ITUPublications
Study period 2018-2021

International Telecommunication Union
Development Sector

Study Group 2 Question 3

Securing information and communication networks: Best practices for developing a culture of cybersecurity

Output Report on ITU-D Question 3/2

Securing information and communication networks: Best practices for developing a culture of cybersecurity

Study period 2018-2021

Securing information and communication networks: Best practices for developing a culture of cybersecurity: Output Report on ITU-D Question 3/2 for the study period 2018-2021

ISBN 978-92-61-34101-5 (Electronic version)
ISBN 978-92-61-34111-4 (EPUB version)
ISBN 978-92-61-34121-3 (Mobi version)

Suggested citation. Securing information and communication networks: Best practices for developing a culture of cybersecurity: Output Report on ITU-D Question 3/2 for the study period 2018-2021. Geneva: International Telecommunication Union, 2021. Licence: CC BY-NC-SA 3.0 IGO.

Third-party materials. If you wish to reuse material from this work that is attributed to a third party, such as tables, figures or images, it is your responsibility to determine whether permission is needed for that reuse and to obtain permission from the copyright holder. The risk of claims resulting from infringement of any third-party-owned component in the work rests solely with the user.

General disclaimers. The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of ITU or its secretariat concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

The mention of specific companies or of certain manufacturers' products does not imply that they are endorsed or recommended by ITU in preference to others of a similar nature that are not mentioned. Errors and omissions excepted, the names of proprietary products are distinguished by initial capital letters.

All reasonable precautions have been taken by ITU to verify the information contained in this publication. However, the published material is being distributed without warranty of any kind, either expressed or implied. The responsibility for the interpretation and use of the material lies with the reader. In no event shall ITU be liable for damages arising from its use.

Cover photo credits: Shutterstock

Acknowledgements

The study groups of the ITU Telecommunication Development Sector (ITU-D) provide a neutral platform where experts from governments, industry, telecommunication organizations and academia from around the world gather to produce practical tools and resources to address development issues. To that end, the two ITU-D study groups are responsible for developing reports, guidelines and recommendations based on input received from the membership. Questions for study are decided every four years at the World Telecommunication Development Conference (WTDC). The ITU membership, assembled at WTDC-17 in Buenos Aires in October 2017, agreed that for the period 2018-2021, Study Group 2 would deal with seven Questions within the overall scope of "Information and communication technology services and applications for the promotion of sustainable development."

This report was prepared in response to Question 3/2: **Securing information and communication networks: Best practices for developing a culture of cybersecurity** under the overall guidance and coordination of the management team of ITU-D Study Group 2 led by Mr Ahmad Reza Sharafat (Islamic Republic of Iran), as Chairman, supported by the following Vice-Chairmen: Mr Nasser Al Marzouqi (United Arab Emirates)(resigned in 2018); Mr Abdelaziz Alzarooni (United Arab Emirates); Mr Filipe Miguel Antunes Batista (Portugal)(resigned in 2019); Ms Nora Abdalla Hassan Basher (Sudan); Ms Maria Bolshakova (Russian Federation); Ms Celina Delgado Castellón (Nicaragua); Mr Yakov Gass (Russian Federation)(resigned in 2020); Mr Ananda Raj Khanal (Republic of Nepal); Mr Roland Yaw Kudozia (Ghana); Mr Tolibjon Oltinovich Mirzakulov (Uzbekistan); Ms Alina Modan (Romania); Mr Henry Chukwudumeme Nkemadu (Nigeria); Ms Ke Wang (China); and Mr Dominique Würges (France).

The report was developed under the leadership of the Co-Rapporteurs for Question 3/2, Mr Michael Beirne (United States)(resigned in 2020); Mr Kwadwo Burgee (United States)(resigned in 2020); Ms Aimee K. Meacham (United States); and Mr Dominique Würges (France), in collaboration with the following Vice-Rapporteurs: Mr Damnam Kanlanfei Bagolibe (Togo); Mr Amine Adoum Bakhit (Chad); Ms Maria Bolshakova (Russian Federation); Ms Sonam Choki (Bhutan); Mr Yakov Gass (Russian Federation)(resigned in 2020); Mr Karim Hasnaou (Algeria); Mr Cissé Kane (African Civil Society on the Information Society); Ms Miho Naganuma (Japan); Mr Jean David Rodney (Haiti); Ms Jabin Vahora (United States); Ms Xinxin Wan (China); Mr Jaesuk Yun (Republic of Korea); and Mr Mohamadou Zarou (Mali).

Special thanks go to chapter coordinators for their dedication, support and expertise.

This report has been prepared with the support of the BDT focal points, editors, as well as the publication production team and the ITU-D study group secretariat.

Table of contents

List of tables and figure

Tables

Figure

Executive summary

The aim of Question 3/2 ("Securing information and communications networks: Best practices for developing a culture of cybersecurity") of the ITU Telecommunication Development Sector (ITU-D) is to develop best-practice reports on various aspects of cybersecurity.

This document constitutes the Final Report on Question 3/2 for the most recent study period (2018-2021), for which the work programme for Question 3/2 was established by the World Telecommunication Development Conference held in Buenos Aires in 2017 (WTDC-17).

Activities carried out in the previous study periods had focused on available coursework (2010-2014) and workshops to bring a broad set of actors and content to developing countries (2014-2017).

During the 2018-2021 study period, ITU-D Study Group 2 addressed most of the items in the work programme. A workshop was also held during the study period.

This report on Question 3/2 draws on the material submitted in ITU membership contributions over the study period. The report provides an overview of spam and malware, as well as means to address them. It sets out a number of lessons for national cybersecurity response planning and awareness-building campaigns. It points to particular actions for vulnerable populations, including persons with disabilities and children. In addition, the report contains ideas on smart cities, emerging technologies and data protection.

In the current digitalized world, where the daily lives of citizens as well as economies as a whole have both become increasingly dependent on digital technologies, there is an increased risk of greater vulnerability and exposure to cyberattacks. Cybersecurity has been identified as a priority and a paramount concern for industry, governments and Internet users all over the world, and is critical for secure, safe progress that allows society to grow.

This report aims to provide updated thinking and practices based on the experience of the ITU membership. Recognizing that the general environment and threat landscape are constantly evolving, it intends simply to be a current snapshot in this very sensitive domain of cybersecurity. The report is also published in a very specific and unprecedented context: while there are no specific references to the current pandemic, the impact of COVID-19 has been in the minds of many contributors and has informed the debates during the activities under Question 3/2.

The responses and proposals compiled in this report aim to help achieve a high level of cybersecurity across the ITU membership, and may also serve as a useful tool for tackling potential future crises, on top of the other actions undertaken by ITU.

Chapter 1 provides an update on the status of malware and spam and on mitigation responses. Note that the study group did not receive direct contributions on this issue.

Chapter 2 discusses how to improve national cybersecurity postures through awareness-raising and capacity-building opportunities.

Chapter 3 provides information on child online protection activities.

Chapter 4 discusses cybersecurity challenges for persons with disabilities.

Chapter 5 discusses cybersecurity challenges for emerging technologies, such as the Internet of things (IoT) and cloud computing.

Chapter 6 provides perspectives on how cybersecurity can support the protection of personal data.

Finally**, Chapter 7** considers future areas of exploration.

In addition to this report, it should also be noted that Question 3/2 reviewed the questionnaire serving as basis for the Global Cybersecurity Index (GCI) and provided its comments and proposals, allowing the Telecommunication Development Bureau (BDT) to conduct its annual survey among the ITU Member States. In particular, and through the initiative of Brazil, Question 3/2 developed the survey, which was incorporated in the GCI as an annex. The proposed revisions were included in the fourth iteration of the GCI 2020.

This report does not extensively address the GCI. Nevertheless, Question 3/2 highlights the positive result of the collective effort and rich collaboration with BDT, since the responses to the annex will provide information collected on regulatory policies that BDT will make available to the membership, thereby fulfilling study item "n" of the terms of reference for Question 3/2.

Chapter 1 – Update on the status of spam and malware, including mitigation responses

This section examines the evolution of spam and malware and sets out a number of countermeasures to be implemented at national, regional and international levels, pursuant to Resolution 45 (Rev. Dubai, 2014) of the World Telecommunication Development Conference (WTDC),[1] on mechanisms for enhancing cooperation on cybersecurity, including countering and combating spam. It thereby responds to items 2(b) and (m) of the terms of reference for Question 3/2 set out in the Final Report of WTDC-17:

b) *discuss approaches and best practices for evaluating the impact of spam and malware within a network, as well as evolving and emerging threats, and provide the necessary input for measures and guidelines, including mitigation techniques and legislative and regulatory aspects that countries can use, taking into account existing standards and available tools;*

m) *provide guidance on measures to combat spam and malware at national, regional and international level.* [2]

1.1 The status of spam and malware

Although there is no universally accepted definition for spam, it generally refers to unsolicited bulk electronic communications, delivered over computers or mobile phones through e-mail and text messages.[3] Consumers typically see spam in the form of advertising, including junk or unwanted commercial e-mails, texts and social media contacts.

Although spam commonly means commercial prospecting, it can also use similar user-generated data for criminal purposes, including phishing. By pretending to be trusted third parties, attackers use phishing e-mails encourage recipients to reveal personal data (access accounts, passwords, etc.) and/or banking data.

Spam creates risks for the security of connected users and organizations, not only because it is easily spread via the Internet and electronic communication services (e-mail, websites, social media, SMS and MMS), but also because it can carry malicious software. Countries are implementing various technical and regulatory mechanisms to combat spam, with some success.

Malware, for its part, has experienced strong growth in recent years due to the development of the Internet and, more specifically, the mobile Internet. Malware is a general term for software designed specifically to harm computers or computer systems.[4]

Moreover, increased connectivity, new technologies and the growth in the number of users has provided new opportunities for the creation and use of malware. This paradigm introduces

[1] ITU. Final Report of the World Telecommunication Development Conference (Buenos Aires, 2017), p. 409.

[2] Ibid., pp. 727-728.

[3] See Recommendations ITU-T X.1230 to X.1240, on countering spam.

[4] See Recommendation ITU-T X.1205 Supplement 9 (09/2011). Supplement on guidelines for reducing malware in ICT networks.

greater complexity for cybersecurity by opening gaps and expanding the attack surfaces available to malware threats. In addition to traditional malware (viruses, worms, Trojans, spyware, adware, spam, rootkits, etc.), new, more sophisticated types of malware have emerged, such as botnets, ransomware and mobile malware.

In short, countering spam and malware is critical for the security of users and the growth of businesses.

1.2 Spam and malware: Statistics, trends, evolution and the impact on electronic communication networks

As of March 2020, the proportion of spam in global e-mail traffic was 53.95 per cent.[5] In recent years, this percentage has dropped significantly, from 69 per cent in 2012 to 55 per cent in 2018, possibly as a result of advances in cybersecurity awareness and technological advances. Most spam received by users is promotional in nature, including marketing information. By one estimate, spam costs businesses almost USD 20.5 billion each year in lost productivity and technical expenses. It has been suggested that this cost could rise to USD 257 billion a year if spam continues to grow at its current rate.[6]

According to one estimate, scams and frauds account for around 2.5 per cent of all spam, of which a significant proportion (92 per cent) may be malicious in nature, i.e. associated with malware with the aim of harming users or compromising their IT systems for various purposes.[7] According to another estimate, around 812.67 million malware-related infections of various kinds were identified in 2018.[8] Mobile malware has increased by 54 per cent and ransomware by 350 per cent, while financial losses related to ransomware infections are estimated to cost USD 6 billion per year (until 2021).

As spam and malware can generate substantial traffic, they can have a significant negative impact on network infrastructure and operators and, in turn, on consumers' user experience. Spam-related issues, including resultant network problems, can also damage the reputations of operators.

In order to address these concerns, including potentially massive flows of unwanted traffic, and to ensure network quality, operators may need to develop new tools, including investing in safeguarding and expanding existing infrastructure. For example, service providers could invest in anti-spam filters to improve the quality of the services that they offer. These may entail necessary additional costs for operators and electronic communication service providers.

[5] Statista. Global spam volume as percentage of total e-mail traffic from January 2014 to September 2020, by month

[6] Spam Laws. Spam statistics and facts

[7] DataProt. What's on the other side of your inbox – 20 SPAM statistics for 2021

[8] PurpleSec. 2021 Cyber Security Statistics - The Ultimate List of stats, data & trends.

1.3 Approaches taken to combat and mitigate the effects of spam and malware

1.3.1 Technical approaches to combat and mitigate the effects of spam and malware

Unsolicited e-mail is one of the main channels of malware transmission. To fight spam and malware effectively, the chain of transmission must be broken. As technology has advanced, tools such as spam filters and antivirus software continue to be effective mechanisms for combating spam and malware. The effectiveness of such tools can be enhanced by using them in conjunction with new technologies, such as artificial intelligence (AI). Regularly updating spam filters and anti-virus software is therefore a good practice for users.

Among service providers, policies such as Sender Policy Framework,[9] DomainKeys Identified Mail,[10] Domain-based Message Authentication, Reporting and Conformance[11] and registration on real-time blocking lists can be used to reduce these chains of transmission.

Electronic communication network operators and Internet service providers can also take certain measures to address concerns related to the blocking of IP addresses. One example is Border Gateway Protocol Security using Resource Public Key Infrastructure.[12] Other initiatives include:

- Mutually Agreed Norms for Routing Security, which aims to collaboratively prevent state-of-the-art route hijacking, IP address spoofing and other malicious activities that can lead to distributed denial of service (DDoS) attacks, eavesdropping, loss of revenue, reputation damage, etc.[13]
- Messaging, Malware and Mobile Anti-Abuse Working Group, which regularly publishes best practices for combating abusive messages, all types of malware (including botnets), spam, viruses, denial of service (DoS) attacks and online abuse of any kind.[14]

Other initiatives in the fight against spam and malware include the Internet Society,[15] the Global System for Mobile Communications Association,[16] the Spamhaus Project,[17] the Anti-Phishing Working Group[18] and the Anti-Spyware Coalition.[19]

1.3.2 Examples of regulatory approaches to combat and mitigate the impact of spam and malware

Given the concerns and costs involved in combating spam and malware, in recent years some regions and nations have adopted or strengthened existing legislation in order to provide tools to step up the fight against such attacks. Countries have been developing legislation and policies based on their own domestic needs, such as the European Union General Data Protection Regulation (GDPR), which requires user consent to collect data.

