Arab Republic of Egypt
Cabinet of Ministers
Egyptian Supreme
Cybersecurity Council

National Cybersecurity Strategy 2017-2021

National Cybersecurity Strategy 2017-2021

> “The security of cyberspace is an integral part of the economic system and national security. The State shall take the necessary measures to preserve it as regulated by Law.”
>
> Article (31) of the Egyptian Constitution (Jan 2014).

Introduction

This document entitled “National Cybersecurity Strategy” has been prepared within the scope of the State’s efforts to support national security and develop the Egyptian society, and in order to monitor and confront emerging threats and future challenges in cyberspace and digital society. The national cybersecurity strategy document has been developed in view of the strategic objectives that led to the creation of the Egyptian Supreme Cybersecurity Council (ESCC)— reporting to the Cabinet of Ministers, and chaired by the Minister of Communications and Information Technology. The ESCC was mandated to develop a comprehensive strategy for protecting the Information and Communication (ICT) infrastructure, in order to provide a safe and secure environment that would enable various sectors to deliver integrated e-services.

The strategy entails a number of programs that support the strategic cybersecurity objectives. It emphasizes the distribution of roles among government agencies, private sector, business institutions and civil society, and the measures to be established by the State to support progress towards achieving these objectives. In addition, the strategy outlines an action plan for the years 2017-2021. The plan has been developed in line with these specified objectives and to facilitate their implementation, emphasizing the significance of the partnership among government agencies, private sector, business institutions and civil society. Achieving these objectives, pave the road for the transition to an integrated digital economy that meets citizens’ aspirations for comprehensive socio-economic development; protects their individual welfare as well as the national interests; and contributes to the country’s progress and prosperity.

