Proposal to prepare

International agreement on the use of information technology in cybercrime

Today, digital technology is the main driver of life. It has become the largest part of daily dealings at all levels, for citizens or a government.

Many of the modern concepts of digital technology have led to its great exploitation in many topics that affect people's lives, and its poor use has led to a tool of crime, which is called cybercrime.

This technology has also been used in the absence of international law to protect data in violation of sovereignty, both at the level of individuals and societies as well as the government of states.

What we notice today is the absence of an international document in which all countries participate in setting policies for the general framework for combating and reducing cybercrime.

From this point of view, an international policy document must be prepared for all stakeholders to cooperate and issue local laws in countries in line with the international policy to combat cybercrime.

Therefore, we present to all a proposal for an international committee to establish an international agreement to address the foundations, sources, and tools of cybercrime.

The general framework of the document should include the following areas:

1. .Cooperation between countries in the field of capacity building in the fight against cybercrime.
2. Capacity building on electronic forensics.
3. Preparing the foundations for electronic forensics.
4. Governance of the mechanism of interaction between countries concerning electronic crime.
5. Issuance of a comprehensive document focusing on cyber security for IT infrastructure and digital services service providers.
6. Imposing general cybersecurity policies on information technology infrastructure service providers. which may be used in cybercrime.

7. Forming a technical working group to lay the international foundations for tracking cybercrime.
8. Drafting firm procedures to issue legislation on the mechanism for verifying personal identity in electronic applications.
9. Requiring companies and institutions, whether governmental or otherwise, to adopt a privacy protection policy and not allow access to it except by legal procedures.
10. The cooperation of electronic service providers, especially digital platforms, in cooperation with judicial authorities in all countries regarding the exploitation of these platforms as tools for cybercrime.
11. Instruct countries to develop their laws on cooperating with cases involving virtual crime.
12. Encouraging countries to pass legislation to regulate digital businesses as well as cybersecurity laws.
13. Form a team or committee to follow up on international policies to periodically evaluate international laws and treaties in the field of cybersecurity.
14. Launching projects in countries to raise awareness and spread culture about virtual cybercrime, its tools, and methods
15. Drafting a document obligating manufacturers of infrastructure equipment and peripheral devices, as well as developers of electronic and digital services, not to violate privacy, and to use and circulate data without obtaining the consent of the data owner, whether a person or an institution.
16. Requiring companies manufacturing software, operating systems, telecommunications, and data transmission companies to make maximum efforts to limit the phenomenon of intrusions.

Regards,

Abdulbaset Albaour

Chairman of the General Authority for Communications and Informatics – Libya

a.albaour@gia.gov.ly