SUMMIT IMPLEMENTATION REVIEW GROUP (SIRG)
Ad Hoc Technical Group on the Regional Agenda for Digital Transformation
First meeting
December 13, 2023

OEA/Ser.E
GRIC/CA-IX/GT-DIG/INF.3/24
18 January 2024
Original: Spanish

CONTRIBUTIONS OF CIVIL SOCIETY AND SOCIAL ACTORS

Cybersecurity

28.

The essential roles of dynamic and resilient digital ecosystems are to support vibrant digital economies; enhance preparedness for future health, natural disaster, and climate events; promote digital inclusion for all peoples; encourage respect for human rights and fundamental freedoms; increase innovation, competitiveness, and investment; optimize the provision of public services; and strengthen digital governance, transformation, and trust in the region by leveraging emerging and digital technologies, as some of the opportunities we still have pending. Digital transformation implies digital access as a human right, with an open, interoperable and secure Internet, and with broad access to digital technologies, thus ensuring the digital inclusion of all members of society.

We recommend the creation of a joint country platform to generate and manage reports focused on cybersecurity protection, management, and best practices.

The possibility of encouraging and opening spaces for active listening and permanent participation will enable short and medium-term actions to be envisioned, allowing the design of a list of criteria for possible risks, preventive actions, and first responses to future attacks, in line with the constant advance of technology.

29.

Member states aim to promote specialized digital development in cybersecurity in the region, with a focus on strengthening different stakeholders' cybersecurity risk management and identification capacities and on encouraging appropriate digital behaviors and practices by society at large.

Promote regular engagement where cybersecurity organizations link up to review the latest trends and methods for staying secure, which will allow citizens and businesses to stay up-to-date on evolving knowledge and recovery processes in cybersecurity. We suggest the creation of "cyber insurance" to protect member states, companies, and civil society from losses due to cyber attacks.

30.

Member states should encourage the discussion of standards and the exchange of best practices in the areas of cybersecurity and protection of users and consumers, as well as citizens in general, in relation to cybercrime prevention, in line with the provisions of international and regional instruments, such as the Convention on Cybercrime of the Council of Europe (Budapest Convention), where applicable, with participation of the private sector, academia, and other stakeholders. Standards should be included in all international, academic, and trade agreements and instruments. The standardization of the minimum cybersecurity protocol for the protection of cloud-based companies must be offered. Encourage adoption and best practices based on minimum standards. Promote collaboration between private companies and government organizations to support each other in the event of evidence of a cybersecurity threat.

31.

Member states agreed to promote and strengthen international cooperation among States to effectively prevent, prosecute, investigate, and try cybercrimes, illicit use of data belonging to government agencies, private institutions, and individuals, as well as other criminal activities supported by the misuse of information and communication technologies, such as human trafficking, migrant smuggling, child sexual exploitation and other forms of sexual violence, illicit drug and arms trafficking, and money laundering, among others, in a framework of respect for human rights and with a gender perspective.

Member states are committed to reviewing existing laws to punish cybercrimes committed by adults against children, adolescents, people with disabilities, and older persons, as well as those committed through third parties hired to engage in psychological terrorism, actual persecution, and identity theft against people exercising their political rights, especially those in which the victim is a minor or a member of a group considered vulnerable.

There is a lack of open-data solutions to share information on cybercrime, human trafficking, and missing migrants among member states.

Given that the United States and Canada are technology pioneers, it is important that they support other member states that are less deployed in this area in developing protocols to ensure that information technology and communication services are protected, especially those that serve the areas of health care, human rights advocacy, and environmental defenders, as well as organizations that provide basic services to the population.

32.

Promote technical assistance, programs, projects, and transfer of capacity and experiences in preventing cybercrime in information and communication technologies (ICTs) among states, in accordance with each country’s domestic legal system. Prior to approval, an agreement on cybercrime and technology must be adopted that goes hand in hand with compliance with regulations on the international legal system, the Inter-American Democratic Charter, and the Universal Declaration of Human Rights.

33.

Support discussions at the United Nations and other global and regional fora, on existing and emerging threats, the development and implementation of the framework for responsible behavior by member states in cyberspace, including respect for international law in activities in cyberspace, confidence-building measures, capacity building, and institutional dialogue to foster responsible use of ICTs by member states, and international peace and stability.

Digital transformation must recognize the right to identity; all citizens are required to have access to their identity and citizenship documents—which must not be limited for political, social, cultural, ideological, or economic reasons—and diasporas and exiles should have the right to vote (e-democracy).

Discussions or meetings should have several approaches:

Self-financing by each State, rectification of the agreement by member states, and incorporation into the legal framework in each country of what has already been approved; conclusion of the progress audit and verification of results to qualify for technical assistance financing for self-sustainability. This should take place in a cybersecurity context.

The main requirement to participate in the next international event and be part of the international platform for CICTE certification is for the member state to obtain a certification of legitimacy of its electoral process from the Permanent Council of the OAS.

34.

Strengthen articulation with the private sector, academia, civil society, and other stakeholders to promote shared responsibility and cooperation, and design coordinated actions for digital security and trust in the face of risks in the digital world. Digital transformation as a context of important dynamism requires permanent follow-up on the commitments adopted at the Ninth Summit of the Americas, which is why civil society actors and organizations propose the creation of the Digital Transformation Observatory of the Americas.

Collaboration between private and governmental agencies should be encouraged to guarantee the legitimacy of electoral processes (before, during, and after the event) by protecting the integrity of the final data in any election held in member states.

Within the digital transformation space, one point to emphasize is the identification of critical infrastructure, especially that which provides basic services to citizens; this should be not according to their intended purpose, but their location, and should be categorized by the degree of impact in the event of a cyber attack, in order to achieve a probability metric. The possibility should also exist of performing a threat review with a view to ensuring better protection and care by member states. Critical infrastructure protection in the digital age is a permanent task, and collaboration between governments, private companies, academia, and other stakeholders is essential to effectively address such threats. Develop an emergency protocol every 12 months as a nationwide emergency response to war and cyber attacks.

The collaboration of private companies, governmental organizations, academia, and civil society is essential to protect cyberspace in democratic countries.