Cybersecurity and National Anti-Corruption Efforts

Judge: Hatem Jaafar
Cybersecurity and Digital Forensics Expert at the International Telecommunication Union

Global awareness of the importance of cybersecurity has increased in recent years due to the significant development in the use of technology and the quality of that usage. This has necessitated the adoption of new means, leading to the emergence of the term "digital transformation" and an increase in reliance on these methods.

The urgent need to expand this digital transformation became evident with the emergence and spread of the COVID-19 pandemic worldwide, turning it from a choice and luxury into a necessary and indispensable lifestyle. This propelled the digital transformation in Egypt, with its numerous advantages such as saving time, effort, and money, as well as facilitating service delivery to citizens and enabling them to benefit from this development. This aligns with Egypt's Vision 2030. Consequently, securing the transactions resulting from digital transformation became essential within a coherent framework that complements the state's efforts to prevent and combat corruption in this technological environment. This has led to the emergence of new mechanisms and advanced methods to prevent and combat corruption, which require more advanced approaches.

Egypt has been committed to the field of cybersecurity early on and has aimed to be at the forefront of the Arab and African scenes in international indicators. It ranked 9th globally in the Global Cybersecurity Index (GCI) for 2014. In the context of cybersecurity governance at the national level, Egypt has issued the National Cybersecurity Strategy 2017-2021, aligning with modern global trends and constitutional obligations as stated in Article 31 of the Egyptian Constitution issued in 2014, which emphasizes that "Information space security is an integral part of the economic and national security system, and the state is committed to taking the necessary measures to preserve it, as regulated by law."

Egypt has sought to build and establish a modern system capable of protecting the Egyptian cyberspace. The Supreme Cybersecurity Council was established, chaired by the Minister of Communications and Information Technology, and it includes representatives from the government, private sector, and civil society. The Administrative Control Authority is also represented among its members. The Council aims to enhance cybersecurity in Egypt and protect vital government and private infrastructures from potential cyberattacks.

The Council has taken several regulatory decisions to achieve this goal, including the development of national cybersecurity capabilities and the enhancement of international cooperation in this field, in addition to overseeing the implementation of the National Cybersecurity Strategy.

Highlighting the role of cybersecurity in combating corruption requires emphasizing that corruption is a social, political, and economic phenomenon that threatens public order, national security, and sustainable development of countries. It can be defined as "deviation or destruction of integrity in the performance of public functions through bribery and favoritism." It can also be defined as "unethical acts committed by individuals occupying positions of power to achieve personal gains or abuse available resources."

The cybersecurity, as defined by the International Telecommunication Union (ITU), is "a collection of tools, policies, guidelines, risk management approaches, actions, training, best practices, assurance mechanisms, and technologies that can be used to protect the availability, integrity, confidentiality of assets in connected infrastructures, including networks, devices, employees, infrastructure, applications, services, and data in the cyberspace environment."

One of the most dangerous forms of cybercrimes targets governmental sectors, especially those responsible for combating corruption. These sectors require high protection for their data and systems from any external interference that may aim to disrupt their operations, disclose confidential information, alter investigation results, tarnish their reputation, or disable their services. These measures are the core of what cybersecurity aims to achieve through three main objectives:

1. Confidentiality: It prevents unauthorized access to information, allowing only authorized individuals to modify, delete, or add to it.
2. Integrity: It ensures the accuracy and integrity of information when entering, storing, or transmitting it within the system.
3. Availability: It guarantees access to information at any time without disruption. Compromising any of these three components is a violation of cybersecurity measures.

Considering the previous definition of cybersecurity and its components, as well as the definition of corruption, we find that cybersecurity is the anti-corruption apparatus in automated systems and their databases after digital transformation. The more cybersecurity policies are accurately implemented, the more an organization's ability to prevent and combat corruption increases, taking into account external breaches, the evolution of technologies used for vulnerability detection, and internal threats (insider threats) resulting from collusion of some corrupt individuals within the organization. Hence, continuous work is required to:

1. Raise awareness among users about the importance of cybersecurity and enhance their capabilities.
2. Regularly update systems and software used and follow up on that.
3. Utilize security programs to detect and analyze cyberattacks.
4. Keep up with global advancements in this field, especially in the use of artificial intelligence techniques.

