



Date: 13 October 2021 Issue: 649 Source: youm7.com

## 6-hour outage of Facebook platforms ...

A dark night for social media ... The world is in confusion without Facebook, and Zuckerberg loses \$7 billion from his net worth so far ... WhatsApp has not fully recovered



Facebook services are slowly getting back online after one of the biggest outages in recent memory, and the Facebook, Instagram and Messenger apps seem to be working again, although websites are loading slower than usual. Meanwhile, WhatsApp appears to be working again in some regions, but the application in general is still suffering connectivity issues.

[Link to the News Story](#)

## Our Views

What the world witnessed in terms of the interruption of social media platforms, and the seizure and circulation of customer data is not new. This interruption has occurred previously, but this time was the longest and the most extensive. Aside from the magnitude of initial expert estimates about the financial losses from this interruption - which may reach about \$160 million<sup>1</sup> - the matter has many other dimensions; including the role and importance of cybersecurity in addressing such matters, which is the focus of this issue.

Cybersecurity is a double-edged sword; while it may play a supportive role in achieving sustainable development, it can also be an obstacle. Issues of technology governance and standards related to transparency, privacy, protection and others remain a constant concern of the international community. The World Economic Forum indicated in the Competitiveness Report issued in 2019 that the pace of innovation in technologies related to the Fourth Industrial Revolution is proceeding in a way that far exceeds what is being done in the field of governance of these technologies, this becomes a new challenge facing both the developed and developing world alike.

The Global Risks Report issued by the World Economic Forum for 2021 ranked cyber risks among the most prominent threats to the world during the next ten years. The volume of losses borne by the world as a result of cyber-attacks is expected to

---

<sup>1</sup> <https://twitter.com/netblocks/status/1445073059237466123?lang=en>

double from about \$5 trillion in 2020 to about \$10.5 trillion by 2025.

It is estimated that the economic cost of cyber-attacks to companies studied in the Middle East and North Africa in 2021 is about \$6.9 million per incident which is higher than the global average cost of about \$4.2 million per incident—and that small and medium-sized businesses are the most affected.<sup>2</sup>

Locally, Egypt witnessed many cyber risks, the most recent of which was the theft of EGP 3 million from Banque Misr's customers' accounts by hacking their data in August 2021.<sup>3</sup> There are many other risks that are not disclosed due to fear of losing their customers' trust.

All these global and local events renew and emphasize the importance of cybersecurity as one of the pillars of national security, especially following the Corona pandemic that drove all countries, including Egypt, to shift toward digitization.

In principle, Egypt recognizes the importance of enhancing cybersecurity. Article No. 31 of the Egyptian Constitution issued in 2014 was devoted to emphasizing that the security of the information space (cybersecurity) constitutes an essential part of the systems composing the economy and national security. Several serious steps in this direction followed, including the establishment of the Supreme Council for Cybersecurity in 2014,<sup>4</sup> the launch of the National Cyber Security Strategic Plan

---

<sup>2</sup> IBM Security, "2021 Cost of a Data Breach Report", available at: [Enterprise Security | IBM](#).

<sup>3</sup> <https://ar.scoopempire.com/%d8%b3%d8%b1%d9%82%d8%a9-%d8%ad%d9%88%d8%a7%d9%84%d9%8a-3-%d9%85%d9%84%d9%8a%d9%88%d9%86-%d8%ac%d9%86%d9%8a%d9%87-%d9%85%d9%86-%d8%b9%d9%85%d9%84%d8%a7%d8%a1-%d8%a8%d9%86%d9%83-%d9%85%d8%b5%d8%b1/>

<sup>4</sup> Prime Minister's Resolution No. 2259 of 2014.

2017-2021, and the establishment of the Egyptian Computer Emergency Readiness Team (EG-CERT). The key question here is how effective are these efforts? especially since Egypt came in 23<sup>rd</sup> place out of 192 countries according to the Global Cybersecurity Index issued by the International Telecommunication Regulatory Union for 2020 that was issued in 2021 . This a low ranking compared to other countries such as Saudi Arabia (2), UAE (5) and India (10). This shows that there are challenges in the different dimensions covered by the index.

