally, and internationally. They also support cyber competitions, such as Capture the Flag (CTFs) and cyber drills. At the operational level, public-private partnerships and empowering the cybersecurity industry are key to the success of cybersecurity operations as well as for drafting and implementing cybersecurity strategies, at the organizational and at the national levels.
- **Research and Development are essential for comprehensive cybersecurity.** Most countries rely on technologies and solutions from a variety of vendors, national and international. Having the capability to investigate and test emerging technologies and new gadgets is essential for

successful deployment. Furthermore, cybersecurity professionals often need to develop new tools or customize systems provided by the vendors, for better utility or higher efficiency. R&D capabilities expand the operation horizon and provide a much needed and desired effectiveness.

- **Establish trust.** The engagement with the constituents should be based on dedication, full confidence and discretion. Although EG-CERT is affiliated with the telecom regulator, the NTRA, the information on cyber incidents or vulnerabilities provided to the EG-CERT professionals are kept fully confidential, and thus are not shared even with the NTRA regulatory division.
- **Balanced awareness.** When raising awareness with regard to emerging cyberthreats, the message should be balanced: it needs to be clear and relevant in order to affect those who are unaware of the cyber risk ahead of them, especially if they are in a "***State Of Denial***". Yet, it needs not to be exaggerated, so as not to cause a "***State Of Panic***."

## 7. CONCLUSIONS

The Egyptian national cybersecurity strategy recognizes that:

- **"Confronting cyberthreats and cybercrimes requires sincere, coherent and sustained efforts, as well as extensive community partnerships, involving government agencies, private sector, research and educational institutions, business organizations and civil society; in order to maximize the benefits of the unique opportunities offered by advanced ICTs in various economic, social and cultural domains, while protecting our society from the risks of cybercrimes and cyberattacks**." Indeed, such a comprehensive view and inclusive partnerships are essential for the successful implementation of any strategy, especially cybersecurity strategies.
- **"Cybersecurity is not the responsibility of the ICT professionals exclusively, nor is it the duty of the government by itself. Cybersecurity requires comprehensive, inclusive and integrated efforts from governments, international organizations, businesses, civil society, professionals, and citizens. Cooperation and partnerships are central to the success of such efforts**."

## 8. REFERENCES


[1] USA, **The National Strategy To Secure Cyberspace,** The White House, Washington DC, 2003.

[2] USA, **International Strategy For Cyberspace**, The White House, Washington DC, 2011.

[3] USA, **National Cyber Strategy of the United States of America**, The White House, Washington DC, 2018

[4] ENISA, **National Cyber Security Strategies: Practical Guide On Development And Execution**, ENISA, Greece, 2012.

[5] ITU, **Report Of The Chairman Of High Level Expert Group on Cybersecurity**, ITU, Geneva, 2008.

[6] ITU, **National Cybersecurity/CIIP Self-Assessment Tool,** ITU, Geneva, 2010.

[7] ITU, **Child Online Protection: Statistical Framework And Indicators**, ITU, Geneva, 2010.

[8] ITU, **Global cybersecurity Index (GCI) 2017**, ITU, Geneva, 2017.

[9] OECD, **Recommendation of the Council on the Protection of Critical Information Infrastructures**, OECD, Paris, 2008.

[10] OECD, **Policies For Information Security & Privacy**" OECD, Paris, 2009.

[11] K. Geers, **Strategic Cyber Security**, NATO CCD COE, Estonia, 2011.

[12] C. Czosseck, R. Ottis, and K. Ziolkowshki, **Proceedings of the 4th International Conference on Cyber Conflict,** NATO CCD COE, Estonia, 2012.

[13] A. Klimberg, **National Cyber Security Framework Manual**, NATO CCD COE, Estonia, 2012.

[14] NATO CCD COE, **Cybersecurity Strategy Documents**, on-line publication, Jan 2018, https://ccdcoe.org/cyber-security-strategy-documents.html/

[15] UN GGE, **Report of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security**, United Nations, New York, June 2013. https://undocs.org/en/A/68/98

[16] UN GGE, **Report of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security**, United Nations, New York, July 2015. https://undocs.org/en/A/70/174

[17] General Assembly of the United Nations, **The Resolutions of the 73rd Session.** http://www.un.org/en/ga/73/resolutions.shtml

[18] GSMA, **Children's Use Of Mobile Phones: An Iternational Comparison**, GSMA & NTT DOCOMO, 2013.

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

[20] FBI, **Archives on Operation Phish Phry**. (Oct 2009).https://archives.fbi.gov/archives/news/stories/2009/october/phishphry_100709

[21] ESCC, **Egypt's National Cybersecurity Strategy**, ESCC, Cairo, 2017, http://www.escc.gov.eg/

[22] M. Rasslan and M. Nasreldin, "Identification Protocols Based on Discrete Log Representation Problem*,"* **Procedia Computer Sciences**, Vol. 21, pp. 368-373, Elsevier Science, 2013.

[23] M. Rasslan and H. Aslan, "On the Security of Two Improved Authenticated Encryption Schemes, **International Journal of Security and Networks**," Vol. 8, No. 4, pp. 194-199, 2013.

[24] M. Rasslan, "Security comments on Hwang-Lo-Hsiao-Chu Authenticated Encryption Schemes," **Procedia Computer Sciences**, Vol. 19, pp. 565-569, Elsevier Science, 2013.

[25] H. Aslan and M. Rasslan, "A New Multicast Authentication Protocol using Erasure Code Functions and Signcryption

Techniques," **World Congress on Internet Security (WorldCIS-2013)**, Proceedings of the IEEE, 2013.

[26] S. Sayed, R. Darwish and S.A. Salem, "A Real-Time Approach for Detecting Malicious Executables," **Proceedings of the International Conference on Systems Science 2013 (ICSS 2013),** Vol. 240, 2014, pp 355-364

[27] A.A. Awad, S.G. Sayed and S.A. Salem, "A network-based framework for RAT-bots detection," **Proceedings of the 8th IEEE Annual Information Technology**, **Electronics and Mobile Communication Conference (IEMCON),** 2017.

[28] A.A. Awad, S.G. Sayed and S.A. Salem, "A Host-based framework for RAT-bots detection," **Proceedings of the IEEE International Conference on Computer and Applications (ICCA),** 2017.

[29] D. Wael, A. Shosha and S.G. Sayed, "Malicious VBScript detection algorithm based on data-mining techniques," In **Proceedings of the International Conference on Advanced Control Circuits Systems (ACCS) Systems & International Conference on New Paradigms in Electronics & Information Technology (PEIT)**, 2017.

[30] S.G. Sayed and M. Shawkey, "Data Mining Based Strategy for Detecting Malicious PDF Files," In **Proceedings of the 17th IEEE International Conference on Trust, Security And Privacy In Computing And Communications (IEEE TrustCom-18)**, 2018.

[31] M. Medhat, S.G. Sayed, and N. Abdelbaki, "A New Static-based Framework for Ransomware Detection," In **Proceedings of the 16th IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC 2018)**, 2018.

[32] D. Wael, S.G. Sayed and N. Abdelbaki, "Enhanced Approach to Detect Malicious VBScript files Based on Data Mining Techniques," In **Proceedings of Fifth International Workshop on Privacy and Security in HealthCare 2018**.