[Ref: CL-19/47](https://www.itu.int/md/S19-SG-CIR-0047/en) - P**articipation in the process for developing guidelines for utilization of the Global Cybersecurity Agenda**

**Contribution submitted by Jordan**

| Area | Point # | Description | Response |
| --- | --- | --- | --- |
| **1- Legal Measures** | | | |
| 1 | 1.2 | Governments should cooperate with other stakeholders to develop necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks: for example, UNGA Resolutions 55/63 and 56/121 on "Combating the criminal misuse of information technologies" and regional relevant initiatives including, but not limited to, the Council of Europe's Convention on Cybercrime. | Highly agree |
| 1 | 1.3 | Considering the Council of Europe’s Convention on Cybercrime as an example of legal measures realized as a regional initiative, countries should complete its ratification, or consider the possibility of acceding to the Convention of Cybercrime. Other countries should, or may want to, use the Convention as a guideline, or as a reference for developing their internal legislation, by implementing the standards and principles it contains, in accordance with their own legal system and practice. | We echo the sentiment in the member notes, in regards to using Europe’s Convention on Cybercrime as a reference or guideline for developing legislation, but not necessarily to ratify the Convention itself. |
| 1 | 1.4 | It is very important to implement at least Articles 2-9 in the substantive criminal law section, and to establish the procedural tools necessary to investigate and prosecute such crimes as described in Articles 14-22 in the section on procedural law. | Governments should clearly mention the procedures that will be taken against the cybercrime this could be happened through establishing a standalone legislation to assist the judiciaries to do their work in transparent way.  As mentioned in report’s recommendations it is important to define the preservation of stored data, Search and seizure of stored computer data, Real-time collection of computer data, Extradition of cyber perpetrators, Confidentiality and limitation of use. And this should not be limited to computer devices but also extended to any devices that deal with data |
| 1 | 1.5 | Cybercrime legislation should be designed using existing international and regional frameworks as a reference or as a guideline, and the Convention on Cybercrime was designed in a way so that it could be adapted to technological developments, and laws using the Convention as a guideline should be able to address modern developments.  One member wished to delete the first phrase on how cybercrime legislation should be developed. A few other members wished to delete the text referring to the history of the design of the Convention and the normative statement as to what it might be able to achieve | We echo the suggestion to remove the first phrase, and focus more on the need for legislation to be able to adapt to technological developments. In addition, it is important for legislation to remain as agnostic as possible to specific technologies or protocols. Moreover, we do agree that could affect the developments of developed countries since an international framework could restrict them, but we can suggest to have a common baseline that help all member states to be at the same level of understanding about main articles of cybercrimes legislations |
|
| 1 | 1.8 | Countries should consider how to address data espionage and steps to prevent pornography being made available to minors.  One member considered that the term "data espionage" is ambiguous, and should be defined properly, whilst another member wished to remove this term. Two members wished to delete this recommendation | We are totally agree with a comment regarding to data espionage, this term need to be clearly defined since there are different perspectives in member states regarding personal data and how the local and international companies are deal with that. Deletion of that recommendation could raise negative consequences on the legal pillar since data are the key factor in cyberspace  In addition to that, we propose to add a new item related to combating the seizure / control of data through its encryption and financial extortion to restore this data or the so-called (Ransom ware) and emphasize the need for international coordination to combat this phenomenon |
| 1 | 1.9 | The introduction of new technologies always presents an initial challenge for law enforcement. For example, VoIP and other new technologies may be a challenge for law enforcement in the future. It is important that law enforcement, government, the VoIP industry and ICT community consider ways to work together to ensure that law enforcement has the tools it needs to protect the public from criminal activity.  Two members wished to delete this recommendation. Some members wished to replace the specific references to VoIP with more general text recognizing that the introduction of a broad range of new technologies presents initial challenges for law enforcement. One member supported reference to “government, industry and ICT community”, whilst another wished to make more general reference to “all relevant parties” [who] “should work together to ensure that law enforcement has the tools, resources and training needed” | We echo the suggestion to replace reference to VoIP with more general, technology/protocol-agnostic term |
