|  |  |
| --- | --- |
| **Telecommunication Development Advisory Group (TDAG)**  **30th Meeting, Geneva, Switzerland, 19-23 June 2023** | A close up of a sign  Description automatically generated |
|  |  |
|  | **Document** **TDAG-2****3/36-E** |
|  | **6 June 2023** |
|  | **Original:** **English** |
| Timor Leste | |
| Advancing Cybersecurity to Propel Timor Leste’s Digital Transformation | |
|  | |
| **Summary:**  This contribution emphasizes the complex challenges faced by Timor Leste, one of the Least Developed Countries, as it endeavors to embark on a transformative digital journey. While Timor Leste acknowledges the urgent need for digitalization, it must simultaneously grapple with the growing risks presented by cyber threats, cyber incidents, and cyber crimes. Given the existence of global resolutions aimed at addressing cybersecurity challenges encountered by member states, particularly those in the LDC category, it is crucial to facilitate the operationalization of these commitments by providing accelerated support and interventions.  **Action required:**  TDAG is invited to consider this document and provide guidance as deemed appropriate.  **References:**  WTDC Resolution 45 (Rev. Kigali, 2022) – Mechanisms for enhancing cooperation on cybersecurity, including countering and combating spam  ITU-D Study Group Question 3/2 – Securing information and communication networks: Best practices for developing a culture of cybersecurity | |

1. **Introduction**

Resolution 45 (Rev. Kigali, 2022) Mechanisms for enhancing cooperation on cybersecurity, including countering and combating spam, calls for the continuation of recognising cybersecurity as one of ITU's priority activities and to address the issue of building confidence and security in the use of telecommunications/ICTs, by , among others, raising awareness, identifying best practices, providing assistance in implementing technical measures, enhancing collaboration and cooperation with all relevant international and regional organisations taking into account the need to assist developing countries. In that regard, instructs the Director of the Telecommunication Development Bureau to continue carrying out studies on strengthening the cybersecurity of developing countries based on a clear identification of their needs including countering and combating spam as well as the online protection of children and youth and any vulnerable persons. Moreover it instructs the director to, among others:

* to support developing countries, regarding mechanisms for enhancing cooperation on cybersecurity, including countering and combating spam; and
* to disseminate to the developing countries information on guidelines, recommendations, technical reports and best practices related to cybersecurity
* to assist developing countries with guidance and best practices to overcome challenges in terms of cybersecurity and spam arising from new and emerging technologies;
* to assist the developing countries in enhancing their states of preparedness in order to ensure a high and effective level of cybersecurity, including cyberresilience, for their critical telecommunication/ICT infrastructures, and
* to assist in the establishment of an appropriate framework between developing countries allowing rapid response to major incidents and propose an action plan to increase their protection and strengthen cyberresilience, taking into account mechanisms and partnerships, as appropriate;

Question 3/2 Securing information and communication networks: Best practices for developing a culture of cybersecurity includes:

* promoting sound, open, transparent, collaborative and future-proof policy and regulatory decisions with a view to facilitating digital transformation in the aftermath of the COVID-19 pandemic and beyond;
* fully exploiting the opportunities provided by digital transformation of various sectors of the economy by supporting all relevant stakeholders to unleash new and emerging telecommunication/ICT technologies and services.; and
* providing support to and cooperating with developing countries, including LDCs, LLDCs and SIDS, in addressing their constraints for accessing digital-centric new and emerging telecommunication/ICT technologies and services and for the integration thereof into different sectors, such as government services, agriculture, education, health, finance, transport, etc

Timor Leste is undertaking a significant initiative to embark on a comprehensive digital transformation journey, as outlined in the Strategic Development Plan (SDP) 2011-2030 and more recently, the Timor Digital 2032 roadmap. The latter is a roadmap for the Eighth Constitutional Government to embrace digital technologies as a catalyst for national development. The emphasis is on leveraging digital solutions in vital areas that have the greatest potential to enhance human well-being and economic growth. This includes the efficient delivery of government services, fostering an inclusive economy, and improving services in crucial sectors such as healthcare, education, and agriculture.