[9] Mimecast. Everything you need to know about SPF
[10] DKIM.org. DomainKeys Identified Mail (DKIM)
[11] DMARC. Domain-based Message Authentication, Reporting and Conformance
[12] RFC Editor. RFC 6480 - An Infrastructure to Support Secure Internet Routing. February, 2012.
[13] MANRS. Mutually Agreed Norms for Routing Security
[14] Messaging, Malware and Mobile Anti-Abuse Working Group (M^{3}AAWG). Why M^{3}AAWG?
[15] Internet Society. The Internet Society's Anti-Spam Toolkit
[16] GSMA. GSMA Security
[17] Spamhaus. Spamhaus ZEN + DBL + RPZ
[18] APWG. Unifying the global response to cybercrime through data exchange research and public awareness
[19] Anti-Spyware Coalition. Internet, Marketing y Actualidad

Another example is the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), which provides a set of standards that States parties in the Africa region are encouraged to incorporate into their domestic legislation. In Article 4.3, the Convention provides that "*State Parties shall prohibit direct marketing through any kind of indirect communication using, in any form, the particulars of an individual who has not given prior consent to receiving the said direct marketing through such means*". The Convention nevertheless authorizes direct marketing under certain conditions; for example, "*direct marketing by electronic mail shall be permissible where: (a) the particulars of the addressee have been obtained directly from him/her; (b) the recipient has given consent to be contacted by the marketing partners; (iii) the direct marketing concerns similar products or services provided by the same individual or corporate body*" (§ 4.4).

As both the European Union GDPR and the Malabo Convention are implemented, we will be able to evaluate and understand their full effect on reducing spam and malware.

1.3.3 Contributions related to the work to combat and mitigate the impact of spam and malware under Question 3/2

During the study period, some countries and ITU Sector Members provided additional examples of approaches to combat spam and malware:

- Some contributors described how they are collecting real-time information on cybersecurity threats in order to inform and build resilient cybersecurity strategies. In the complex world of information technology, real-time data are essential to protect information. Situational awareness and cyberthreat intelligence, when combined, help countries and public and private organizations identify threats as they emerge so that they can protect their resources more effectively. To better protect organizations from targeted attacks and persistent threats, it is therefore imperative to develop cyberresilient strategies based on security intelligence.[20]
- Some contributors are mapping cybercrime threats to understand the various effects of spam and malware on Internet users (e.g. phishing and lottery fraud) and businesses (e.g. unauthorized system access and DoS attacks). For example, in 2017 Côte d'Ivoire monitored threats and offences related to cybercrime, which were recorded by the Platform for Combating Cybercrime (PLCC), thereby providing useful, qualitative information to guide operational activities for improving education of consumers and businesses. Patterns of mobile money services fraud were identified, with 453 cases recorded, amounting to a loss of nearly USD 800 000. Mobile money services fraud is a well-crafted scam, in which, after transferring funds to or from a mobile money account using an Unstructured Supplementary Service Data (USSD) syntax, the victim receives a call from the fraudsters claiming that there was an issue with the transfer; if the victim falls for the scam, the fraudsters are able to remotely withdraw money from the victim's mobile money account using that same USSD syntax.[21]
- Some contributors described how they are creating open and transparent processes to identify and promote actions to be taken by relevant stakeholders with a view to significantly reducing the threats posed by automated and distributed attacks (e.g. botnets). With the arrival of new botnets, which can create enormous pressure on networks, using more than one terabit of data per second, traditional DDoS mitigation techniques based on the reservation of resources by network access providers are no longer effective. Mitigating threats from automated and distributed cyberattacks requires ongoing collaboration between the public and private sectors.[22]

[20] ITU-D SG2 Document 2/167 from Symantec Corporation (United States)
[21] ITU-D SG2 Document 2/174 from Côte d'Ivoire
[22] ITU-D SG2 Document SG2RGQ/153+Annexes from the United States

- Taking a few simple steps can help companies effectively protect themselves against the threat of ransomware attacks. In a recent ransomware advisory, the National Cyber Security Centre (NCSC) in the United Kingdom recommends a number of straightforward risk-mitigation techniques, such as:
  - keeping devices and networks up to date (e.g. through rapid updates and patches and regular scans);
  - preventing and detecting lateral movements in corporate networks;
  - using a virus scanner;
  - backing up all files.[23]
- A complete and detailed list of the recommendations can be found on the NCSC website.[24]
- Some contributors described how they are creating a flexible national cybersecurity framework that is adapted to changing needs. For example, the United Kingdom has launched the Active Cyber Defence programme, which focuses on taking positive technical steps to improve the online environment for all. This programme has delivered significant, measurable benefits for government networks. It has been implemented across public service networks in the United Kingdom in order to demonstrate the practical benefits and possible follow-up steps.[25]As part of continuing efforts to address such challenges, the United Kingdom provided an update on the programme a year after its launch.[26]
- Some contributors are taking steps to educate vulnerable communities (e.g. persons with disabilities) about their increased risk level. Spammers and hackers are using increasingly sophisticated techniques to determine whether potential hijacking targets have disabilities. In some cases, hijackers use a person's disability as a means of posing as that person from the hijacked e-mail account.[27]
- Some contributors are introducing reporting services for phishing e-mails. Crowdsourcing the collection of malicious e-mails, and taking action against the domains and other entities that they contain, is an effective tool for reducing cybercrime and fraud. For example, in the first four months of operation of the Suspicious Email Reporting Service, the United Kingdom's NCSC and the City of London Police removed more than 16 000 online threats reported by the public.[28]

[23] ITU-D SG2 Document SG2RGQ/155 from the United Kingdom

[24] National Cyber Security Centre (NCSC). Guidance: Mitigating malware and ransomware attacks

[25] ITU-D SG2 Document SG2RGQ/55 from the United Kingdom

[26] ITU-D SG2 Document SG2RGQ/175 from the United Kingdom

[27] ITU-D SG2 Document 2/71 from the Global Initiative for Inclusive Information and Communication Technologies (G3ict)

[28] ITU-D SG2 Document SG2RGQ/234 from the United Kingdom

Chapter 2 – Improving national cybersecurity postures: Awareness-raising and capacity-building opportunities

In recent years, ICTs have experienced rapid growth and innovation. Around the world, ICTs play an important role in enabling countries to expand their digital economies and support social prosperity. Furthermore, the COVID-19 pandemic has shown that people are increasingly dependent on ICTs in their day-to-day lives. Given this reality, it is paramount that countries continue to take important steps to improve and enhance their national cybersecurity postures in order to safeguard against cybersecurity risks and challenges.

This chapter examines key focus areas for improving national cybersecurity postures, including:

- establishing relevant national cybersecurity authorities;
- computer emergency response teams (CERTs)/computer security incident response teams (CSIRTs)/computer incident response teams (CIRTs);
- cybersecurity awareness-raising campaigns;
- cybersecurity risk management frameworks;
- public-private partnerships;
- other capacity-building initiatives.

During the study period, a number of entities provided contributions on these issues. Refer to **Annex 1** for a compendium of relevant, ongoing cybersecurity activities conducted by Member States, organizations, the private sector and civil society at national, regional and international levels. Refer to **Annex 2** for a list of related best practices and lessons learned submitted by some of these entities.

2.1 Establishing relevant national cybersecurity authorities

As new advances and innovations are made in ICT, so too are cybersecurity risks and challenges growing. Governments need to continuously evaluate and improve their national cybersecurity postures and strategies to address such challenges, including through the establishment of relevant national cybersecurity authorities. During the study period, Member States described their approaches to establishing such authorities. Different countries have taken different approaches depending on their domestic governance structures, rules, regulations and policies.

These cybersecurity authorities range in expertise and focus, but they generally serve the same key functions, including developing and coordinating regulatory policies; developing and implementing cybersecurity awareness campaigns; providing users (from large organizations to individuals and small businesses) with up-to-date information; and issuing statements and guidance on cybersecurity incidents. Given the broad cybersecurity landscape, it is critical that governments promote coordination and collaboration among the various authorities and entities and between the public and private sectors.

For example, in the United Kingdom, the National Cyber Security Centre works with other relevant government entities and leads efforts to measurably reduce the impact of ransomware attacks.[29] In the event of an attack, organizations are advised to contact the National Crime Agency, a cyber incident response-certified company or the Cyber Security Information Sharing Partnership. The NCSC led the United Kingdom's response to the WannaCry ransomware attack, in collaboration with the National Crime Agency. Over the course of each incident, the centre publishes statements and guidance for large organizations, as well as for home users and small businesses. The latest information is also announced via the centre's Twitter account (@NCSC).

Brazil has adopted its National Cybersecurity Strategy (E-Ciber), which was ratified by the Brazilian President and published in February 2020.[30] For this forward-looking strategy, which represents the federal government's cybersecurity vision for 2020-2023, Brazil undertook an exhaustive and comprehensive approach, involving the participation of numerous stakeholders, including from the government, the private sector and academia. With the ratification of E-Ciber, Brazil has supplemented a legal framework that was previously lacking. Under E-Ciber, Brazil has established 10 strategic actions, in respect of each of which it has outlined measures and initiatives. Examples of these strategic actions include:

- strengthening cybersecurity governance;
- establishing a centralized national cybersecurity governance model;
- improving the national legal framework for cybersecurity;
- expanding Brazil's international cooperation in cybersecurity.

In Benin, various government entities are involved in ICT management in the country.[31] The Information Systems and Services Agency (ASSI), formerly the Benin Agency for Information and Communication Technology (ABETIC), is the national entity charged with the operational implementation of programmes and the creation of strategies to develop secure digital information systems and services in the country. It is responsible for a number of key activities, including:

- implementing flagship projects for smart government and e-commerce;
- drafting, updating and operationally implementing master plans for national information systems;
- ensuring the technical, application and financial consistency of national information systems and services;
- ensuring the hosting and control of, and secured access to, critical information and data belonging to the State and critical infrastructure operators.

In Chad, the National Information Security and Electronic Certification Agency (ANSICE), established in February 2015, reports directly to the Office of the President.[32] The agency has been operational since January 2018 and has broad authority and competence, including over the security of information systems and networks throughout the country.

[29] ITU-D SG2 Document SG2RGQ/155 from the United Kingdom
[30] ITU-D SG2 Document SG2RGQ/216 from Brazil
[31] ITU-D SG2 Document 2/152 from Benin
[32] ITU-D SG2 Document 2/136 from Chad

The United Kingdom also shared an updated case study of its efforts to implement good security practices for consumer Internet of Things (IoT) devices, notably by:

- publishing the Code of Practice for Consumer IoT Security, which sets out 13 high-level principles (also available in German, Spanish, French, Japanese, Korean, Mandarin and Portuguese);
- carrying out a public consultation on proposed regulations and legislation;
- supporting ETSI EN 303 645,[33] the first globally applicable standard for IoT security, published by the European Telecommunications Standards Institute (ETSI). Many organizations have already based their products and certification schemes around the standard and its predecessor, ETSI TS 103 645;
- publishing a call for views on the United Kingdom's regulatory proposals to gather feedback from stakeholders on the proposed scope, obligations, security requirements and enforcement approach;
- commissioning the Department for Digital, Culture, Media and Sport and the NCSC to jointly develop guidance materials and online webinars for IoT manufacturers, which have been conducted repeatedly to account for global time zones;
- maintaining a landscape map that outlines existing standards, and supporting organizations in implementing good practices across the IoT.[34]

2.2 Computer emergency response teams (CERTs)/computer security incident response teams (CSIRTs)/computer incident response teams (CIRTs)

National incident response capabilities (in the form of CERTs/CSIRTs/CIRTs) are key tools for addressing operational cybersecurity challenges. Such capabilities facilitate the coordination of cybersecurity information and responses to security incidents. During the study period, the study group received key contributions from ITU Member States and Sector Members on the topic, many of whom shared the view that national CERTs/CSIRTs/CIRTs should serve as the main point of contact for cybersecurity issues and as coordinators for incident responses.

For example, the Bhutan Computer Incident Response Team (BtCIRT) was established in April 2016 to enhance cybersecurity in the country by facilitating the coordination of cybersecurity information and establishing national capabilities for the handling of computer security incidents.[35] BtCIRT is a unit under the Department of Information Technology and Telecom of the Ministry of Information and Communications. Under its mandate, BtCIRT acts as the national point of contact for cybersecurity issues and represents the country in international forums. Having one organization to coordinate all cybersecurity initiatives ensures that there is no duplication of efforts or developments. As most international forums and groups with a focus on cybersecurity communicate with CIRTs that have a national mandate, it is important for governments to appoint either a CIRT or a single designated organization to spearhead national cybersecurity initiatives and plans.

Although BtCIRT was established as the point of contact for cybersecurity-related issues in Bhutan, it has been a challenge for the team to gain the trust of stakeholders, mainly owing to its limited technical capabilities and to its being a relatively new team. Moreover, large corporations such as telecommunication operators and banks already have robust ICT infrastructure with

[33] ETSI. Standard ETSI EN 303 645. Cyber Security for Consumer Internet of Things: Baseline Requirements.
[34] ITU-D SG2 Document SG2RGQ/241 from the United Kingdom
[35] ITU-D SG2 Document SG2RGQ/79 from Bhutan

technical capabilities, making cooperation between the government and such large organizations challenging. Collaboration and cooperation among stakeholders, especially Internet service providers and CIRTs, is essential to provide concerted security solutions for Internet users. Bhutan turned to international organizations to help build BtCIRT's critical technical capacity.

Lastly, the Lithuanian company NRD Cyber Security proposed that, in addition to serving as the main point of contact for cybersecurity incidents and as response coordinators, national and sectoral CSIRTs should also act as facilitators or catalysts for the development of additional independent and distributed resilience to cyberthreat capabilities in the country.[36]

2.3 Awareness-raising campaigns

Various stakeholders around the world – from governments and commercial entities to community organizations and individual citizens – make extensive use of ICTs. However, many users are not fully aware of the cybersecurity risks involved in their use. For some developing countries, the biggest challenge is lack of user awareness. In the contributions received during the study period, there was a common understanding that cybersecurity awareness campaigns play an important role in addressing such challenges. The primary purpose of such campaigns is to encourage the adoption of secure behaviour online.

Countries and businesses are looking at creative ways to develop effective campaigns, including how to reach a broad set of users.

For example, Mexico shared its experience of developing and conducting an Internet user survey, which can be applied to guide different approaches to cybersecurity awareness-raising campaigns.[37]

Some countries have used surveys to identify citizens' key concerns and develop tailored awareness campaigns based on the results. Based on its experience, Mexico also identified the following lessons:

- install and update anti-virus protection;
- regularly change passwords and make sure passwords are strong (i.e. use a combination of numbers, letters and special characters);
- back up data regularly;
- only connect to secure public networks.

In another example, Bhutan's BtCIRT created awareness programmes tailored to meet the cybersecurity needs arising from the daily occupational and personal engagements of general end users around the country.[38] The participants were shown how attacks are executed through social engineering and phishing scams, how to communicate securely using e-mail and social media services and what the common threats and remediation responses were. Bhutan's awareness programmes have been highly successful in making users aware of security risks and have received positive feedback. While its current focus is on government officials, the BtCIRT team is looking to expand its efforts to children and other vulnerable users.

[36] ITU-D SG2 Document 2/172 from NRD Cyber Security (Lithuania)
[37] ITU-D SG2 Document 2/165 from Mexico
[38] ITU-D SG2 Document SG2RGQ/79 from Bhutan

Another creative example provided by Bhutan is the launch of an annual national website competition, organized by the Department of Information Technology and Telecom of the Ministry of Information and Communications.[39] All government websites are submitted to the competition, in which the best websites in the country are selected based on the following core criteria:

- usability and reliability;
- content and currency;
- security and uptime;
- appearance;
- interactive design.