Cybersecurity always consists of three essential components: people, processes or operations, and technology. These components must integrate to achieve cybersecurity. Purchasing the latest systems and implementing best practices is not beneficial without conscious personnel capable of understanding and working with the system. Similarly, having knowledgeable personnel and advanced technologies without clear procedures and policies would be a waste of resources. Therefore, it is an integrated triangle where each component is indispensable to the others.

To achieve cybersecurity governance within state institutions and others, it is necessary to adopt a cybersecurity strategy that includes well-defined legislative and regulatory frameworks and declared policies that govern procedures, practices, and accountability within digital systems. Responsibilities and authorities between the executing and auditing entities must be clearly defined to prevent interference. There should also be specific and transparent mechanisms for oversight and accountability in both the public and private sectors.

The relationship between cybersecurity and combating corruption is always positive. The more awareness and attention given to implementing cybersecurity standards and controls, the greater the prevention and combating of corruption. Empowering cybersecurity governance is crucial as it forms the backbone of cybersecurity. When countries and institutions prioritize it, the results are impressive. Having a clear, well-regulated, and declared cybersecurity policy enhances transparency and enables monitoring, whether through data classification and access authorization or through the analysis of automated system results.

One of the most dangerous forms of cybercrime are the ones that target government sectors, especially those responsible for combating corruption. These sectors require high protection for their data and systems from any external interference that may aim to disrupt their operations, disclose confidential information, manipulate investigation results, tarnish their reputation, or disable their services

Egypt has been devoted to the field of cybersecurity since early on and has been at the forefront of countries striving for continuous improvement and pioneering experiences in the Middle East. It achieved 9th place globally in the Global Cybersecurity Index (GCI) for 2014. In light of cybersecurity governance at the national level, Egypt has issued the National Cybersecurity Strategy 20172021-, committing to modern global trends and constitutional obligations

In the era of digital transformation, where process reengineering and control were dominant terms, having specific procedures and instructions that hold individuals accountable for their actions has become the optimal standard for auditing and review. The presence of cybersecurity policies and controls highlights the importance of cybersecurity and its effective role in preventing and combating corruption.

Since combating corruption is one of the most important challenges facing societies worldwide, and cyber threats are an integral part of these challenges, fighting corruption through cybersecurity requires the use of a wide range of tools and applications that help detect and prevent cyber crimes. These tools include:

- Network monitoring tools: They assist in detecting unauthorized activities on networks, mitigating cyber risks, and countering electronic attacks. It is preferable to have a Network Operations Center for this purpose.
- Data analysis tools: They are used to identify unusual or suspicious patterns based on the nature and characteristics of databases and functions.
- Data encryption and decryption tools: They are used to protect sensitive data.
- Anti-virus and anti-malware tools: They work to block and remove viruses and malicious software.
- Identity and access management tools: They verify authorized users and manage their access.
- Privilege management tools: They administer and assign account permissions.
- Cyber incident management tools: They help in the recovery of systems and data.

The real challenge in the current stage is the transition to digital transformation without the ability to keep up with a strong and solid cybersecurity framework. This in itself is a corruption in the administrative path because the expenditure on cybersecurity in institutions represents only one percent of the losses, especially in some ransomware attacks, data encryption, and data leakage, especially since it falls within the digital assets that require protection, especially critical infrastructure of the state. It is enough to say that the cost of cyber attacks on the global economy is expected to exceed $11.5 trillion in 2023, and the global cost of cybercrime is projected to reach $23 trillion by 2027.

We face numerous challenges and risks, but the challenges of combating corruption, especially in cyberspace, represent a new pattern that requires the ability to confront and counter it. This starts with conducting an analytical study of systems, explaining the reasons for granting and denying permissions, testing the system's source code, examining vulnerabilities, and addressing them, leading to assessment reports and performance indicators for the entire system.

Determining permissions based on characteristics and job titles in the system helps regulate performance and governance of authorities. The foundation for this is the principle that "knowledge is proportional to the need," and the need is determined by the functional attribute. This prevents any corruption resulting from overlapping authorities, lack of clarity, or user exploitation because every permission holder is required to maintain and exceed their responsibilities and not compromise what is attributed to them within the electronic system. There is no room for denial of responsibility with the identification of digital identities and ensuring access through identity verification systems and others.

Working within state systems, especially in cases of diversity and variation in technologies and structures, requires a high level of expertise and flexibility in securing, analyzing, and processing their data while adhering to regulatory laws. Big data is the future's oil, and detecting manipulation patterns within it is the ability to analyze this oil and prevent and combat corruption within it.