The Strategic Development Plan 2011-2030 and the national digital transformation roadmap play a pivotal role in driving Timor-Leste's progress and competitiveness in the digital age. They serve as a blueprint that outlines the strategic initiatives and policies required to harness the power of technology and digitization across various sectors. By aligning government, industry, and society, a national digital transformation roadmap enables the efficient and effective adoption of digital technologies, fostering innovation, economic growth, and societal development. They emphasize the importance of infrastructure development, digital literacy, cybersecurity, data governance, and the creation of a conducive ecosystem for digital entrepreneurship and innovation. Furthermore, the roadmap promotes inclusivity by ensuring equitable access to digital services and bridging the digital divide, thereby empowering citizens, businesses, and government entities to fully embrace the opportunities and benefits of the digital revolution.

However as Timor Leste, a country UNCTAD currently characterizes as a least developed country (LDC), venturing into digital transformation, cyber risks can pose significant challenges and threats. As a LDC country embraces digital technologies to drive economic growth and development, it becomes more susceptible to cyberattacks and data breaches. Arguably LDCs may lack the necessary infrastructure, expertise, and resources to effectively address and mitigate cyber risks. The digital transformation journey may expose Timor-Leste to various vulnerabilities, such as weak cybersecurity frameworks, limited awareness of cyber threats, inadequate data protection measures, and a shortage of skilled cybersecurity professionals. Additionally, a LDC may face heightened risks due to factors like limited financial resources, political instability, and inadequate legal and regulatory frameworks. Cyberattacks can have severe consequences, including financial losses, disruption of critical services, compromised personal data, and damage to the country's reputation. Therefore, it is essential for LDCs embarking on digital transformation to prioritize cybersecurity and invest in robust measures to safeguard their digital assets, strengthen their cybersecurity capabilities, raise awareness among stakeholders, and collaborate with international partners to address cyber threats effectively.

In the face of these challenges, Timor-Leste has set-up the Timor-Leste Computer Security Incident Response Team (TLCSIRT).

Additionally, Timor-Leste is accessing ITU support on cyber security programs including those extended by ITU-D Sector Member including BitSight, Welchman Keen, and the Axon Partners Group.

1. **Cybersecurity Challenges faced by Timor Leste**

The readiness against cybersecurity challenges in Timor-Leste can be gauged by its robust cybersecurity capabilities, aimed at preventing, detecting, mitigating, and promptly responding to cyber threats. Furthermore, it involves effectively recovering from the negative consequences of such threats while acquiring valuable insights to strengthen digital resilience. A resilient digital ecosystem in Timor-Leste should have the ability to safeguard critical national infrastructure, governance, business development, the economy, and the general public, especially vulnerable groups. It must also respond swiftly and decisively against cyber attacks to ensure the protection and well-being of internet users.

For Timor-Leste to achieve digital resilience, the following areas require improvement:

1. Infrastructure Development: to invest in developing robust and reliable digital infrastructure, including high-speed internet connectivity, data centers, and secure communication networks. This infrastructure forms the foundation for a resilient digital ecosystem.
2. Cybersecurity Capacity Building: Building cybersecurity capabilities is crucial to protect against cyber threats. Timor-Leste should invest in training programs, workshops, and certifications to enhance the technical skills of cybersecurity professionals and promote awareness among government agencies, businesses, and the general public.
3. Legal and Regulatory Frameworks: to establish comprehensive legal and regulatory frameworks to govern digital activities, including data protection, privacy, cybercrime, and information security. These frameworks should align with international best practices to ensure effective governance and accountability.
4. Public-Private Partnerships: Collaboration between the government, private sector, and civil society organizations is vital to address digital resilience challenges. Establishing partnerships can facilitate knowledge sharing, resource allocation, and joint initiatives for cybersecurity capacity building, infrastructure development, and policy implementation.
5. Awareness and Education: to prioritize cybersecurity awareness campaigns and educational programs to promote safe digital practices among individuals, businesses, and government entities. Educating the public about potential cyber threats, best practices for online safety, and responsible digital behavior can significantly contribute to digital resilience.
6. Incident Response and Recovery: to develop TLCSIRT capabilities and to equip it with an effective incident response mechanism to detect, analyze, and respond to cyber incidents promptly. This includes developing procedures for incident reporting, coordination between relevant stakeholders, and recovery plans to minimize the impact of cyber attacks.
7. International Cooperation: Engaging in international cooperation and collaboration with other countries, regional organizations, and international bodies can provide Timor-Leste with access to expertise, resources, and best practices in building digital resilience. Participating in regional cybersecurity initiatives and engaging in bilateral partnerships can facilitate knowledge exchange and technical assistance.