Similarly, in November 2019, Brazil launched the #ConexãoSegura ("Safe Connection") cybersecurity awareness campaign through the Brazilian National Telecommunication Agency (Anatel).[40] The campaign provided consumer tips on protecting personal data and creating secure passwords. The campaign was motivated by complaints from consumers about attempted scams and by doubts about how to safeguard personal data. With the arrival of the COVID-19 pandemic and the surge in new scams, new posts about COVID-19 fraud and scams were created to help users. The posts were also shared through Anatel's social media networks, including Facebook, Twitter, Instagram and LinkedIn. Some of the main best practices from the campaign were to:

- use all security options provided by mobile apps, such as two-factor authentication;
- create strong and safe passwords by combining uppercase and lowercase letters, numbers and special characters;
- be wary of e-mails and messages with invoices attached and always contact the company's customer service department to verify whether a document is real;
- do not provide personal information or passwords when answering unknown calls.[41]

The United Kingdom provided a case study on cybersecurity resilience best practices for small and medium enterprises, in which it outlined efforts being deployed to improve the cyberresilience of organizations throughout the country.[42] One example of such efforts is the Cyber Aware communications campaign, which, beyond simply raising awareness, seeks to drive widespread adoption of basic cybersecurity behaviours. The campaign, aimed at the public and small businesses, was launched in April 2020, having been rapidly redeveloped to meet the changing cyberthreat landscape produced by the COVID-19 pandemic. The campaign promoted actionable mitigation measures, backed up with new guidance on how to work securely from home, move businesses online and use videoconferencing. Other tools include:

- Small Business Guide on Cyber Security;
- Small Business Guide on Response and Recovery, which provides a continuity plan to help SMEs prepare for cyberincidents and mitigate the potential impact;
- Exercise in a Box, a free online tool to help SMEs test their cyberresilience and complete micro-courses without requiring significant technical knowledge;

[39] ITU-D SG2 Document SG2RGQ/135 from Bhutan

[40] ITU-D SG2 Document SG2RGQ/215 from Brazil

[41] More information on Anatel's Safe Connection campaign can be found at the following website: https://www.anatel.gov.br/consumidor/component/content/article/109-manchetes/960-conexaoseguro-confira-dicas-para-proteger-dados-pessoais.

[42] ITU-D SG2 Document SG2RGQ/272 from the United Kingdom

- COVID-19 guidance to help businesses stay secure while adapting to the pandemic, covering topics such as home working and moving business operations online.

The United Kingdom also provided details of its government-backed certification scheme, Cyber Essentials, aimed at protecting businesses against commodity cyberattacks without requiring them to conform to multiple complex standards. Cyber Essentials was designed to be achievable by all organizations, even those without prior cybersecurity knowledge or a dedicated cyberteam.

2.4 Cybersecurity risk frameworks

Cybersecurity risk frameworks are critical for both governmental and non-governmental organizations. These are usually voluntary frameworks that provide guidelines and best practices for managing digital risks. During the study period, the study group received contributions from entities that provided different examples of, and approaches to, cybersecurity risk frameworks.

For example, the National Institute of Standards and Technology (NIST) in the United States recently updated its Framework for Improving Critical Infrastructure Cybersecurity.[43] This is a business-driven, proactive framework for voluntary cyberrisk management, designed for companies of all sizes that operate in diverse sectors of the economy. It provides a common starting point and language for assessing cyberrisk, and it is easily adaptable, enabling organizations – regardless of size, degree of cybersecurity risk or cybersecurity sophistication – to apply the principles and best practices of risk management in order to improve the security and resilience of critical infrastructure.

The framework was developed through successful public-private collaboration on cybersecurity risk management, following a year-long, voluntary development process that included input from more than 3 000 stakeholders from industrial sectors, academia, the government and international partners.

The framework is based on existing international standards, guidelines and industry best practices that have proven to be effective in protecting IT systems from cyberthreats, ensuring business confidentiality and protecting individual privacy and civil liberties, with a view to promoting the protection of critical infrastructure through risk management. In addition, the framework provides a structure for organizing practices, as well as tools to support the use and adoption of standards and practices. Because it references globally recognized cybersecurity standards, the framework also has the flexibility to serve as an international model for managing cyber risks.

Based on stakeholder feedback, the NIST made the following updates in version 1.1 of the framework:

- Declaring the applicability of the framework to "technology", which is composed of, as a minimum, information technology, operational technology, cyberphysical systems and IoT;
- Enhancing guidance for applying the framework to supply chain risk management;
- Summarizing the relevance and utility of measurements provided in the framework for organizational self-assessment;
- Providing additional information on self-assessing cybersecurity risk;

[43] ITU-D SG2 Document SG2RGQ/151 from the United States

- Taking greater account of authorization, authentication, identity-proofing and vulnerability disclosure requirements;
- Providing an administrative update to the informative references in order to reflect advances in standards and guidelines made by private and public organizations.

Additionally, in Bhutan, the Royal Monetary Authority (the central bank) has issued a directive promoting the implementation of a cybersecurity framework for financial institutions in order to enhance the resilience of the banking system to unknown and advanced cyberrisks.[44] The directive covers the following areas:

- All member banks must work towards compliance with the Payment Card Industry Data Security Standard, aimed at protecting cardholder data environments. Further, banks should implement ISO/IEC 27001:2013, on information security management systems, to complement their own cybersecurity measures.
- The directive outlines the need to establish a financial institution cyberresponse team to promote active collaboration and effective sharing of information pertaining to cybersecurity among banks and the Royal Monetary Authority. The team would actively monitor cyberthreats, plan for and coordinate counter-threat measures to prevent cybersecurity risks, and report any incidents to the relevant supervisor or the authorities as soon as possible. A cyberteam for the banks has been recently formed, with the Royal Monetary Authority taking the lead role.
- Member banks must also implement the relevant cybersecurity control framework and responsive actions as an immediate measure to ensure basic information security.

In a separate example, China has created an evaluation index to measure the national vision in planning, developing and implementing network security, using three levels of increasingly complex indicators.[45] The first level evaluates five indicators:

- *Policy*: National strategies, legislation, government agencies and international cooperation.
- *Industry*: Development of the network security industry in a market-driven environment, including the development environment, scale, capabilities and sustainability.
- *Technology*: Research and development and application level of national security in technology, including specific scientific research projects, investment, technical standards and personnel training.
- *Capability*: Level of network security protection and threat prevention, including risk perception, security protection, emergency response and active defence.
- *Resource*: Necessary resources to support capacity building, including network infrastructure resources, security awareness and international influence.

The index also includes 19 second-level and 53 third-level indicators. Under the scoring system for the index, each indicator is worth between 0 and 1 point, with 53 being the highest possible score. Calculations for each indicator are based on official public information published on national and international websites and by research institutions.

[44] ITU-D SG2 Document SG2RGQ/135 from Bhutan
[45] ITU-D SG2 Document 2/155 from China

2.5 Private-public partnerships

Government entities alone cannot improve national cybersecurity postures. Successful cybersecurity efforts and projects require strong partnerships between public and private-sector entities.

In the United States, the National Institute of Standards and Technology developed its Framework for Improving Critical Infrastructure Cybersecurity through a cooperative process as part of a public-private partnership.[46] As noted in more detail in section 2.4, the institute took care to ensure that all stakeholders were engaged in developing the update in order encourage maximum compliance with the framework. By engaging stakeholders and incorporating their feedback into version 1.1 of the framework, stakeholders were more likely to adhere to and implement the best practices, guidelines and standards that it included.

In the Republic of Korea, the Ministry of Science and ICT developed the 2019 National Cybersecurity Basic Plan for the private sector in consultation with relevant stakeholders, including academia, industry and public organizations.[47] The plan set out two objectives: ensuring a safe cyberspace and developing the information security industry. The main strategic projects to that end were aimed at expanding the cybersafety net, promoting the information security industry and strengthening information security infrastructure.

Given the rapidly changing ICT environment, the ministry intends to update the plan every year. The Public-Private Consultation Council of the Republic of Korea also meets twice a year to monitor the progress of the plan and identify areas for improvement.

As described in section 2.1, Brazil's national cybersecurity strategy, E-Ciber, is another example of the importance of public-private partnerships (PPPs) in developing comprehensive national cybersecurity strategies. PPPs are highlighted in the key strategic actions contained in E-Ciber, which include promoting a collaborative, participative, safe and trustworthy environment between the public and private sectors and civil society and expanding cybersecurity partnerships between the public and private sectors, academia and civil society.

In another strong example of PPPs, Brazil provided an overview of its experience of holding a national cyberdrill, known as the Cyber Guardian Exercise, in 2018, with a focus on national critical infrastructure.[48]In 2019, Brazil conducted a follow-on exercise, significantly expanding the range of participants to include representatives of the ministries of defence, justice and foreign affairs, the Institutional Security Office, military forces, federal government agencies such as Anatel, national CSIRTs, the Central Bank of Brazil, public and private banks, nuclear, electrical and telecommunication companies, academic researchers and invited regional and international observers.

Other examples of PPPs are CERTs/CSIRTs/CIRTs. Through such teams, public agencies and the private sector are able to work together to resolve cybersecurity events. Collaboration and trust are necessary to ensure that such teams remain effective, however.

[46] ITU-D SG2 Document SG2RGQ/151 from the United States
[47] ITU-D SG2 Document 2/168 from the Republic of Korea
[48] ITU-D SG2 Document SG2RGQ/214 from Brazil

2.6 Additional capacity-building measures/initiatives

2.6.1 Establishing cybersecurity education institutions

Acting on the realization that investment in cybersecurity training and education is necessary to combat growing cybersecurity challenges, many governments have established educational institutions to train the next generation of cybersecurity experts. Several contributions received from ITU Member States during the study period acknowledged the need for efforts in that area, including by strengthening relations between public stakeholders, universities and research centres.

For example, in 2015 Chad established the National Higher School of Information and Communication Technologies (ENASTIC), thereby clearly demonstrating the political will of the country's highest authorities to provide a framework for advanced ICT education (including providing degrees in cybersecurity, networks, telecommunications, etc.).[49]

Similarly, Senegal established the regionally focused National Cybersecurity School (ENC) to build capacities and raise awareness among decision-makers, senior defence staff and others involved in the digital ecosystem of the region.[50]

The key missions of the school include the provision of:

- training and awareness raising for State officials, Senegalese and foreign staff, students and people in the public and private cybersecurity sectors, in order to improve understanding of risks and threats;
- regular training to help dedicated CERT/CSIRT staff respond to the most sophisticated cyberattacks;
- periodic training for staff of State and subregional institutions to give them the capacity and knowledge to prepare for, guard against, respond to and recover from incidents.

2.6.2 Other capacity-building initiatives

Throughout the study period, the Telecommunication Development Bureau (BDT) Cybersecurity Focal Point provided regular updates on BDT's work programme, including its various capacity-building initiatives. The Bureau has been working jointly with different organizations and entities to provide capacity-building training for developing countries, including conducting cyberdrill exercises, assisting in CSIRT development and running training sessions. These efforts were also highlighted in Member State and Sector Member contributions. See **Annex 1** for additional information.

[49] ITU-D SG2 Document 2/136 from Chad
[50] ITU-D SG2 Document SG2RGQ/146 from Senegal

Chapter 3 – Child online protection

3.1 Overview

The modern-day Internet is no longer just a knowledge bank – a "huge, messy library" – as it was in the era of Web 1.0. It has become a communication platform used by all, including children. In fact, children account for one third of the global Internet population, according to the United Nations Children's Fund (UNICEF).[51]

The nature of the online threats facing children has evolved. While earlier threats were purely information-based – for example, access to information about drugs, pornography or extremist movements – current threats are also behavioural in nature, such as desocialization, gambling addiction, uncontrolled spending, virtual bullying, disclosure of personal data and dangerous acquaintances.

Over the past 10 years, the technological community has been actively inventing ways to protect children from sites that contain inappropriate information, but developers and parents now face a new challenge, namely how to properly introduce young users to the digital space and how to swiftly control and correct virtual behaviour. With the rapid development of Internet technology, the issue of child protection, on which there is global consensus, has naturally extended to cyberspace. Cyberspace safety is paramount when it comes to introducing children to digital devices and the Internet.

The Buenos Aires Declaration adopted by WTDC-17 states that "*opportunities provided by telecommunications/ICTs should be fully exploited with the aim of ensuring equitable access to telecommunications/ICTs and to innovations that foster sustainable socio-economic development, poverty alleviation, job creation, gender equality, child online protection, entrepreneurship and the promotion of digital inclusion and empowerment for all*".[52]

Resolution 179 (Rev. Dubai, 2018) of the ITU Plenipotentiary Conference and Resolution 67 (Rev. Buenos Aires, 2017) of WTDC set out the role to be played by ITU and ITU-D in child online protection.

As the COVID-19 pandemic has shown, the behaviour patterns of attackers and criminal networks are constantly evolving, and criminals are taking advantage of the fact that many children are spending much more time online than usual. In these circumstances, the publication of the 2020 Child Online Protection Guidelines, designed to protect the well-being, integrity and safety of children, is timely.[53]

The guidelines were co-authored by ITU and a working group of contributing authors from leading institutions active in the ICT sector and in child (online) protection and rights. They provide a comprehensive set of recommendations for all relevant stakeholders on how to contribute to the development of a safe and empowering online environment for children

[51] UNICEF. The State of the World's Children 2017. December, 2017.
[52] ITU. World Telecommunication Development Conference (Buenos Aires, 2017). Buenos Aires Declaration. October 2017.
[53] ITU. Guidelines on Child Online Protection

and young people. The aim of the guidelines is to raise awareness of the scope of child online protection and provide resources and tools to help children and their families develop digital skills and to help industry and government stakeholders develop corporate and national child online protection policies and strategies. Aimed at children, parents, educators, industries and policy-makers, the guidelines are designed to act as a blueprint that can be adapted to national or local customs and laws.

Under the ITU strategic plan set out in Resolution 71 (Rev. Dubai, 2018) of the ITU Plenipotentiary Conference, one of the objectives of ITU-D is to "*Foster the development and use of telecommunications/ICTs and applications to empower people and societies for sustainable development*" (§ D.4). In particular, ITU-D must provide "*Products and services on digital inclusion for girls and women and people with specific needs (elderly, youth, children and indigenous people, among others), such as awareness-raising on digital inclusion strategies, policies and practices, development of digital skills, toolkits and guidelines and forums of discussion to share practices and strategies,*" with the aim, among other things, of supporting child online protection (§ D.4-3).

The child online protection activities of ITU-D and its members are covered in item 2(d) of the terms of reference for Question 3/2:

d) *continue to gather national experiences from Member States relating to cybersecurity and child online protection and to identify and examine common themes within those experiences, using that information to provide input for guidelines to assist Member States in developing effective mechanisms for security in the digital environment.*

3.2 Best practices and common trends among ITU Member States

During the study cycle, the main child online protection activities undertaken by Member States focused on raising awareness, developing regulation and conducting thematic surveys.