It remains unclear as to what extent the efforts adopted by Egypt are sufficient to enhance cybersecurity and raise the degree of its personnel, material, technological, legislative and institutional readiness for the technological revolution, and the opportunities, threats and risks inherent therein. This question raises a number of sub-questions:

- To what extent are the various parties aware of digitization in its proper sense; which goes beyond mechanization, and includes cybersecurity as one of its pillars?
- To what extent are the cybersecurity strategy and investment areas linked to the state's plans for economic, social and investment development?
- Is there effective coordination between the agencies responsible for cybersecurity and those responsible for digitization?
- To what extent is there a role for the private sector in the state's cybersecurity efforts and potential investments in this field?

- What are the adequacy and efficiency levels of the services of the Egyptian Computer Emergency Readiness Team and the extent to which private sector institutions benefit from its services?
- What is the rate of implementation of the objectives set in the National Cybersecurity Strategy 2017-2021; considering that it did not assign tasks to specific entities, and did not include performance indicators for follow-up and evaluation?
- Does the new strategy that is currently being prepared avoid the problems of its predecessor?
- How extensive are ongoing works to complete the legislative structure of cybersecurity, whether through new laws related to data management, digital identity, or through the development of existing legislation?
- Is the government raising awareness regarding issues related to cybersecurity in the required manner, in terms of quantity and quality? Are there incentives to ensure the retention of human resources after qualifying?
- What are the state's efforts in spreading the culture of cybersecurity for society as a whole and for the private sector in particular? Especially that there is a tendency for some countries to provide tax incentives to the private sector to encourage it to pay attention to cybersecurity issues.

Finally, it should be emphasized that cybersecurity is a condition for the success of digitization. Therefore, the state's approach should not be limited to collecting revenue from traders on social networking sites, as the issue has more

serious dimensions, and calls for greater efforts to effect the governance of these businesses.

### **Worthy of Note:**

ECES has made many efforts to support the government's digitization process in the proper manner, by evaluating current efforts and identifying the required policies in light of best practices, as highlighted in what follows:

- In January 2019, ECES, in cooperation with the Ministry of Communications and Information Technology, and the Ministry of Planning and Economic Development; held a series of workshops titled\* "A Detailed Research Agenda to Enhance Ongoing Governmental Efforts to Digitize the Egyptian Economy. Its 3<sup>rd</sup> Workshop\*\*", held on February 27, 2019, focused on the issue of information generation and protection.
- In December 2019, ECES organized, in cooperation with KPMG Egypt, a joint conference entitled "Managing Cyber Security and Its Risks: Focusing on the Case of Egypt" \*\*\* (cyber Security and Risk Management Summit: A State of Cyber Security, Regulations and Trends in Egypt).<sup>5</sup>
- ECES published a study on the concepts of Digitization and Cybersecurity Governance in June 2020. \*\*\*\*

\*"A detailed research agenda to support the government's digital transformation of the Egyptian economy;"

---

<sup>5</sup> [https://home.kpmg/eg/en/home/events/2019/12/cyber\\_security\\_summit\\_2019.html](https://home.kpmg/eg/en/home/events/2019/12/cyber_security_summit_2019.html)

\*\* Third workshop

\*\*\* “Managing Cyber Security and Its Risks: Focusing on the Case of Egypt”

\*\*\*\* Digital Transformation and Cybersecurity Governance

Source:

World economic forum (WEF). 2021. Global Risks Report. 16th Edition, WEF: Geneva.

———. 2019. Global Competitiveness Report. WEF: Geneva.

Khashaba, Majed et al. 2021. The developmental and strategic dimensions of cybersecurity and its role in supporting digital and encrypted economies: Paths of the Egyptian experience in light of global experiences. Institute of National Planning, Planning and Development Issues No. 325. Institute of National Planning: Cairo.

[Previous Issues](#)

[Other Reports](#)



## Disclaimer

This report was prepared for distribution to members of the Egyptian Center for Economic Studies only and may not be published or distributed without the written consent of ECES management. The data, analyses or information contained in this report do not constitute any form of recommendation or assurance of the commercial feasibility of the activity subject of the report or its ability to achieve certain results.

The data and investment analyses contained in this report were prepared based on the viewpoint of ECES, and rely on information and data obtained from sources we believe in their validity and integrity. We believe the information and conclusions contained in this report are correct and fair at the time of their preparation, and should not be considered as a basis for taking any investment decision. ECES is not responsible for any legal or investment consequences as a result of using the information contained in this report. Any errors that may have occurred at the time of preparing these data are accidental and unintentional.

Egyptian Center for Economic Studies (ECES)  
All rights reserved