| 1 | 1.10 | The implementation of a data retention approach is one approach to avoid the difficulties of getting access to traffic data before they are deleted, and countries should carefully consider adopting such procedural legislation.  Two members wished to delete this recommendation. Another member proposed the alternative text: “the implementation of a data preservation approach has proven to be a key resource to law enforcement in investigations. Development of a balanced and reasonable data retention requirement should be carefully examined, taking into account expectations of privacy, security risks, etc., when considering adopting such procedural legislation”. | Agree with the proposed article |
| 1 | 1.11 | In the fight against terrorist misuse of the Internet and related ICTs, countries should complete their ratification of the Convention on the Prevention of Terrorism of 2005. Other countries should, or may want to, use the Convention as a guideline, or as a reference for developing their internal legislation, by implementing the standards and principles it contains, in accordance with their own legal system and practice. Article 5 on public provocation to commit a terrorist offence, Article 6 on recruitment for terrorism, and Article 7 on training for terrorism are especially important. In addition, the Convention on Cybercrime has been studied with relation to terrorist misuse of the Internet and has been found to be important for defense against it.  One member wished to delete the last sentence. | This needs a revision of “Convention on the Prevention of Terrorism of 2005” because this is a critical issue since it is related to the terrorist. |
| 1 | additional recommendations | In addition to the above specific notes and comments, we have few general recommendations in the legislation area which are:   * There should be ways of some Encouragements for the use of PETs (privacy enhancing technologies) at the policy level in a way that preserves privacy without losing control. So, the Regulators should help/encourage PET adoption in any industry that deals with sensitive data. * Juridical legislations should emphasize the freedom of disclosure of sensitive information & data for developed countries, that is critical for the less developed countries in specific data & information that is related to national security of those countries. * Protection criteria of entry logs for citizens in the developing countries should be as well as DEVELOPED COUNTRIES in terms of protecting their privacy and mechanisms to deal with them in a manner that prevents their exploitation in spying on the actions of individuals. * International judicial legislation should be strengthen by combating the mechanisms of cyber bullying and to extend to campaigns / hate speeches based on religion / belief (for example, Islamophobia), race, color, abuse of human peoples, etc. and criminalize these practices internationally. * The legislations for the protection of privacy and the disclosure of data should be conducted and harmonized with developed countries. * With regard to clause (1.3) of the WA1 Recommendations, the concerned authorities should study the outcomes of the Council of Europe conference with regard to cybercrime, in order to verify its conformity with Jordanian legislation and discuss the possibility of benefiting from it on a voluntary basis and in a manner that takes into account Jordanian interests and does not conflict with the judicial ones, and therefore not Its application or adoption only by the signatory parties only. * Making sure cybersecurity is part of the dialogue at the highest levels of policy making and government organizations. * Juridical Legislation should include the protection of Cybersecurity aspects (CIA triad) Confidentiality, Integrity and availability and should also include critical Infrastructure for the energy sector (Nuclear Reactors), dams, water-resources management units, critical financial systems, Transportation, and agricultural projects. Also to emphasize more, to execute what mentioned within UNGA (United Nations General Assembly) Resolution No.(A/55/593/63). | |
| **2-Technical & Procedural Measures** | | | |
| 2 | 2.2 | ITU should take steps to facilitate it becoming the global “centre of excellence” for the collection and distribution of timely telecommunications/ICT cybersecurity-related information – including a publicly available institutional ecosystem of sources – to enhance cybersecurity capabilities worldwide.  One member preferred to refer to ITU being “a” global centre of reference rather than “the” global centre for reference, whilst another member expressed its opposition to making this change. | Adding:  Enabling a threat intelligence platform that helps CISRTs to share threat information. |
| 2 | 2.12 | Internet: HLEG Members called for the investigation of ways to collaborate with private industry to enhance the security of public communication networks and ISPs - for example, Trusted Service Provider (SPID) initiative, DNSSEC, or systemic and economic incentives for security for protection of global telecommunications might be further examined and discussed. In collaboration with private industry, the ITU may examine the role of ISPs in blocking spam and other issues. Particular attention should be paid to investigating results of SG 13 - ITU-T's largest and most active standards body that addresses global information infrastructure, Internet protocol aspects and NGNs that has engaged a broad, large cross-section of industry players and technical bodies. | To make ISP’s adopt Child protection programs and help in increasing the level of security threats for their subscribers. Also ISP’s should help inform their subscribers about vulnerabilities and risks. Also ISP’s should co-operate with governmental CISRT to implement CISRT’s recommendations. |