Awareness raising

There are many aspects to protecting children in cyberspace, which requires not only tools and platforms but also appropriate data. Cultural programmes should be used to disseminate such resources throughout society.

For example, the Information Technology Organization of Iran developed the Kids and Internet (KOVA) project to protect children in cyberspace, which was selected as a champion project in the World Summit on the Information Society Prizes contest in 2018.

Given the rapid development in Internet infrastructure in recent years and the large number of young Internet users, including children, in 2016 the Iranian government launched a national programme to protect children on the Internet. As part of the programme, the Ministry of ICT launched the KOVA project to increase awareness among children and their parents regarding the risks of the Internet and how to protect children against them. The main goals of the project are to:

- identify the most important threats to children in cyberspace and provide solutions and legal protection services;
- create awareness among primary school students, high-school students, teachers and parents of the various threats posed to children at different ages;
- help children and teenagers to use social media and the Internet safely and securely;

- respond to questions posed by children, teenagers, educators and parents about security and safety challenges in cyberspace.

To achieve the project's goals, a diverse range of tools and methods (such as theatre, films and animations) were used to teach children about online safety. In the first phase of the project, more than 200 000 students across 900 schools received training, and the target for the second phase is to reach 4 000 schools.[54]

In Bhutan, the number of Internet users has increased by more than 28 per cent since 2016, as a result of increasing ease of access, affordability of connection and availability of cheaper smartphones. Most schoolchildren have access to a smartphone, which creates a higher risk of security incidents. Bhutan does not yet have a school curriculum on cybersecurity, as the rise in the use of the Internet and mobile devices is a recent trend. It is of the utmost importance, however, that governments embrace the changing times by including cybersecurity in school curricula. Private colleges in Bhutan have already begun to explore how to provide related degree programmes, particularly in cybersecurity. Schoolchildren need to be aware of cyberrisks, as they are more susceptible to attacks in the form of phishing and online games.[55]

In response to these considerations, after examining the online habits and behaviours of children, Bhutan is developing animation videos covering topics such as child trafficking, cyberbullying, privacy and online game security, which it will broadcast on national television. It is also developing posters and pamphlets incorporating cybersecurity best practices targeting students, which will be distributed to various schools in the country. Bhutan is also establishing a national-level task force, with representation from various relevant agencies, to frame relevant child online protection guidelines in the country.[56]

China holds an annual national network security publicity week to raise cybersecurity awareness and improve the online protection skills of the entire population through exhibitions, forums, competitions, lectures, thematic publicity days and other activities. For example, lectures on network security are given to share knowledge and skills in line with the needs of different groups, such as primary and secondary school students, the elderly and special groups (such as persons with disabilities), based on their IT skill level.[57]

The United States provides parents and teachers with information about practices for children and teens, including: What you post can last a lifetime! Be aware of what is being shared! Be careful about too much personal information! Post only about others what you would like them to post about you! Own your online presence by limiting who can see and share information! Know what data are being collected![58]

Regulation

Given the wide availability of information technology, governments are taking serious regulatory steps to ensure the safety of all citizens who have access to the Internet, in particular minors. While cybersecurity legislation varies slightly around the world, the roots of the problem remain the same.

[54] ITU-D SG2 Document 2/82 from the Iran University of Science and Technology (Islamic Republic of Iran)
[55] ITU-D SG2 Document SG2RGQ/79 from Bhutan
[56] ITU-D SG2 Document 2/385 from Bhutan
[57] ITU-D SG2 Document 2/286 from China
[58] ITU-D SG2 Document 2/400 from the United States

One of the main reasons for the emergence of such regulations is the particular vulnerability of children of preschool and primary school age on the Internet, who easily fall victim to Internet predators (persons who sexually harass minors via the Internet), humiliation and online grooming (in which a stranger gains a child's trust for his or her own purposes), and misuse of personal data.

Children have gradually become the group at highest risk of privacy disclosure and identity theft. The protection of children's personal information is therefore extremely urgent.

For example, China has issued a special regulation on cyberprotection for children's personal information, which governs the full lifecycle of collecting, storing, using, transferring and disclosing children's personal information.[59] The regulation provides for special protections, clear principles and cooperative governance with the aim of creating a beneficial online environment for children's healthy growth. The special protections include, among other things, deletion rights and the non-disclosure of children's personal information, while the principles cover legitimate necessity, informed consent, clear purpose, security and legal use. The regulation applies primarily to the protection of personal information pertaining to children under the age of 14.

In December 2010, the Russian Federation enacted a law on protecting children from information harmful to their health and development, which ensures the information security of minors and establishes the conditions and procedures for the dissemination of information among children.[60]

In addition, the Media Act of the Russian Federation forbids the dissemination in the media or via any information and communication network (such as the Internet) of information about any minor who is the victim of an illegal act (or omission), including:

- the surname, given name or patronymic;
- photographic or video imagery of the minor or his or her parents or other legal representatives;
- the birthdate of the minor;
- audio recordings of the minor's voice;
- the minor's place of residence or temporary address;
- the place where the minor studies or works;
- any other information that could be used to identify the minor directly or indirectly.[61]

Thematic surveys

ITU has provided technical assistance in the ongoing drafting process for Bhutan's national cybersecurity strategy.[62] During the process, a survey of 126 students (with an average age of 16) was carried out, in which multiple-choice questions were used to assess Internet usage, security incidents such as cyberbullying, and the prevalence of computer viruses or offences committed by students.

[59] ITU-D SG2 Document SG2RGQ/179 from China

[60] ITU-D SG2 Document 2/264 from the Russian Federation

[61] See Article 4 of Federal Act No. 2124, https://digital.gov.ru/ru/documents/6406/ [in Russian]. ITU-D SG2 Document 2/264 from the Russian Federation

[62] ITU-D SG2 Document SG2RGQ/135 from Bhutan

The survey revealed that students were using the Internet intensively. Almost all students who participated in the survey used the Internet, and more than 40 per cent used the Internet for more than two hours a day. Cybersecurity was a pressing topic for the students: while almost 40 per cent had experienced a malware infection, only around 10 per cent reported that they used anti-virus software.

With regard to cybersecurity education, school remained an important source of knowledge for the students. Almost 40 per cent of the students reported that they had learned about cybersecurity in school.

The students had also been exposed to cybercrime and other harmful activities. Aside from computer viruses, more than 10 per cent of the students surveyed had been victims of cyberbullying, while 25 per cent had been contacted by a stranger online. The questionnaire also contained a section on illegal or inappropriate acts, which revealed that around 35 per cent of the students had sent mean or harmful messages that could be considered as cyberbullying. Around the same number of students had tried, or succeeded in, breaking into a protected wireless network.

Because this initial survey was limited, Bhutan conducted another survey on child online safety and protection at the national level. The survey was part of the Digital Kids Asia Pacific (DKAP) project initiated by the United Nations Educational, Scientific and Cultural Organization (UNESCO Bangkok) with support from Korea Funds-in-Trust (KFIT). It engaged 2 381 students aged 12 to 17 from 45 schools across the country, asking 112 questions in order to ascertain the level of cybersecurity awareness, threats and preventive measures. The study found that the majority of students (81 per cent) have access to smartphones at home. Most students tend to spend on average one to two hours online daily. Further, 54 per cent of students lack the knowledge to segregate reliable information from unreliable information. Some 49 per cent of students fear someone misusing their personal information.

A few students (10 per cent) circumvent age-restricted applications by giving false information, bully others and log into other people's accounts. In addition, 85 per cent of students are willing to make new friends online and 68 per cent do not mind talking to people from different places or backgrounds. The survey raised safety concerns insofar as 51 per cent of students have met in person strangers whom they initially met online, and another 22.8 per cent are open to the idea of meeting strangers, with more females than males meeting strangers.[63]

In Côte d'Ivoire, the PLCC conducted a survey of 200 young people from three high schools in Abidjan in order to analyse children's online behaviour, identify risks and suggest effective security strategies to combat online abuse.[64]

In total, 83 per cent of respondents to the survey reported that they used the Internet. The primary reason why the remaining percentage of respondents did not use the Internet was because of the cost of smartphones and terminals. For children aged 15-18, television had been relegated to a secondary usage level, while 86.3 per cent had a social media account. This age group preferred to access the Internet through smartphones. Violent imagery and films were reported as the primary source of negative experiences online, followed by piracy and, lastly, insults and threats. To a lesser extent, respondents reported negative experiences with sexual connotations. Some respondents reported being blackmailed over sexually explicit videos.

[63] ITU-D SG2 Document 2/385 from Bhutan

[64] ITU-D SG2 Document 2/201 from Côte d'Ivoire

The potentially most harmful experiences for children, according to the survey, were:

- viruses, bugs, spam or hacking (24 per cent)
- sexual videos (7.5 per cent)
- violent images or videos (28.6 per cent)
- use of photos without prior agreement (7.5 per cent)
- insults, malice or threats (19.5 per cent)
- identity theft (6.7 per cent)
- contact with a stranger (4.51 per cent)
- scams (0.75 per cent)
- sextortion (0.75 per cent).

ITU support for Member States regarding child online protection

From 4 to 6 April 2018, in cooperation with the A. S. Popov Odessa National Academy of Telecommunications, ITU held a regional workshop on cybersecurity and child online protection for Europe and the Commonwealth of Independent States (CIS) in Odessa, Ukraine.[65] The final versions of all documents (including the agenda, reports, conclusions and recommendations, the list of participants, presentations and photographs) were published on the website of the academy[66] and on the ITU website.[67] The workshop participants, representing 14 Member States, concluded that the European and CIS regions needed to increase their cooperation in order to optimize the use of available resources and achieve practical results, including through the translation of training materials on cybersecurity and child online protection. The conclusions and recommendations developed by the workshop participants are presented in the outcome document.[68]

Child online protection is one of the key areas of focus of the ITU Regional Initiative for Europe on building confidence and security in the use of telecommunications/ICTs. In response to members' requests for roadmaps for child online protection initiatives, ITU conducted a survey among national governments covered by the regional initiative, addressing a broad range of issues related to contemporary policy and practice across all technology platforms used by children and young people in the digital space. The survey was first conducted among all Member States in 2009, and a revised version was conducted in 2016 among Central Eastern European, Baltic and Balkan Member States.

Drawing on the survey responses, in 2017 BDT issued a regional review of national activities on child online protection in Europe, which indicated where participating countries stood in terms of policy development, adoption, implementation and monitoring in the area of child online protection.[69] It also provided examples of current practice in Albania, Bosnia and Herzegovina, Bulgaria, Cyprus, Croatia, Estonia, Finland, Greece, Hungary, Latvia, Liechtenstein, Lithuania, North Macedonia, Monaco, Montenegro, Poland, Slovakia, the Czech Republic, Romania, Serbia, Slovenia and Turkey.

[65] ITU-D SG2 Document 2/75 from the A.S. Popov Odessa National Academy of Telecommunications (Ukraine)

[66] A.S. Popov Odessa National Academy of Telecommunications. ITU Regional Workshop for Europe and CIS - Cybersecurity and Child Online Protection, Odessa, Ukraine, 4-6 April 2018.

[67] ITU. ITU Regional Workshop for Europe and CIS on Cybersecurity and Child Online Protection, Odessa, Ukraine, 4-6 April 2018.

[68] ITU. Conclusions and recommendations. ITU Regional Workshop for Europe and CIS on Cybersecurity and Child Online Protection, Odessa, Ukraine, 4-6 April 2018.

[69] ITU-D. Regional review of national activities on child online protection in Europe, 2017.

The ITU Council Working Group on child online protection (CWG-COP) conducts its work in line with Resolution 1306 of the ITU Council (2009), in addition to Resolution 179 (Rev. Dubai, 2018), in which the Plenipotentiary Conference resolved that ITU should continue the Child Online Protection initiative as a platform to raise awareness of child online safety issues; continue providing assistance and support to the Member States, especially developing countries, in developing and implementing roadmaps for the initiative; and continue to coordinate the initiative, in cooperation with relevant stakeholders.[70]

Information on the 15th, 16th and 17th meetings of CWG-COP, held on 26 September 2019, 4 February 2020 and 26 January 2021, respectively, in Geneva and remotely, was provided for the consideration of Question 3/2.[71, 72]

At the meetings, the following documents were presented:

- An update on the ITU Child Online Protection Guidelines[73]
- A presentation on the outcomes of the Youth Online Consultation[74]
- A presentation on ITU's work and activities in child online protection[75]
- A presentation on the Child Online Protection Guidelines review process 2019-2020.[76]
- A presentation on the ITU Child Online Protection Initiative and implementation of the 2020 COP Guidelines.[77]

One of the main outcomes of the meetings was the recognition of the need to provide guidance on how to improve the number of responses from young people and increase the involvement and participation of stakeholders in CWG-COP, given the importance of evaluating programme effectiveness.

In 2020, ITU held a series of thematic forums[78] to share experiences of child online protection among various stakeholders and to publicize the Child Online Protection Guidelines and facilitate their promotion, adaptation and contextualization at national and regional levels:

- Africa: 30 October 2020[79]
- Americas: 19 October 2020[80]
- Arab States: 23 November 2020[81]
- Asia and the Pacific: 3 November 2020[82]

[70] ITU. Plenipotentiary Conference. Resolution 179 (Rev. Dubai, 2018), on ITU's role in child online protection.
[71] ITU-D SG2 Document SG2RGQ/242 from the Council Working Group on Child Online Protection (CWG-COP)
[72] Contributions from members and outside experts can be found at the following links: 15th meeting, 16th meeting, 17th meeting
[73] ITU. CWG-COP. Document CWG-COP-14/2: Update on the ITU Child Online Protection (COP) Initiative.
[74] ITU. CWG-COP. Document CWG-COP-15/INF/3: Youth Online Consultation.
[75] ITU. CWG-COP. Document CWG-COP-16/5: ITU's work and activities in child online protection.
[76] ITU. CWG-COP. Document CWG-COP-16/4: ITU Child Online Protection: COP Guidelines Review Process 2019-2020.
[77] ITU. CWG-COP. Document CWG-COP-17/2(Rev.1): ITU COP 2020, Child online protection and empowerment.
[78] ITU. Regional launches: COP 2020 Guidelines
[79] ITU-D. Regional launch of the revised COP Guidelines for Africa. 30 October 2020.
[80] ITU-D. COP Guidelines for the Americas. 19 October 2020.
[81] ITU-D. Online Regional Dialogue on the 2020 ITU COP Guidelines and opportunities for implementation in the Arab region. 23 November 2020.
[82] ITU-D. ITU Regional Development Forum for Asia and the Pacific (RDF ASP). Post-Forum Session on Cybersafety – Launching the 2020 Child Online Protection Guidelines for Asia and the Pacific. 3 November 2020.

- Commonwealth of Independent States: 27 October 2020[83]
- Europe: 26-27 November 2020[84]

3.3 Lessons learned, future steps, actions and conclusions

The need for child online protection has become especially acute during the COVID-19 pandemic.