By focusing on those areas, Timor-Leste can enhance its digital resilience, strengthen its cybersecurity posture, and mitigate the risks associated with the digital transformation, ultimately enabling sustainable development and economic growth in the digital era

Meanwhile, similar to other LDCs as highlighted in ITU literature, Timor-Leste is likely to face various challenges in establishing effective cybersecurity measures. These challenges include:

1. Limited Information, Awareness, and Technical Competence: a LDC normally encounters gaps in terms of information, awareness, and technical expertise required to develop its own cybersecurity measures. Addressing this gap is crucial for building a resilient cyber defence system.
2. Regulatory Framework Updates: a LDC normally struggles with the continuous updating of its regulatory framework to keep pace with the rapid production and expansion of malicious models, techniques, and products. A dynamic regulatory environment is necessary to address evolving cybersecurity threats effectively.
3. Competing National Budget Allocation: a LDC faces the challenge of allocating sufficient national budget resources to cybersecurity amidst more pressing development and service priorities. Balancing cybersecurity investments with other critical areas is a complex task.
4. Limited Access to Cybersecurity Information and Research: There is a lag in accessing up-to-date cybersecurity information, which hinders the country's ability to stay ahead of emerging threats. Furthermore, gaps in research and development, as well as cybersecurity-related digital skills and competence, pose additional challenges.
5. Coordination Gaps in Digital Transformation: a LDC experiences coordination gaps in digital transformation across different sectors, resulting in divergent security approaches and varying speeds of implementation. Ensuring alignment and synchronization in security aspects are necessary for comprehensive cybersecurity measures.
6. Dependence on External Hardware and Software: a LDC normally relies on hardware and software originating from external sources, limiting its control over their operations. This dependence may lead to the utilization of popular templates that are susceptible to manipulation and compromise by malicious actors.
7. Lack of Public Awareness: a LDC lacks sufficient public awareness regarding cyber hazards, particularly among specific groups such as children and women. Promoting awareness and education on cybersecurity risks is essential for protecting vulnerable segments of society.

Addressing these challenges will be crucial for Timor-Leste to enhance its cybersecurity posture and develop effective measures to safeguard its digital landscape and the well-being of its citizens.

1. **Related ITU Programs**

Timor-Leste would like to invite TDAG to consider support measures that will accelerate the strengthening of Cybersecurity in Timor-Leste as it embarks on Digital Transformation.

These measures may include:

* To deploy technical assistance and resources to develop the cybersecurity workforce pipeline within Timor-Leste;
* To enhance the capacity of the Timor-Leste Computer Security Incident Response Team (TLCSIRT) through targeted capacity building;
* To provide technical assistance and capacity building to enhance the cybersecurity of the educational sector in Timor-Leste through the proposed Safe and Secure School Connectivity project;
* To expand on the assistance under the Cyber4Good project by providing additional ITU-D Sector Member cybersecurity services and resources;
* To provide guidelines and training on safety and protection of internet users particularly children and women including access to ITU Child Online Protection guidelines and training, as well as advocacy and strengthening activities under the Women-in-tech and the International Girls in ICT Day;
* To further enhance the national cybersecurity strategy lifecycle in Timor-Leste through technical assistance and capacity building, including tabletop exercises;
* To sensitize stakeholders in Timor-Leste about the need to improve country’s score under the Global Cybersecurity Index and to provide recommendations on how to increase commitment to the Global Cybersecurity Agenda; and
* To establish a platform among LDCs and SIDS to share cybersecurity-related information and awareness; to identify and share case studies on cybersecurity risks and threats, and to examine the cybersecurity challenges in developing countries and recommend innovative solutions.

\_\_\_\_\_\_\_\_\_\_\_\_\_