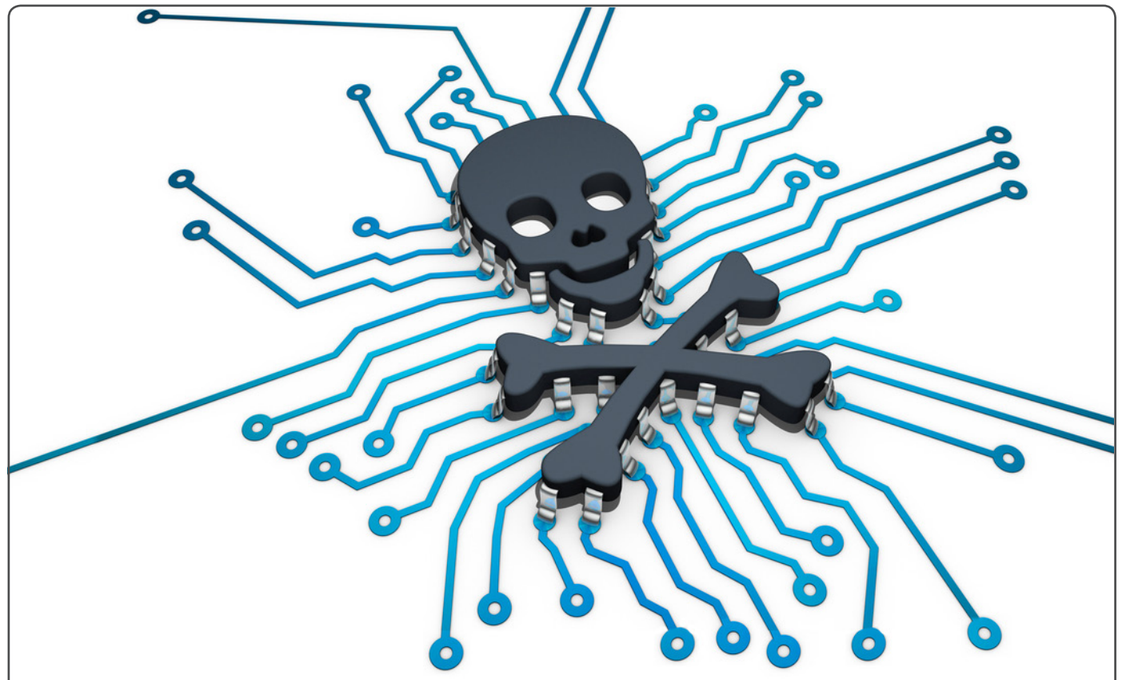
Background

The last three decades have seen an increased proliferation in the number of Internet and smart phones users and uses in business, commerce, government services, education, knowledge, entertainment, tourism, health care and other economic, social and cultural activities. Alongside the opportunities brought about by the continuous growth in the telecommunications and Internet usage and the proliferation of e-transactions and e-services, it is important to face the threats and challenges that target the ICT infrastructure and e-transactions in general, and undermine confidence and trust in e-services and e-business, in particular.

The Most Significant Cyber Challenges and Threats are:

- **Threat of Penetrating and Sabotaging ICT Infrastructure**

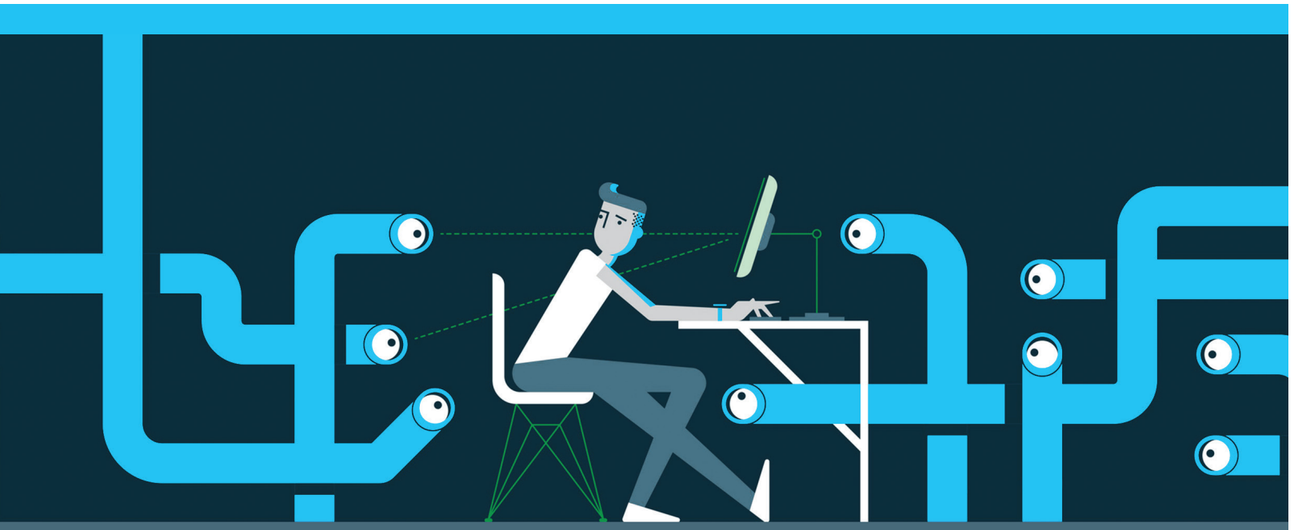
  New types of extremely serious cyberattacks have recently emerged, aimed at disrupting critical services, and deploying malware and viruses to destroy or disrupt the ICT infrastructure and critical industrial control systems, especially in key facilities, including entities of nuclear power, oil, natural gas, electricity, aviation, various forms of transportation, key national databases, government services, health care, and emergency aid services. Such cyberattacks deploy several channels including wireless networks and mobile memory, and other common channels such as e-mails, websites, social media and telecommunications networks, which may have a significant impact on the utilization of the critical infrastructure and the associated services and businesses. In practice, critical facilities may be vulnerable to advanced cyberattacks, even if they are not directly connected to the Internet.