A number of lessons can be drawn from Member States' activities on issues related to child online protection, such as that:

- every country should acknowledge its responsibility to ensure that the Internet and its associated technologies are safe for children and young people;
- countries are increasingly integrating awareness of online risks into a broader child protection and parenting agenda;
- while the idea is taking hold that the Internet can also be a positive factor in promoting citizenship and learning, in many instances a shortage of resources and locally available expertise appears to be acting as a brake on development;
- while the legislative frameworks in many countries are broadly in line with international and regional legal instruments, it is extremely important for every country to ensure that its legal measures and legislative framework stay in step with technological developments and changes in behaviour;
- national focal points are a key element in effective online protection, and all countries should have a well-resourced national focal point that is involved in regional and international initiatives.[85]

There are also several areas in which Member States could further facilitate child online protection activities, such as by:

- raising awareness and providing digital literacy training both for professional cybersecurity specialists and for children, parents and teachers;
- developing laws and regulations to protect children online;
- carrying out representative surveys to better tailor existing policies, initiatives and actions related to child online protection.

Non-profit associations and community organizations may wish to take steps to raise awareness and develop skills among children to help them make better use of the Internet in a safe environment, such as by:

- de-dramatizing prevention, which may otherwise contribute to the fear culture among parents regarding their children's use of the Internet, thus avoiding an approach liable to increase anxiety among parents who are already worried about a technology that they do not understand well, thereby sabotaging the extraordinary learning tool that is the Internet;
- encouraging educational programmes to develop best practices in content management, and raising children's awareness of how to use the Internet responsibly;
- creating an Internet portal to provide children, adolescents, parents and teachers with an educational base;

[83] ITU-D. ITU-UNESCO IITE Forum on Child Online Protection for the CIS region. 27 October 2020.
[84] ITU-D. ITU Forum for Europe on Child Online Protection. 26-27 November 2020.
[85] ITU-D SG2 Document SG2RGQ/47 from the BDT Focal Point for Question 3/2

- involving all stakeholders in community awareness activities, including government agencies, the private Internet sector, non-governmental organizations, community groups and the general public.[86]

Overall, it may be concluded that:

- the role played by international cooperation and State support in ensuring cybersecurity and child online protection is key;
- national policy tools should be used to elaborate cybersecurity strategies in developing countries;
- public-private partnerships are important for increasing the effectiveness of organizational and technical tools for cybersecurity;
- the development of new strategic and regulatory mechanisms for child online protection, and the evaluation of existing mechanisms, has reached a peak;
- educational institutions and private companies should be involved in implementing projects to create organizational and technical tools for child online protection, including within the framework of the ITU regional initiatives;
- educational programmes and tools for child online protection that take into account the needs of children with disabilities must be developed;
- Member States should review their Global Cybersecurity Index (GCI) commitments and initiate further action;
- educational institutions, private-sector entities and non-governmental organizations should be engaged in the activities of ITU-D, including the work of the ITU study groups and the centres of excellence that provide cybersecurity training courses.

If more effective solutions are to be developed, it is crucial that information be shared among all stakeholders about the tools available in the field of cybersecurity and child online protection, given the growing importance of child online protection around the globe and the need for collaborative efforts in this area, particularly within ITU-D activities.[87]

[86] ITU-D SG2 Document 2/201 from Côte d'Ivoire

[87] ITU-D SG2 Document 2/75 from the A.S. Popov Odessa National Academy of Telecommunications (Ukraine)

Chapter 4 – Cybersecurity challenges for persons with disabilities

4.1 Introduction

For cyberattackers, no one is considered off limits. Persons with disabilities should not be allowed to face higher cyberrisks owing simply to a lack of information or awareness.

During the 2014-2017 study period, ITU-D Study Group 2 conducted a cybersecurity awareness survey, the results of which were published in the final report.[88] The findings showed that the elderly and persons with disabilities were the two groups least targeted by cybersecurity awareness campaigns. In addition, 69 per cent of Member States that took part in the survey did not include persons with disabilities among their target groups for cybersecurity awareness-raising.

The results clearly demonstrate that further work is required in this area. To raise awareness about specific cybersecurity needs among persons with disabilities and other stakeholders, including governments and private organizations, Question 3/2 has continued to examine specific security considerations and cybervulnerabilities based on use cases. The use cases, lessons learned and other useful information are reported in this chapter.

4.2 Use cases

4.2.1 Spammers and phishers who target persons with disabilities

Overview

Spammers and e-mail hijackers are becoming more sophisticated, having developed the ability to identify whether a potential target has a disability and to use that disability to pose as the target. Persons with disabilities also face challenges in gaining help from the security and fraud departments of their e-mail providers.

Persons with disabilities are being targeted by spammers and hijackers, who pose as the target by using the person's disability as an identifier. In one case, the e-mail account of a deaf person who used sign language was hijacked. In this instance, the victim had a Gmail account, but the account could have belonged to any e-mail account provider. Unfortunately, the Gmail helpdesk provided little support. Once the victim had clicked on the phishing link and his account had been hijacked, the spammer was able to gain access to the victim's address book and, possibly, to other files on the victim's computer.

[88] ITU. Final Report on ITU-D Study Group 2 Question 3/2 for the study period 2014-2017. Securing information and communication networks: Best practices for developing a culture of cybersecurity. ITU, 2017.

The helpdesk told the victim that the only solution was to change his e-mail provider and e-mail address. While the disability in this example was deafness, it is not inconceivable that any disability could be used in this form of identity theft.

It is important that e-mail users, including users with disabilities, understand the importance of verifying all links sent to them, even from friends, before clicking on the link. E-mail provider helpdesks also need to take an active interest in this form of abuse, especially when vulnerable communities are being targeted. In this case, the victim contacted the helpdesk telephone number via a friend or a telephone relay service for the deaf; service providers should treat such calls more earnestly or should provide a special telephone number populated by human beings which deaf users can contact directly using a teletypewriter. Even better, service providers should hire helpdesk staff who are fluent in sign language. In the United States, Amazon has taken steps to provide such a service, for example.

E-mail examples

Below are two examples of the type of e-mail that the spammer in the above example sent to the victim's contact list. In response, the victim changed his e-mail provider after informing his contacts that he had been hacked.

Example 1: The spammer is posing as the person with a disability.

From: Person with disability personwithdisability@gmail.com
Sent: 23 March 2018 13:00
Subject: WOW !! Country X INCREASES DEAF MONTHLY ALLOWANCE BY 70 per cent

Wow! Country X gave a thought to all Deaf and Hard of hearing people and Country X Leader has decided to increase SSA, SSI and SSDI by 70 per cent and this is Good News for all the Deaf and Hard of Hearing in Country X

To read more and to know by how much your SSA, SSI and SSDI was increased,

click here http://noisecancel.net/js/gggg/G/G/us/index.php

[Note: The original phishing link has been changed.]

And Sign on with your e-mail and make sure everything is correct

DeafNews

Example 2: From the victim notifying his contacts that he has been hacked.

Hi to all!

Like I said earlier, as a result of my being lured to view a video in ASL three weeks ago, my OLD Gmail got hacked!

[Note: ASL stands for American Sign Language.]

The hacker continues to send FAKE e-mails using my Gmail account. What is scary is that the contents appear to be realistic and related to my deaf-related activities.

After hours of going through the Google robotic network, I found a phone number, (855) 836-3987, to reach a human.

Guess what? Instead of trying to assist me, they said "too bad".

Is your Gmail safe?

In the meantime, delete ANY e-mails.

<from personwithdisability@gmail.com>

Apologetically

Person with disability

Lessons learned and suggested best practices

- The disability community should be educated about known spamming and malware issues.
- Service providers should provide trained staff to handle customer inquiries from the disability community.
- E-mail users should not click on any web addresses unless the source has been verified.
- Victims of e-mail hijacking should:
  - inform their e-mail service provider;
  - forward the suspicious e-mail to the e-mail provider's fraud section;
  - request that the hijacked e-mail address be blocked;
  - change e-mail address;
  - inform all contacts that the e-mail address has been hacked and provide them with the new address.

4.2.2 Cyberrisks associated with IoT-enabled assistive technologies

Background

According to the World Health Organization (WHO), more than 2 billion individuals have a disability, representing 37.5 per cent of the global population.[89] As the United Nations Department of Economic and Social Affairs notes, countries do not share a uniform definition of "persons with disabilities" and have consequently adopted different classifications and thresholds.[90] According to the internationally accepted WHO definition, a person with disabilities is anyone who has a problem in body function or structure, an activity limitation, or difficulty in executing a task or action.[91]

As this definition suggests, there are many types of disabilities. Each disability represents a barrier that affects people's lives. However, technology is playing an important role in breaking down these barriers and helping persons with disabilities enjoy better living conditions.

Nowadays, technology is widespread, influencing both individuals' daily lives and society as a whole. Over the past decade, IoT has demonstrated the potential to change the lives of persons with disabilities for the better.[92] IoT-enabled assistive technology is therefore increasingly being used to overcome the limits arising from disabilities.[93]

The Convention on the Rights of Persons with Disabilities identifies ICTs as an essential element in assisting persons with disabilities. In particular, Article 9, on accessibility, underlines the role of ICTs in promoting the independence and full participation of persons with disabilities across different domains, and mandates State Parties to make conscious joint efforts to advance access to ICTs.[94]

Both ICTs and IoT increase safety, mobility and independence; from Internet-connected prosthetics to smart shoes that vibrate to guide the wearer, many IoT devices and services are designed to improve living conditions and reduce the reliance of persons with disabilities on others.[95] For instance, individuals who are blind or who have a visual impairment can use technology to help them navigate their surroundings and access written information. Furthermore, smart home technologies allow individuals to control appliances and other items in their homes that may be difficult to reach, such as lights, door locks and security systems.

Technology: A double-edged sword

While providing many benefits, IoT-enabled assistive technologies also exponentially increase users' exposure to cyberrisks. Given the growing reliance on assistive technologies, any disruption to or alteration in such technologies could lead to increased vulnerability.

[89] WHO. World Report on Disability 2011. WHO, 2011.
[90] United Nations Department of Economic and Social Affairs (UNDESA). Disability and Development Report: Realizing the Sustainable Development Goals by, for and with persons with disabilities. United Nations, New York, 2018.
[91] WHO. Op. cit., Chapter 1.
[92] Future of Privacy Forum. The Internet of Things (IoT) and People with Disabilities: Exploring the Benefits, Challenges, and Privacy Tensions. January 2019.
[93] WHO. Health topics. Assistive technology
[94] UNDESA. Convention on the Rights of Persons with Disabilities (CPRD). Article 9 – Accessibility.
[95] Future of Privacy Forum. Op. cit.

IoT devices and services are often characterized by less than optimal security levels. For instance, they might not use proper encryption for transmitting data, which can lead to the improper disclosure of data and data leakage. For persons with disabilities in particular, personal data may be sensitive in nature, as they could reveal details of the individual's medical conditions.

Given the importance of assistive technologies for persons with disabilities, the negative impact of cyberrisks can be catastrophic. For example, some persons with physical disabilities rely on biomechanical prostheses to restore full or partial movement. Such prostheses use specific sensors to read and analyse muscle contraction parameters in order to reproduce movements through the devices (e.g. moving the fingers of prosthetic arm). Prostheses routinely send data to the cloud to inform their computational analysis and improve their effectiveness. This connectivity makes such devices susceptible to attacks aimed at gaining access to, manipulating or deleting data held in the cloud or gaining access to users' personal data. Moreover, attackers could take control of prostheses remotely. If the prosthesis is connected to a brain implant, the consequences could be even worse.[96]

As another example, some persons with hearing impairments rely on cochlear implants, which are more invasive than a standard hearing aid. This technology relies on three basic components, namely a microphone, a speech processor and an implanted receiver-stimulator. Some modern cochlear implants are accompanied by remote-control devices that allow users to control the implant's settings via a mobile application. At a basic level, attackers could seek to turn off the implant, rendering the victim deaf. More sophisticated attacks could prevent the speech processor from receiving input from the microphone or alter the receiver to transmit sounds generated by the attacker. These more sophisticated attacks could be harder to detect, especially when cochlear implant users have no other way of verifying what they are hearing.

In addition to attacks tailored to assistive technologies, attackers can also target technologies commonly used by persons with disabilities. For instance, visually impaired persons would lose all reliable means of navigation if the GPS tools that they used were faulty or were deliberately compromised by attackers. In GPS spoofing attacks, a radio transmitter located near the target is used to interfere with a legitimate GPS signal.[97] The attacker can then transmit inaccurate coordinates or interrupt the transmission of data, potentially leading to physical harm and other significant consequences.

While these are just few examples of possible cyberattacks targeting digital assistive technologies, they highlight the relevance of cybersecurity in guaranteeing the safety of persons with disabilities who rely on such technologies.

Next steps for consideration

The Internet and IoT can facilitate the social, economic and civil participation of persons with disabilities. While the potential of such technologies is evident, constant efforts are required to align societal, legislative, personal and infrastructural factors within the IoT ecosystem in a way that prioritizes the security of IoT devices. There are concrete actions that governments could take to improve the security and, consequently, reliability of assistive technologies.

[96] Vladimir Dashchenko. How to Attack and Defend a Prosthetic Arm. Securelist (Kaspersky), 26 February 2019.
[97] Maria Korolov. What is GPS spoofing? And how you can defend against it. *CSO website*, International Data Group (IDG), 7 May 2019.

Governments could take steps to improve legislation and policy on IoT accessibility and security and develop mechanisms to promote and enforce their implementation. These frameworks need to start with an assessment of the needs of persons with disabilities and should outline clear roles and responsibilities. Since the topic is likely to involve representatives from a variety of governmental areas (e.g. technology and telecommunications, welfare and medicine), collaboration is key and should be promoted in every initiative.

Specific initiatives could be introduced. For instance, governments could develop cybersecurity certification schemes for assistive technologies, which could include periodic security checks and tests and an obligation to perform regular system updates to adapt to technological evolutions. Governments could also support manufacturers by offering incentives, promoting public-private partnerships and offering start-up funding and research and development grants.

Likewise, there is a need to promote a security culture that responds to the risks that these technologies entail. Governments should work with the private sector to conduct cyberawareness campaigns among the population.

In conclusion, while IoT-enabled assistive technology is a key element in supporting persons with disabilities, it can also pose a number of risks that, if not properly addressed, could have severe consequences. Assistive technologies should therefore meet the highest security standards and should respond to technological developments.

Lessons learned and suggested best practices

As described above, cybersecurity measures should be implemented for persons with disabilities, especially those with hearing difficulties, such as telecommunication relay services and remote captioning, in order to enhance the accessibility of information and communication services.

4.2.3 Consideration of security issues for ICT accessibility services

Introduction

ICT accessibility services, such as telecommunication relay services and remote captioning, enable persons with disabilities to communicate and access information. Such services naturally require security measures to be taken to protect the safety and privacy of persons with disabilities and to mitigate the cybervulnerability of these and other groups with specific needs, such as children and older persons.