| 2 | 2.16 | Management system and personal certifications: HLEG members called for the selection and improvement of information security management system certification schemes, as well as personal information security certifications.  One member wished to delete recommendation 2.16. Another member understood rec. 2.16 to refer to information on security management systems, and identity management systems and 12 certification/compliance mechanisms for potential users. This member believed that many ICT markets operate well based on supplier declarations of compliance. The selection of systems and certification/compliance mechanisms is the user’s decision - UN agencies should only undertake selection processes for their own procurement, and not select them for others. | No company should work in cyber security field unless they have a certificate according to a predefined criteria |
| 2 | additional  recommendations | In addition to the above specific notes and comments, we have few general recommendations in the Technical area which are:   * More influential institutions ‎should evaluate the ‎advantages vs. threats posed ‎by evolving technologies, and ‎working with the pioneers ‎and developers of these ‎technologies to integrate data ‎protection in from the start.‎ * Moving away from the vender-buyer model, toward a more collaborative approach for dealing with cyber threats and development. Thus creating solutions better suited to the industry in question, and more ingrained into the fabric of the institution’s operations. * It is highly recommended to dedicate a group to analyze the gap between current Security guidelines for IoT Platforms, Cloud Computing and any emerging technology to help all members to revise their regulations accordingly to reduce the gaps and harmonize international efforts towards new emerging technologies * Share expertise on Digital Signature and Digital Identity frameworks, we recommend that EU countries should share their expertise on this subject. * Also data retention policies and instructions are different between member countries depending on factors that distinguish a particular country, like population, amount of traffic, number of licensed ISP companies and etc. Therefore the regulatory bodies that have already implemented such legislations can share their view on this issue. | |
| **3-Organizational Structures** | | | |
| 3 | additional recommendations | Regarding this work area, few recommendations would be sufficient such as:   * Propose industry specific structures (e.g. Financial CERT, Medicine CERT), if possible. This would help narrow the scope of potential cyber-intelligence to that which is most relevant. * Standardize DRP, Risk Management, Risk Assessment and incident response for all regulatory bodies for member countries, share and harmonize knowledge. * dedicate a specialized group that emerges from HLEG or Study Group 17 (SG-17) that is a part of ITU-D, which should be assigned the task or research & development for the impact of new technologies like the Internet of Things (IoT), Big Data, Artificial Intelligence (AI), on cyber security, and with membership of country members in order to follow up with the international best practices and recommendations * With regard to Working Group Three (WA3), Item (3,6) of the recommendations it is proposed to add to the text "The necessity of holding workshops and exchanging experiences on cybersecurity issues from the organizational aspects" | |
| **4-Capacity Building** | | | |
| 4 | additional recommendations | we have few general recommendations in the capacity building area which are:   * ITU should conduct more Table Top Exercises and cyber drills to help CISRTs. * Create a sort of Cybersecurity starter kit/program for new institutions that are relatively inexperienced in the field. Since nowadays, any institution, no matter how small, is at risk of cyber-attacks. * Institutions should be sure to create well-defined and structured response plans, with appointed individuals and designated responsibilities. * Provide an access portal for all regulatory bodies to share latest cyber security updates, threats and latest safe guards, and to notify members with any trans-country cyber-attacks. * ‎juridical Training and awareness is a key factor to ‎implement the ‎Cybersecurity legislations. ‎So, Judges should have a ‎detailed view of disclosing ‎of sensitive information and ‎Technical background of ‎dealing with cybercrimes * Allocate judicial chambers and trained judges to address issues related to cybersecurity and information security. | |
| **5-International Cooperation** | | | |
| 5 | additional recommendations | Regarding the international cooperation area, we have the following recommendations which are:   * There should be central body for national security and intelligence, so this body will be the institution with which the international community communicates and cooperates. * There should be support for regulatory bodies members in terms of cyber security capacity building, training plans and international certifications required for all member countries. * Establish an annual meeting included within SG-17 and ITU-D to discuss and share innovations and the emerging technologies and international policies available. * Reference to the United Nations General Assembly Resolution No.(A/55/593/63),of year 2001, in particular item 1(b), Law enforcement in member countries should include coordination in Trans-country Cyber Security Cases. * Making sure cybersecurity is part of the dialogue at the highest levels of policy making and government organizations. | |