- **Threat of Cyber Terrorism and Cyberwarfare**

  Recently, dangerous types of cyberattacks and cybercrimes have spread, using advanced technologies, such as cloud computing, wiretapping and network intrusion devices, advanced encryption, and automated hacking tools targeting computer systems and databases. In addition, advanced malicious software (malware) may be deployed to undermine networks security systems and compromise computer systems to form botnets, that can be used later on in a variety of criminal and illegal activities. An automated botnet may consist of tens, hundreds of thousands or millions of compromised computers that can be used to launch serious cyberattacks, such as Distributed Denial-of-Service (DDoS) attacks, on targeted networks and websites for destructive, terrorism, and/or extortion purposes.

  The development of complex and sophisticated computer viruses often requires advanced knowledge levels and unconventional expertise, available only in technologically advanced countries, to be used for strategic, tactical, and warfare purposes, to be used in addition to, or sometimes instead of, conventional military attacks, in what is known as cyberwarfare. However, such malicious technologies are being transferred, copied or reproduced by terrorist organizations and international crime gangs, to be used in terrorist operations and organized crimes, as well as in threatening and disrupting the ICT infrastructures for extortion and/or industrial espionage purposes. Leading cybersecurity experts expect an increased proliferation of ferocious and sophisticated cyberattacks in the coming period.



Threat of Digital Identity and Private Data Theft:

Digital identity theft is one of the most serious crimes that threaten Internet users and the future of e-services. Stolen credentials and personal data can facilitate impersonating individuals in cyber space, and may result in monetary and property loss, or may entangle the names of the victims in suspicious or illegal activities. The identity thief usually uses information already available on the Internet, especially on open social media and professional networks; national databases; networks of government services, social security services and health care; e-commerce websites; virtual markets; e- payments networks; Automated Teller Machines (ATMs); and stock exchanges. In addition, tools and systems used in performing e- transactions may be compromised, stolen or damaged, which poses a serious threat to the interests of users and the future of e-services. Extensive and widespread attacks may affect the national financial sector. Data of public institutions and companies may also be stolen, resulting in considerable material and credibility losses, damage to reputation, customer attrition and reduction in value of intangible assets, which may harm the national economy at large.

Most-Targeted Critical Sectors:

- **ICT Sector**
  It includes telecommunications networks, submarine and land cables, communications towers, communications satellites, communications control centers, telecommunications and Internet service providers.

- **Financial Services Sector**
  It includes networks and websites of banks, banking transaction, e-payment platforms, stock exchange, securities trading companies and postal financial services.

- **Energy Sector**
  It includes systems, networks and stations that control the production and distribution of electricity, oil and gas; High Dam stations; nuclear power plants; and others.

- **Government Services Sector**
  It includes the e-government portal and websites, government agencies and institutions websites, national databases— the most important of which is the national ID database, and associated networks and websites.

- **Transportation Sector**
  It includes air, land, sea and Nile transport. It covers all train and metro control systems, centers and networks, as well as air and sea navigation traffic networks and control systems.

- **Health and Emergency Aid Services Sector**
  It includes relief and emergency networks, blood banks, hospital systems and networks, health care networks and websites.

- **Information and Culture Sector**
  It includes networks, systems and websites of information and broadcasting services.

- **The State's official websites and sectors that affect the economic activity such as investment, tourism, commerce, industry, agriculture, irrigation and education at the different levels.**

Key Aspects of the Seriousness of Emerging Cyberthreats:

Emerging cyberthreats may be very serious due to three main aspects:

- **They often deploy advanced and sophisticated technologies**

  Few countries and large companies often have a monopoly on these technologies. Many of these technologies are top-secret and not available for export. Furthermore, the exportable versions of some technologies may contain backdoors or vulnerabilities that make them a source of additional threats.

- **They can spread easily and rapidly**

  Spreading malicious viruses, launching DDoS attacks and other advanced cyberattacks can occur very quickly and easily, due to the widespread use of ICTs, and because of the ease of launching these attacks remotely and transmitting viruses across borders from anywhere and at a low cost. It is also difficult and often impossible to trace the main origin of those threats and risks in time to address and overcome them.

- **They can have a widespread impact**

  Cyberattacks may have extensive direct and indirect impact on the infrastructure, causing substantial damage and losses. In addition, they may be executed remotely and expand suddenly in unpredictable manner, while potentially affecting critical entities and large numbers of citizens (thousands or millions).