Security aspects of remote captioning

Remote captioning is a service in which words spoken at a meeting or conference are transcribed at a different location from that in which the meeting took place.[98] ICT services, such as telephones, cellphones or computer microphones, are used to send the voice of the speaker to the captioner, who transcribes the voice to text. The transcribed text is then transmitted in real time back to the location of the meeting, where the text can be read. Remotely captioned text is often displayed on a public screen or monitor in the meeting room or on a personal display. Not only are remote captioning services essential to allow persons who are deaf or hard of

[98] ITU Telecommunication Standardization Sector (ITU-T). Technical Paper FSTP-ACC-RCS - Overview of remote captioning services, 17 October 2019

hearing to participate in meetings, but they are also useful for individuals whose first language is different from that used in the meeting or for situations where speakers with different voices and accents are participating in various groups (e.g. at work, in a classroom or in community halls). The person who provides transcriptions for a remote captioning service, called a "captioner", must be qualified as a verbatim reporter. A captioner is often also known as a "speech-to-text-reporter".

Remote captioning services are required under various national or local codes of practice. The provider must take all reasonable precautionary measures to secure the privacy of the meeting, as it may contain confidential information.

Types of confidential information

The following is a non-exhaustive list of potentially confidential information:

- sensitive information discussed in meetings and/or conferences
- patients' medical information
- legal information regarding individuals
- counselling sessions
- information on compliance with data-protection regulations.

Remote captioning service providers must follow the applicable privacy and data-protection laws and regulations, such as those laid down by the European Union.[99]

Encryption of captioned text

The text streamed to a display or personal terminal should be password protected. The remote captioning service provider is responsible for the security of the script and is required to follow relevant data-protection requirements. It is recommended that the text and, if applicable, the URL of the text source should be encrypted using the Secure Sockets Layer protocol or other relevant technology.

Encryption of audio

Original audio data from the event must be securely protected.

Security consideration for telecommunication relay services

Functional equivalency

Functional equivalency is defined as "*the capability to which persons with different range of abilities (in particular persons with disabilities and persons with specific needs) are able to use a communication service or system with a level of offered functions and convenience-of-use that is similar to those offered to the wider group of users in a population [...] These include both technical and economic considerations and that no financial discrimination is imposed on relay service users*".[100]

Functional equivalency includes the security obligations applicable to communication service providers in any given jurisdiction. Functional equivalency implies that the users of relay services

[99] European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal

[100] ITU-T. Recommendation ITU-T F.930. Multimedia telecommunication relay services

must be on an equal footing with other users in the community, especially with regard to the types of calls permitted by relay services, which may have implications for security.

Security requirements for functional equivalency

To achieve functional equivalency, it is essential to ensure the confidentiality, privacy and security of telephone relay services, the technologies used by such services and the human communication assistants who work for them.

Requirements for telephone relay services regarding confidentiality and call security, including encryption, should be in harmony with those applicable to general telecommunication services in the country or region in question.

Cybervulnerability considerations for persons with specific needs

Ensuring secure Internet use is especially important for persons with disabilities and for groups with specific needs, such as the elderly and children. Reducing the cybervulnerability of these groups is an urgent and important issue, requiring guidelines to be drawn up and observed.

4.3 Useful information

ITU-D Study Group 1 Question 7/1 addresses "Access to telecommunication/ICT services by persons with disabilities and other persons with specific needs" and discusses various topics in this area.[101]

The Future of Privacy Forum publishes a report entitled "The Internet of Things (IoT) and People with Disabilities: Exploring the Benefits, Challenges, and Privacy Tensions".[102]

Further information can be found from those sources.

[101] ITU-D Study Group 1. Question 7/1.

[102] Future of Privacy Forum. Op. cit.

Chapter 5 – The state of cybersecurity challenges, including those facing emerging technologies such as IoT and cloud computing

5.1 Introduction

The exponential growth in technological capabilities has led to an increasingly digitalized, connected and interconnected world. According to the World Economic Forum, a period known as "Globalization 4.0" has already begun, in which digital assets and services constitute the backbone of the economy and exports.[103]

Innovation is transforming the technology landscape to meet new business and practical needs. IoT devices, together with 5G technology, are becoming increasingly pervasive, with an estimated 41.6 billion connected devices around the world by 2025.[104] Cloud solutions have become critical to operations, with 94 per cent of businesses worldwide relying on them.[105] Given the growing availability and accuracy of data, artificial intelligence is also continuing to find broader applications.

The emergence of new technologies brings an increased need for cybersecurity, however. Digital innovation has introduced more products, as well as significant complexity, thereby increasing the likelihood of vulnerabilities and weaknesses that could be exploited.

Cyberthreats are constantly increasing. In 2018, there were 80 000 cyberattacks per day, amounting to more than 30 million attacks per year.[106] In 2019, more than 90 billion attempts to compromise sensitive information were registered on a daily basis.[107] Cyberthreats are also increasingly sophisticated, threatening the entirety of the digitally enabled world and economy, including cyberphysical systems in homes, smart cities, vehicles, production systems and critical infrastructure. Experts have demonstrated that it is even possible to hack medical devices implanted in human bodies, such as pacemakers and insulin pumps.[108]

Such an increase in attacks is also due to the proliferation, via the dark web, of hacking as a service, often for an affordable price. Cybercrime is increasingly being commercialized and has developed into a large sector, in which hackers sell a wide variety of malicious tools and services, ranging from low-level password theft to highly sophisticated exploit kits and attack technologies,

[103] Klaus Schwab. Globalization 4.0 - What Does It Mean? *World Economic Forum*, 5 November 2018.

[104] Business Wire. The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast, 18 June 2019.

[105] Kim Weins. Cloud Computing Trends: 2019 State of the Cloud Report. *Flexera Blog*, 21 May 2020.

[106] PurpleSec. 2019 Cyber Security Statistics Trends & Data: The Ultimate List of Cyber Security Stats. *PurpleSec* (blog), accessed 27 April 2020.

[107] Check Point. Prepare for a New Cyber Cold War in 2020, Warns Check Point. Press release, 24 October 2019.

[108] Lily Hay Newman. These Hackers Made an App That Kills to Prove a Point. *Wired*, 16 July 2019; Dan Goodin. Insulin Pump hack delivers fatal dosage over the air. *The Register*, 27 October 2011.

such as DDoS, malware, ransomware and spyware.[109] Moreover, emerging technologies, which are often used to improve cyberdefence solutions, can be used maliciously to enhance the efficiency and reach of hacking tools.[110] Artificial intelligence, automated botnets, IoT and cloud solutions are increasingly employed in large-scale cyberattacks, and the combination of new hacking techniques – such as automated phishing tools – with emerging technologies has broadened the cyberrisk landscape.

A major challenge for cybersecurity is the general shortage of professional skills and the lack of employee awareness. As cyberthreats grow in sophistication, organizations are struggling to recruit skilled cybersecurity experts capable of protecting their systems.[111] In 2017, 82 per cent of employers reported that their personnel had inadequate cybersecurity skills. By 2021, 4 million professional cybersecurity positions will be unfilled.[112] Furthermore, general personnel demonstrate little awareness of cyberthreats. The human factor plays a key role in cybersecurity and has proved to be a significant liability. In 2018, one study found that 99 per cent of digital incidents were unwittingly initiated by employees who fell victim to social engineering, while only 1 per cent stemmed exclusively from technological failures or exploitations.[113]

Cybersecurity is a dynamic domain, and organizations must continuously revisit their cybersecurity posture to defend against emerging threats. In order to create a more secure environment, it is important to engage stakeholders in a conversation around cybersecurity and privacy risk management; verify, supplement and refine existing cybersecurity and privacy risk management processes; and identify key cybersecurity and privacy considerations that may be specific to certain technology solutions and environments. This chapter discusses many cybersecurity threats linked to emerging technologies, including IoT, the cloud, 5G, AI and the fourth industrial revolution (known as "Industry 4.0"). It also outlines the current trends, challenges and possible solutions to address threats that could offset the gains made through digital innovation.

5.2 Cybersecurity threats, actors and motivations

The aim of cyberthreats is to undermine the three traditional objectives of cybersecurity, namely confidentiality, integrity and availability. Confidentiality protects information against all but those authorized to access it. Integrity ensures the accuracy and reliability of information and prevents unauthorized data alterations. Availability refers to the capacity to access data and information when needed.

The cyberthreat landscape is a heterogeneous environment, populated by various actors that are pursuing different goals and that have different capabilities. Broadly, malicious actors can be classified as follows:

- **Insiders**: According to recent reports, around 40 per cent of incidents are perpetrated by internal personnel, often disgruntled employees seeking revenge against their

[109] Armor. The Dark Market Report: The New Economy, 28 September 2020.

[110] Deloitte. Protecting against the changing cybersecurity risk landscape. Future of risk in the digital era. Deloitte & Touche LLC, 2019.

[111] William Crumpler and James Lewis. The Cybersecurity Workforce Gap. Center for Strategic and International Studies, 29 January 2019.

[112] Rob Saunders. 134 Cybersecurity Statistics and Trends for 2021. Varonis. Updated 16 March 2021.

[113] Proofpoint. Proofpoint's Annual Human Factor Report Details Top Cybercriminal Trends: More than 99 Percent of Cyberattacks Need Humans to Click, 9 September 2019.

employers.[114] Insiders can be particularly dangerous as they have direct access to data, information and digital assets.

- **Hacktivists**: These are individuals motivated by political and social causes. They typically steal and disseminate sensitive information with the aim of embarrassing political leaders or celebrities, and they disclose proprietary and classified data in the name of free speech. They also often deface websites and conduct DDoS attacks against particular services or websites.[115]
- **Cybercriminals**: These are criminals motivated by financial gain. They target information pertaining to individuals, companies and organizations with the aim of monetizing it. They typically blackmail targets, exfiltrate and sell data and intellectual property on the black market and execute ransomware attacks. As discussed above, cybercrime has evolved to become a service in which various groups sell offensive goods and services, ranging from system exploits to full attack lifecycles.
- **Advanced persistent threats (APTs)**: As defined by the United States National Institute of Standards and Technology (NIST), these are highly sophisticated and resourceful adversaries able to establish a foothold in the network of the target for purposes such as exfiltrating information, undermining or impeding critical aspects of the target's mission or degrading its digital assets.[116] Advanced persistent threats adapt to victims' defence systems by using multiple attack vectors, and they are able to pursue their objective stealthily for prolonged periods of time. These adversaries are the most sophisticated in terms of technical skills, funding and organizational resources, and they are often sponsored by States seeking to pursue their geopolitical interests.

While all malicious actors target the confidentiality, integrity and availability of information and assets, there is a wide spectrum of possible outcomes for network intrusion. The catch-all expression "cyberattack" covers a variety of actions, ranging from nuisances, such as website defacement or DoS attacks, to critical destruction of data and systems through weaponized attacks.

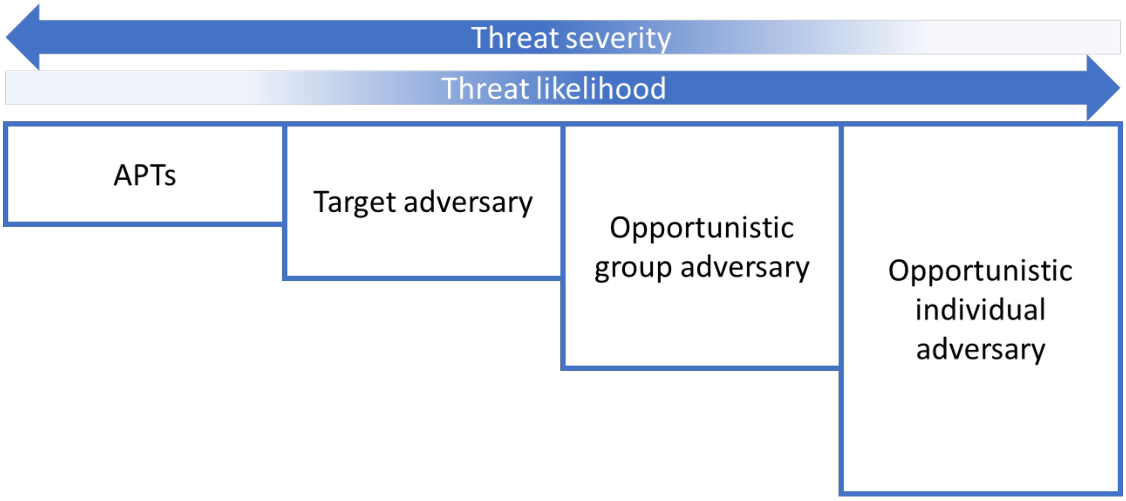
Malicious actors and their attacks differ in terms of sophistication, duration and harmfulness. While it is impossible to defend against all threats, organizations can apply threat models to identify relevant threats according to their profile, risk and context. **Figure 1** illustrates a general cyberthreat model, which demonstrates that the majority of organizations typically face opportunistic and less sophisticated threats, thus requiring less articulated defence postures.

[114] Verizon. 2019 Data Breach Investigations Report. Verizon, 2019.

[115] Lillian Ablon. Data Thieves: The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data. RAND Corporation, 2018.

[116] NIST. Joint Task Force Transformation Initiative. NIST Special Publication 800-39: Managing Information Security Risk - Organization, Mission, and Information System View, March 2011.

Figure 1: Threat model


Threat severity
Threat likelihood
APTs
Target adversary
Opportunistic group adversary
Opportunistic individual adversary

On the contrary, large businesses, organizations that operate in critical and strategic sectors and subjects that manage valuable information and assets are more likely to be attacked by targeted threats or advanced persistent threats.

This section has provided a general overview of cyberspace threats. The remainder of the chapter will provide information on how such threats apply to emerging technologies and what workable strategies, frameworks and solutions are available to defend against them.

5.2.1 Threats seen from a technological perspective

Emerging technologies collect, share, store and analyse enormous amounts of data, often at unprecedented speed. However, specific characteristics, such as the increasing connectivity and complexity of environments in which these tools interact, can raise a number of technological and organizational challenges for security.

Virtualization

Virtualization constitutes a key pillar of modern technological environments, as it allows developers to customize infrastructures to respond to the needs of network applications and support the development of new architectures and protocols in an ideal environment.[117] However, the sharing of communication channels and router devices in multitenancy situations presents a number of security risks:[118]

- The risk of unauthorized disclosure of data, both intentional and unintentional, is exacerbated in virtual environments in which physical resources are shared between several clients or users. Malicious activities such as interception and scavenging (searching for data residue in a network in order to acquire information) can be more easily conducted if the system allows cross-inspection of the various users.
- Multitenancy may increase the risks that stem from the supply chain and makes it more difficult to defend against intrusions. Adversaries can obtain privileges and intrude on the target's network by using resources with a lower protection level that share the same physical layer as a vector.

[117] Leonardo Richter Bays et al. Virtual network security: threats, countermeasures, and challenges. *Journal of Internet Services and Applications* 6, article no. 1 (2015).

[118] European Union Agency for Cybersecurity (ENISA). Security aspects of virtualization, 10 February 2017.