  Cyberattacks and cybercrimes may transcend the geographical boundaries of countries, and usually rely on both traditional and technical organized crime networks. Confronting such attacks and crimes must therefore include the traditional mechanisms of international cooperation to combat crimes and face cyberthreats, as well as legislative and regulatory frameworks with special mechanisms to handle the emerging technical developments. Effective response to cyberattacks and cybercrimes necessitates cooperation and coordination at the national level, among partners providing and operating infrastructure at critical sectors, and partners providing services, including government agencies, institutions and companies. In addition, international and regional cooperation and coordination are highly essential, and need to include key international organizations, regional gatherings and professional and specialized international forums.

Strategic Objective

"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."

Pillars of Strategic Direction to Face Cyberthreats

The main preparedness pillars to face cyberthreats can be identified as follows:

- **Strategic and Executive Political and Institutional Support:**

  This includes raising awareness of the seriousness of cyberthreats and the need to address them as a priority and with the utmost urgency. This also entails placing an emphasis on preplanning, including developing strategic and operational plans, contingency plans and emergency coordination mechanisms; and preparing cadres and technical and logistic equipment.

- **Legislative Framework**:

  Establishing an appropriate legislative framework is essential for enhancing cyberspace security, combating cybercrimes, protecting privacy and digital identity and supporting information security, with the participation of key stakeholders, experts from the private sector and Civil Society Organizations (CSOs), guided by relevant international expertise, experiences and programs. This needs to be coupled with preparing and training professionals and specialists in law enforcement at judicial and police entities.

- **Regulatory and Executive Framework**:

  A regulatory framework and a national system for cybersecurity protection need to be established and set up, securing the ICT critical infrastructure, national information systems and databases, online government service portals and websites by preparing Computer Emergency Readiness and Response Teams (CERTs) in critical sectors at the national level, based on the pioneering experience of the ICT sector. CERTs are responsible for cybersecurity monitoring of national ICT networks and connected computers, addressing any cyberthreats or cyberattacks directed against them, raising awareness and strengthening readiness to confront cyberattacks.

- **Scientific Research and Development and Cybersecurity Industry Development:**

  It is essential to encourage, empower and develop scientific research and development, and support cooperation between research institutions and local companies, especially in the field of: advanced malware analysis, cyber forensic analysis, protecting and securing industrial control systems, developing devices and equipment for securing systems and networks, encryption and e-signature, protecting ICT infrastructure, securing cloud computing and protecting major databases.

- **Developing Human Calibers and Enhancing Expertise Needed to Implement Cybersecurity System at Various Sectors**

  This effort is to be carried out in cooperation and partnership with the private sector, universities and CSOs.

- **Cooperating with Friendly Countries and Relevant International and Regional Organizations**

  Cooperation includes exchange of experiences and coordination of positions in fields of improving cybersecurity and combating cybercrimes, since cyberthreats and cybercrimes do not recognize geographical or political boundaries.

- **Community Awareness**:

  Community awareness plans and campaigns need to be developed, highlighting the opportunities and benefits of secure e-services provided to individuals and organizations, and to raise awareness of the significance of cybersecurity to protect these services from the risks and threats that may affect them. This is in addition to protecting privacy and launching children online protection programs.

Implementation Mechanism

The Supreme Council for ICT Infrastructure Protection (Egyptian Supreme Cybersecurity Council (ESCC)):

The Ministry of Communications and Information Technology (MCIT) led efforts for the creation of a supreme council for ICT infrastructure protection (the Egyptian Supreme Cybersecurity Council (ESCC)), reporting to the Cabinet and chaired by the Minister of Communications and Information Technology. The Council is comprised of stakeholders involved in national security and infrastructure management and operation in critical sectors and public utilities, and experts from the private sector and research and educational entities. ESCC was mandated with developing a national strategy for cybersecurity and confronting cyberattacks. It supervises the implementation and updates of the strategy, in order to keep up with successive technological developments. The Council began its preliminary work in January 2015 and the Prime Minister approved the formation of ESCC Executive Bureau, Technical Committee and the description of their respective roles and responsibilities in June 2016.

Key Strategic Programs during the Current Phase (2017-2021)

1 Program to develop the appropriate legislative framework to secure cyberspace, combat cybercrimes and protect privacy and digital identity:

2 Program to develop an integrated national system for protecting cyberspace and securing ICT infrastructure:

3 Program to protect the digital identity (Digital Citizenship Program), to improve the infrastructure necessary to establish trust in e-transactions in general, and in e-government services in particular:

4 Program to prepare human calibers and expertise necessary to implement the cybersecurity system in various sectors:

5 Program to support scientific research and development and 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 risks and challenges.

1- Program to develop the appropriate legislative framework to secure cyberspace, combat cybercrimes and protect privacy and digital identity:

The program is to be implemented in cooperation with key stakeholders and experts from the government, private sector, academia and CSOs, guided by relevant international expertise, experiences and programs, and the African Union Convention on Cyber Security, recently adopted by the African Union (AU) Executive Council. A vacuum in cybercrime legislation may have serious consequences on e-transactions and e-services. The “Principle Of Legality in the Criminal Law and Penal Code”— one of the most fundamental principles—states that only the law can define a crime and prescribe a penalty, which restricts the application of penal provisions and the criminalization of acts that current legislation doesn’t define or prescribe appropriate punishment for them. Thus, states should keep abreast with developments and draft new and appropriate legislative rules to counter such contemporary crimes that threaten security of and trust in e-transactions.

2- Program to develop an integrated national system for protecting cyberspace and securing ICT infrastructure:

The program aims to prepare Computer Emergency Response (or Readiness) Teams (CERTs) or Computer Security Incidents Response Teams (CSIRTs), in the critical sectors at the national level, based on the pioneering experience of the ICT sector. CERTs and CSIRTs are responsible for monitoring security of national communications and information networks and connected computers, addressing any cyberthreats or cyberattacks directed against them, raising awareness and strengthening readiness to confront any cyberattacks.

3- Program to protect the digital identity (Digital Citizenship Program), to improve the infrastructure necessary to establish trust in e-transactions in general, and in e-government services in particular:

This program includes the Public Key Infrastructure (PKI), on which the e-signature is based. e-Signature is regulated and supervised by the Information Technology Industry Development Agency (ITIDA), through ITIDA- Egyptian Root Certificate Authority (Root CA), the Government Electronic Certification Authority (Gov-CA) operated by the Ministry of Finance, and other companies licensed by ITIDA to provide e-signature services. The program is based on the formation of a supreme committee for digital citizenship, aiming to prepare a strategic vision—at the national level— for digital citizenship and an action plan to transform the concept of digital citizenship into reality. It also aims to launch national projects aimed at using expanding applications that support facilitating and securing e-transactions relying on the PKI infrastructure.

4- Program to prepare human calibers and expertise necessary to implement the cybersecurity system in various sectors:

The program is to be implemented in cooperation and partnership between governmental entities, the private sector, universities and CSOs, based on the leading experience carried out by the National Telecom Regulatory Authority (NTRA).

5- Program to support scientific research and development and cybersecurity industry development

This program supports cooperation initiatives and projects between research institutions and local companies, especially in the fields of: advanced malware analysis, cyber forensics, protecting and securing industrial control systems, developing devices and systems for securing systems and networks, encryption and e-signature, protecting ICT infrastructure, securing cloud computing and protecting major databases. High priority must also be given to establishing national centers/ labs to adopt the systems, devices, software and applications used at key agencies and critical infrastructure.

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 risks and challenges.

This program includes organizing annual events and campaigns nationwide, as well as conferences, seminars and workshops in various sectors. It should address different levels, starting from the leadership level to children, school students, university students and citizens. Periodic reports should be issued and circulated to raise awareness of the most important cyberthreats, mechanisms used to address them, efforts employed, and other activities related to cybersecurity.

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 CSOs; 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.