- In virtualized environments, identity-handling results are particularly complex, owing to the highly hierarchical systems of privileges administration. This context provides room for malicious actors to commit identity fraud and escalate privileges.
- Sharing resources may also magnify the risk of malicious or involuntary system disruptions that can negatively affect the supply of services. For example, the overloading of physical resources can degrade the performance of virtual networks, with a consequent disruption in communication.

Cloud security

In cloud solutions, the delivery of IT service and resources, including the associated security functions and responsibilities, is outsourced to the cloud provider. On the one hand, this can allow new technologies to scale quickly and strengthen security, since the provider, building on economies of scale, can potentially offer advanced protective measures and controls. However, cloud vulnerabilities can be tempting to cyberattackers, given that a single, successful hack could compromise many customers. Cloud solutions comprise several layers of abstraction (namely application, operating system, architecture and network), meaning that adversaries can target them through multiple vectors:

- Software vulnerabilities can be exploited through structured query language injections and other attack patterns. In this scenario, it is important for cloud customers to be aware of who is in charge of the patching activities (namely the cloud solution provider for software-as-a-service solutions, and the customer for infrastructure-as-a-service and platform-as-a-service solutions).
- Cloud solution providers offer a wide range of services and Internet-connected application programming interfaces to allow customers to administrate and monitor their assets. Such connectivity makes cloud solutions a potential target for network attacks, such as sniffing/eavesdropping on network traffic, DoS attacks and man-in-the-middle attacks.
- If an attacker is able to illegitimately acquire users' credentials, it might be able to access the management interface used by administrators to manage a large number of assets. Strong authentication and authorization mechanisms, especially for high-privilege employees, must therefore be established.
- Multitenancy increases the risk of data breaches or data leaks if separation controls fail or are hacked (isolation failure).
- When transitioning to cloud solutions, customers generally have less visibility and control over their data and assets. This increases the risks associated with the secure deletion of data stored over a number of devices within the cloud solution provider's infrastructure. It is important to verify that data have been securely and thoroughly deleted. This problem is exacerbated by multicloud solutions.
- Vendor lock-in, in which customers face difficulties in migrating to another cloud solution provider, can pose serious security risks. Users should include plans for changing providers in their business continuity strategies and should store all data in a standard, easily transferrable format.
- According to the Communication Regulatory Authority of Namibia, the storage of customer data in cloud service data centres located outside national borders is a pressing problem. In countries where data servers are hosted, regulators have no jurisdiction and little oversight to deal with matters of customer protection and cybersecurity when cyberattacks occur, resulting in personal identity theft, leakage of personal information and, in some cases, potential revenue loss. Furthermore, legislation in host countries can differ with regard to access to information, data protection and lawful interception, which may expose customers to unauthorized access of personal data.[119]

[119] ITU-D SG2 Document SG2RGQ/75 from Namibia

Internet of Things

With the diffusion of a security-by-design culture still in its infancy, increasing connectivity is one of the most concerning trends in terms of risk, and it poses significant security challenges: [120]

- Smart objects – which range from cameras, doors and refrigeration to air conditioning systems and wearable devices – collect an enormous amount of information (both data and metadata). Attackers can learn a lot about the life of their target by eavesdropping on the data sensed by the target's smart objects.
- An emerging threat to IoT is ransomware. Smart devices offer an appealing extortion landscape to attackers, not only because of the vast number of low-hanging targets, but also because attacks of this fashion can disrupt the functionality of devices, thereby inconveniencing the target and forcing them to pay the ransom.[121]
- IoT devices are particularly vulnerable to DoS and DDoS attacks, as most of them have limited technical capabilities (memory, storage, central processing unit, etc.). Attackers can easily overwhelm their limited resources, causing service disruptions.
- The limitation of resources in IoT devices constitutes a critical challenge when it comes to including security measures, which can be computationally heavy.[122]
- A key security issue for IoT lies in its level of complexity. Devices merge different technologies, such as virtualization, cloud computing, sensors and networks, which carry their own vulnerabilities. To secure IoT means to secure the whole chain of such components. Similarly, IoT has applications in several domains (home automation, healthcare, wearables, etc.), which have different security needs and are subject to different threats.
- Although Internet-based attacks are the most common, IoT devices can also be targeted through physical attacks. In areas with little or no surveillance, attackers can easily reach and tamper with IoT devices.
- IoT devices can also be used as vectors to launch DDoS attacks. In 2016, for instance, a famous domain name system provider fell victim to a DDoS attack that originated from tens of millions of IP addresses, with the majority of the malicious traffic coming from IoT devices such as printers, routers and cameras.[123]

5G

The fifth generation of communication technology, known as 5G, will deliver a more reliable and high-quality connection based on high speeds and low latency, which will maximize the output of emerging technology applications in areas such as energy, health and manufacturing. These assets are an appealing target for attackers, and their intrinsic vulnerabilities make cybersecurity particularly challenging. Furthermore, as 5G solutions are still in the pilot phase, there is a paucity of information and data about cyberattack incidents, which makes it even harder to understand the potential threat:[124]

- The 5G threat landscape is broad and heterogeneous; by combining diverse technologies, it also inherits their vulnerabilities and threats. In particular, 5G networks and assets can be targeted by leveraging legacy insecurities from second-, third- and fourth-generation

[120] Amit Ashbel. The rise of IoT and the associated security risks. 7 July 2016.

[121] Syed Rameem Zahra and Mohammad Ahsan Chishti. RansomWare and Internet of Things: A New Security Nightmare. *Proceedings of the 9th International Conference on Cloud Computing, Data Science Engineering (Confluence)*, Uttar Pradesh, India, 10-11 January 2019.

[122] Ammar Rayes and Samer Salam. Internet of Things From Hype to Reality: The Road to Digitization. Springer International Publishing, 2019.

[123] Nicole Perlroth. Hackers Used New Weapons to Disrupt Major Websites Across U.S. *The New York Times*, 21 October 2016.

[124] ENISA. ENISA threat landscape for 5G Networks. November 2019.

technologies, traditional IP-based weaknesses, and flows introduced by virtualization technology. Attackers can also target 5G-specific assets, such as core, access point and edge elements.

- Attacks against 5G technologies can include attempts to steal, manipulate or destroy data, intercept or disturb communications, damage physical assets or disrupt the supply of services. 5G will connect a wide spectrum of sectors and verticals, which will more than likely change the cybersecurity landscape, leading to new vulnerabilities.
- A critical threat factor stems from the supply chain, in particular compromised vendor and service providers. The risk is that a vendor could maliciously embed in its products concealed backdoors, software or critical flaws. The implementation of automatic (and uncontrolled) updates and the manipulation of functionalities also pose issues for security. The relation between 5G and national security is evident, and providers should be selected carefully based on a risk-oriented approach.

Artificial intelligence

The proliferation of artificial intelligence solutions in different sectors of society will impact the cybersecurity landscape in several ways. Such assets can be targeted by malicious actors or used by adversaries and defenders:

- AI assets may be manipulated by altering automated decisions and behaviours, in particular through data poisoning, tampering of categorization models, and backdoors.[125]All these methods leverage the learning capacity of the system in order to negatively alter the output by feeding the system erroneous data and information.[126]
- Hackers are turning to AI solutions to improve their reach and capabilities. AI can be used to provide malware capable of bypassing defensive measures autonomously, adapting its strategies on the basis of successes and constantly improving its operations.
- AI is also an important defensive resource. It can significantly increase a system's resilience by enhancing typical defensive activities, such as the detection of threats and anomalies, incident response and threat analysis.

5.2.2 Threats seen from an Industry 4.0 perspective

The Industry 4.0 paradigm entails the application of automation, together with IoT, virtualization solutions, analytics and AI, to different verticals. These technologies allow huge amounts of data to be collected, stored, shared and interpreted and can bring significant improvements in terms of speed, efficiency, cost-effectiveness and supply of services. Industry 4.0 can be applied to various sectors, each of which is susceptible to specific threats and security risks.

Smart homes

Smart homes are one of the many verticals in which Industry 4.0 can be applied, in particular in smart energy consumption, lighting and heating. Smart homes contain a wide variety of smart

[125] Battista Biggio and Fabio Roli. Wild patterns: Ten years after the rise of adversarial machine learning. *Pattern Recognition,* Vol. 84, December 2018, pp. 317-31.

[126] Matthew Jagielski et al. Manipulating Machine Learning: Poisoning Attacks and Countermeasures for Regression Learning. *IEEE Symposium on Security and Privacy (SP), 2018.*

objects that use sensors and actuators and are remotely managed via the Internet.[127] Connecting devices to the Internet creates a number of security risks:

- Smart homes generate huge amounts of data that are vulnerable to attack. As noted by the Ministry of Posts and New Information and Communication Technologies of Chad, connected objects (including smart televisions) are exposed to information system security threats. For example, the use of connected televisions can allow unauthorized persons to access private data via the Internet and can facilitate Internet-based identity theft. Connected objects are vulnerable in the same way as personal computers connected to a computer network, and they are similarly exposed to malware threats.[128]
- Smart devices have poor security and can easily be hijacked. Attackers who gain control of the device can move laterally within the domestic network in order to take control of other nodes.
- Smart devices typically have poor computational resources, which makes them particularly vulnerable to DoS and DDoS attacks, which render the device or network temporarily unavailable to its intended user.

Smart cities

Smart cities combine emerging technologies with data integration and task automation to optimize the organization of cities and offer better services. Smart cities are based on extensive data flows shared among critical services, such as transportation, energy supply and healthcare, which are increasingly interconnected. The scale of data produced, and the role that data play in the functioning of smart cities, produces a crucial need for cybersecurity in order to protect the privacy of information and the integrity of digital assets against various security threats:

- **E-health**: As the reliance on technology and the volume of health data grows, healthcare providers must protect sensitive information and ensure the provision of services. Although no known incidents have yet occurred, simulations have demonstrated that it is possible to wirelessly turn off implantable cardiac defibrillators,[129] hack insulin pumps to release lethal doses[130] and even infiltrate patient-monitoring systems to modify patients' vital signs in real time.[131]
- **Smart grids**: These are a key component of smart cities. They use bidirectional devices, such as sensors, actuators and meters, which allow a continuous balance and supervision of energy flows from producers to consumers to be maintained.[132] As smart grids rely on ICT protocols and Internet connections, they are vulnerable to cyberattacks.[133] Smart grids make a tempting target for attacks; however, smart grids have a complex architecture, and causing large-scale harm requires high-level technical and organizational resources. To date, there have been only two known cases of major power outages caused by cyberattacks, namely the BlackEnergy3 and Crashoverride attacks, both of which are thought to have been carried out by State actors.[134]

[127] Ado Adamou Abba Ari et al. Enabling privacy and security in Cloud of Things: Architecture, applications, security & privacy challenges. *Applied Computing and Informatics*, 31 July 2020.

[128] ITU-D SG2 Document 2/140 from Chad

[129] Daniel Halperin et al. Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses. *IEEE Symposium on Security and Privacy (SP), 2008.*

[130] Arundhati Parmar. Hacker shows off vulnerabilities of wireless insulin pumps. *MedCityNews,* 1 March 2012; David Klonoff. Cybersecurity for Connected Diabetes Devices. *Journal of Diabetes Science and Technology* 9, Vol. 9, No. 5, 16 April 2015.

[131] Douglas McKee. 80 to 0 in Under 5 Seconds: Falsifying a Medical Patient's Vitals. McAfee, 11 August 2018.

[132] Lindah Kotut and Luay A. Wahsheh. Survey of Cyber Security Challenges and Solutions in Smart Grids. *2016 Cybersecurity Symposium (CYBERSEC).*

[133] Muhammed Zekeriya Gunduz and Resul Das. Cyber-security on smart grid: Threats and potential solutions. *Computer Networks*, Vol. 169, 14 March 2020.

[134] Dragos, Inc. CRASHOVERRIDE: Analyzing the Malware that Attacks Power Grids. 12 June 2017.

- **Intelligent transportation**: Digital assets, physical systems, communication networks and automation can be applied to transport infrastructure to optimize quality and efficiency. By changing data and information, attackers can obstruct traffic and even induce incidents. Furthermore, intelligent transportation systems involve a significant flow of personal and sensitive information that needs to be secured.

Industrial Internet of Things

The industrial Internet of Things (IIoT) adapts the IoT paradigm to the industrial landscape. When combined with robotics and automation, it can generate valuable benefits for industrial companies, including by improving the quality, cost-effectiveness and maintenance of the production process. These cyberphysical systems have specific characteristics and requirements that make transposing traditional cybersecurity measures particularly problematic.

Cyberphysical systems are hard real-time environments with a high level of determinism, in which data availability is prominent compared to integrity and confidentiality.[135] In such systems, digital components interface with physical processes, such as motions of objects, chemical reactions, release of substances and cooling processes, and data flows work as inputs for the execution of tasks. In such contexts, adopting common security controls, such as antivirus software, encryption or firewalls, could slow down the flow of data and interfere with the running of activities, leading to delays that, although quantitatively unimportant, could significantly affect operations.[136]

In addition, most equipment in cyberphysical systems cannot handle sophisticated security measures or updates, which results in Internet-connected assets that are potentially vulnerable. Cyberattacks against industrial cyberphysical systems can inflict serious economic damage by disrupting operations and, consequently, production at a plant.

However, the main concern is that, by manipulating the flow of data, cyberattackers could modify the functioning of a system until it reaches a mechanical break point, leading to a kinetic impact that could have serious consequences for public safety. For example, if an attacker supplies the system with altered figures that tell the controller that a temperature is decreasing too fast, the controller will automatically compensate by increasing heating, leading to undetected overheating.[137] For example, in 2014 a German steel mill was successfully hacked, and the attackers, by preventing a furnace from being properly shut down, were able to cause massive physical damage to critical components.[138]

Offensive cyberoperations with physical effects are extremely complex, requiring not only a good understanding of the digital assets in use, but also extensive knowledge of the physical process targeted and a detailed comprehension of the different variables. For this reasons, advanced persistent threats and State-sponsored proxies are most likely to have the technical and organizational resources required to execute operations of this type.

[135] Roberto Setola et al. Cyber threats for operational technologies. *International Journal of System of Systems Engineering*, Vol. 10, No. 2, 2020.

[136] Roberto Setola et al. An overview of Cyber Attack to Industrial Control System. *Chemical Engineering Transactions*, Vol. 77, 2019.

[137] Stephen McLaughlin et al. The Cybersecurity Landscape in Industrial Control Systems. *Proceedings of the IEEE*, Vol. 104, issue 5, May 2016.

[138] Robert Lee et al. German Steel Mill Cyber Attack. Industrial Control Systems Defense Use Case Dec 30, 2014.

5.3 Existing and emerging solutions

A significant proportion of IoT devices do not have basic cybersecurity features built into them. In October 2018, following 18 months of collaboration with industry representatives and experts at the National Cyber Security Centre, the Department for Digital, Culture, Media and Sport of the United Kingdom published the Code of Practice for Consumer IoT Security.[139] The 13 voluntary guidelines in the code provide a baseline for IoT devices which manufacturers should embed into their products to make them "secure by design". The code contributed to the development of the first globally applicable standard on IoT security, ETSI TS 103 645.[140]

Algérie Télécom has also emphasized the importance of providing guides and recommendations on securing emerging technologies, such as the cloud and IoT, that are due to become the essential engine in the development of the information system and the digital economy.[141]

Table 1 and **Table 2** provide a list of ITU-T Recommendations that are relevant for the protection of cloud and IoT respectively, in terms infrastructure, applications, data and privacy**.**

Table 1: Security architecture for the protection of cloud infrastructure, applications, data and privacy

Title	Topic	Institution	Link
Overview of cloud-computing security			
ITU-T X.1601	Security framework for cloud computing	ITU	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=12613
Cloud-computing security design			
ITU-T X.1602	Security requirements for software as a service application environments	ITU	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=12615
ITU-T X.1603	Data security requirements for the monitoring service of cloud computing	ITU	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=13406
ITU-T X.1604	Security requirements of Network as a Service (NaaS) in cloud computing	ITU	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=14093
ITU-T X.1605	Security requirements of public Infrastructure as a Service (IaaS) in cloud computing	ITU	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=14094
ITU-T X.1631	Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services	ITU	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=12490

[139] United Kingdom, Department for Digital, Culture, Media and Sport. Code of Practice for Consumer IoT Security. October 2018.
[140] ETSI. ETSI TS 103 645 V1.1.1 (2019-02). Cyber Security for Consumer Internet of Things.
[141] ITU-D SG2 Document 2/66 from Algérie Télécom SPA (Algeria)

Table 1: Security architecture for the protection of cloud infrastructure, applications, data and privacy (continued)

Title	Topic	Institution	Link
Cloud-computing security best practices and guidelines			
ITU-T X.1641	Guidelines for cloud service customer data security	ITU	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=12853
ITU-T X.1642	Guidelines for the operational security of cloud computing	ITU	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=12616

Table 2: Security architecture for the protection of IoT infrastructure, applications, data and privacy

Title	Topic	Institution	Link
IoT security			
ITU-T X.1361	Security framework for the Internet of things based on the gateway model	ITU	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=13607
ITU-T X.1362	Simple encryption procedure for Internet of things (IoT) environments	ITU	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=13196
ITU-T X.1364	Security requirements and framework for narrowband Internet of things	ITU	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=14088
ITU-T X.1365	Security methodology for the use of identity-based cryptography in support of Internet of things (IoT) services over telecommunication networks	ITU	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=14089
ITU-T X Suppl. 31	ITU-T X.660 – Supplement on guidelines for using object identifiers for the Internet of things	ITU	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=13411

Other emerging security techniques and frameworks

- AI applications, including both machine learning and deep learning, can significantly benefit cybersecurity strategies in terms of efficiency and cost-effectiveness. These solutions use regression, classification and clustering to detect anomalies, identify different typologies of attacks and develop potential remediation responses. Artificial intelligence systems can also enhance incident response activities by suggesting specific actions in response to particular incidents. They can also improve risk management activities by automatically assigning risk values to new vulnerabilities and misconfigurations based on their descriptions and proactively prevent attacks by dramatically expediting the extraction, elaboration and application of data about threats, actors, attacks, malware, vulnerabilities and indicators of compromise.[142]

- Specific features of distributed ledger technology (DLT) also show promise for security applications.[143] First, DLT-based storage is decentralized, which significantly reduces the risk of extensive data breaches, as attackers are no longer able to access all held data through a single access point. Similarly, decentralization brings essential security benefits to IoT networks, which are traditionally organized according to client-server model logic, in which a central authority manages the data and devices within the network. With DLT applications, IoT devices can identify anomalies and isolate nodes that behave unusually. Also, DLT may create trust in IoT networks, by ensuring that the availability, auditability, accountability, integrity and confidentiality of exchanged data remain constant.[144]
- The security orchestration, automation and response (SOAR) method entails solutions that connect security tools and systems in order to perform activities such as vulnerability management, incident response and security operations automation in an integrated and organic manner. Automation of security processes allows the system to implement remediation and maintenance activities (vulnerability scanning, access and log monitoring) without human intervention.
- Another option is zero-trust models, in which network environments are internally segmented and accesses are administrated according to the principle of least privilege. This means that every module, including users, devices, application programming interfaces and IoT devices, are able to access only the resources, data and assets that are necessary for their legitimate function. Zero-trust models dramatically increase internal security, as they make lateral movement and the escalation of privileges more challenging for attackers who, in order to gain access to the entire network, will need to target multiple devices.
- Cloud access security brokers are policy enforcement points that operate between users and cloud providers. For instance, enforced security policies can include authentication, single sign-on, authorization, credential mapping, device profiling, encryption, tokenization, logging, alerting and malware detection/prevention.[145]
- Privileged access management refers to a set of tools and solutions for monitoring and protecting privileged accounts, such as administrator accounts used to access critical assets, data and resources. Such solutions isolate critical accounts in a secure and monitored repository, thereby reducing the risk of credentials being stolen.
- Organizations should move from a development and operations (DevOps) approach to a development, security and operations (DevSecOps) approach, which integrates security as an intrinsic part of development and operations. Within DevSecOps frameworks and tools, instead of being bolted on to final products (such as software and applications), security is considered an integral and essential feature from the earliest stage of development. This approach makes security more solid, mitigates risks and reduces compliance costs.
- Gartner's Continuous Adaptive Risk and Trust Assessment (CARTA) framework proposes an adaptive approach to security, in which decisions are based on risk and efficiency.[146] CARTA entails three phases: "run", which focuses on major threats analysis; "build", which refers to threats and vulnerabilities identified during the development of products and operations; and "plan", in which analytics are employed to determine security risks and assess whether mitigating them would negatively affect productivity.[147]

[142] Padmavathi Ganapathi and D. Shanmugapriya. Handbook of Research on Machine and Deep Learning Applications for Cyber Security. *IGI Global*, 2019*;* and Dave Shackleford. Who's Using Cyberthreat Intelligence and How?. *SANS,* 12 February 2015.

[143] Nir Kshetri. Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy*, Vol.41, issue 10, November 2017.

[144] Ben Cole. The 'supply chain of trust' inherent to IoT data security. *IoT Agenda*, 28 November 2016.

[145] Gartner. Gartner Glossary. Cloud Access Security Brokers (CASBs)

[146] Gartner. The Gartner IT Security Approach for the Digital Age. 12 June 2017.

[147] Gartner. Gartner Keynote: Leverage Automation for Modern Security. 17 June 2019.

Cost-effective solutions

- According to the Department for Digital, Culture, Media and Sport of the United Kingdom, by focusing on affecting the return on investment of the most common, less sophisticated attacks, it is possible to begin to tackle the impact of cyberattacks at scale with significant global benefits. The Active Cyber Defence (ACD) scheme was developed to raise the cost and risk of mounting commodity cyberattacks against the United Kingdom, thereby reducing the return on investment for criminals.[148] In 2018, the scheme had the greatest impact through its takedown service, which identifies malicious sites (either attacks or attack-supporting infrastructure) and notifies the host or owner that they must be removed from the Internet: a total of 192 256 fraudulent websites were taken down in this manner, 64 per cent of which were taken down within 24 hours. In addition, 22 133 phishing campaigns hosted in IP space delegated to the United Kingdom (totalling 142 203 individual attacks) were taken down, and 14 124 government-related phishing sites were removed.[149]
- According to Lithuanian company NRD Cyber Security, in order to achieve a significant positive impact on the security of the national digital environment, national and sectorial CSIRTs should work not only as points of contact, incident response coordinators and analysts, but also as inspirational facilitators in developing additional independent cybersecurity capabilities within industries, professional communities, education centres, research, events, meetings, conferences, and private and internal CSIRTs.[150]
- According to Estonian company Guardtime, cyberexercises are essential to achieve sustainable cyberresilience as they help teams understand the processes needed to mitigate a cybercrisis. Estonia recommends developing a cyberresilience governance programme that covers education, training and cyberexercises, ranging from localized events to regular customized national-scale exercises. Such programmes should take into consideration various aspects of the national organizational structure and socio-economic situation, the roles and responsibilities of the different stakeholders, the national regulatory environment, the country's regional and international partnerships and the various risks that the country faces within the evolving cyberthreat landscape.[151]

[148] Ian Levy and Maddy S. Active Cyber Defence (ACD) - The Second Year. United Kingdom National Cyber Security Centre. 15 July 2019.

[149] ITU-D SG2 Document SG2RGQ/175 from the United Kingdom

[150] ITU-D SG2 Document 2/172 from NRD Cyber Security (Lithuania)

[151] ITU-D SG2 Document SG2RGQ/32 from Guardtime AS (Estonia)

Chapter 6 – How cybersecurity can support the protection of personal data

6.1 Introduction

With the advent of new information technologies, various new and increasingly convenient services are emerging for day-to-day use. Nonetheless, the advent of new information technologies also bilaterally changes the privacy and data protection risks that individuals face. Although new dangers to personal data continue to emerge, various techniques can be used to minimize or avoid such risks. For this reason, greater focus must be placed on cybersecurity and privacy-enhancing technologies that can support the protection of personal data, such as pseudonymization and privacy by design.

Pseudonymization is a data management and de-identification procedure through which personally identifiable information fields within a data record are replaced by one or more artificial identifiers, or "pseudonyms". A single pseudonym for each replaced field or collection of replaced fields makes the data record less identifiable, while remaining suitable for data analysis and processing.[152] Pseudonymization can help protect personally identifiable information and may reduce the burden on entities that collect and hold such data.

In privacy by design, one does not wait until after a breach to take security measures. Instead, developers predict or anticipate privacy threats or prevent them from happening through preventive measures, such as service planning or design.[153] The difference between the two approaches is that, while pseudonymization requires certain technical measures, privacy by design gives data controllers flexibility in determining which additional technical measures can best ensure data security and privacy.

6.2 Legal landscape and best practices in Member States

In Brazil, the newly adopted General Data Protection Act includes definitions of the various types of personal and processing data and provides for the legal permissions for domestic and international processing, the fundamental rights of data subjects and the creation of a national data-protection authority.[154] The act establishes the principles of data minimization, data breach prevention and data security and stipulates specific rules to govern those areas. The act also embraces security by design, stipulating that security measures to protect personal data shall be implemented from the conception phase of the product or service through to its execution.

[152] Wikipedia. https://en.wikipedia.org/wiki/Pseudonymization

[153] Privacy by design was used in the existing architecture field, but the concept was secondary. It began to gain traction after being referenced by Dr Ann Cavoukian, Information and Privacy Commissioner of Ontario, Canada, in the mid-1990s.

[154] ITU-D SG2 Document SG2RGQ/143 from Brazil

In 2017, China formally released a set of national standards on personal information security specifications in information security technology, which complement the personal information security requirements set out in its Cybersecurity Act. The standards provide guidelines and operational instructions. China is continuing to research and develop standards on personal information protection.[155]

In China, local data security companies are also actively researching and developing security products and services, including in the areas of data loss prevention, database safety auditing, database leak scanning, database encryption and data masking, with a view to providing technical support for personal information protection.

The Republic of Korea has introduced a major amendment to its Personal Information Protection Act to provide for technical measures to protect personal data.[156] The amendment incorporated changes to streamline regulatory supervision and to introduce the concept of "pseudonymized data", which allows data controllers and processors to process data more safely, while minimizing the risk of data misuse and breach through other technological and organizational measures such as data protection by design and by default.

In addition, the Government of the Republic of Korea has published protection guidelines on the automatic processing of personal data. While new technologies, such as AI-based big-data analysis and the sensors used in IoT devices to collect data, are making innovative services possible, there are difficulties in understanding the flow of personal data processing and limitations in follow-up responses. In the automatic processing of personal data from IoT devices, the guidelines encourage the application of privacy by design, in which the potential for personal data breaches is given thorough consideration from the very first planning steps and throughout the data lifecycle.

The 10 protective rules for the automatic processing of personal data included in the guidelines are:

- Planning phase
  - Rule 1: Confirmation of personal data necessary for services
  - Rule 2: Confirmation of legal observances upon collection of personal data
- Design phase
  - Rule 3: Data minimization and processing of necessary personal data only
  - Rule 4: Application of appropriate safety measures in each personal data processing step
  - Rule 5: Transparent dissemination of personal data processing procedures and methods
  - Rule 6: Guarantee that data subjects can easily exercise their rights
  - Rule 7: Clear instructions for data subjects upon provision and commission of personal data for a third party
  - Rule 8: Destruction of personal data and prevention of further collection upon termination of service by data subject

[155] ITU-D SG2 Document 2/156 from China
[156] ITU-D SG2 Document 2/342 from the Republic of Korea

  - Rule 9: Plans for guaranteeing the right of the data subjects upon termination of business

- Examination phase

  - Rule 10: Examination of risk factors related to personal data breaches before service launch.

Given the recent need to track confirmed cases of COVID-19 around the world, the Republic of Korea has taken various institutional and technical measures to protect personal data. In addition to securing the legal basis for tracking confirmed patients by revising relevant regulation, technical measures are being taken to separate and manage identification information to prevent possible personal information breaches. Separate information is used for epidemiological investigations only when confirmed cases occur, and individual user and visitor information are managed safely, such as by being automatically destroyed four weeks after generation.[157]

An Italian company has developed a proprietary methodology that can easily be used by organizations to draw up a list of technical activities for bringing cloud infrastructure (private, public or hybrid) into compliance with privacy regulations.[158] The methodology includes a proposal for defining general guidelines that could be used by Member States to build their own national configurators in order to standardize multicountry compliance more efficiently and cheaply, using the cloud as a powerful platform to facilitate the explosion in the digital economy.

In another case of best practice, Article 25, on data protection by design and by default, of the European Union General Data Protection Regulation (GDPR) recognizes privacy by design as the most suitable method for preventing personal data protection risks posed by IoT devices, big data, AI and other new technologies. With the notion of privacy by design, appropriate organizational and technical measures to ensure personal data security and privacy are embedded into the complete lifecycle of an organization's products, services, applications, and business and technical procedures. Technical measures can include, but are not limited to, pseudonymization and data minimization.[159]

The European Union Agency for Cybersecurity (ENISA) has presented eight key strategies to help businesses apply privacy by design with the aim of examining various methods of approachability, strategies and technical factors for the protection of personal data.[160]

[157] ITU-D SG2 Document SG2RGQ/268 from the Republic of Korea

[158] ITU-D SG2 Document SG2RGQ/25 from Proge-Software (Italy)

[159] European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[160] ENISA. Privacy and Data Protection by Design – from policy to engineering. December 2014.

Table 3: Eight key strategies for application of privacy by design

	Principle	Content
1	Minimize	Minimize the quantity of processed personal data by processing according to clear purposes with a view to reducing the possibility of privacy infractions
2	Hide	Hide plain text transmission when processing personal data in order to prevent access from the outside
3	Separate	Separate and store a variety of personal data to prevent discrimination against a single individual in the database
4	Aggregate	Aggregate large quantities of personal data processing to minimize discrimination against individuals and categorize processing results to make discrimination impossible
5	Inform	Inform data subjects about the entire process of personal data processing in order to provide a transparent understanding of the purposes for which data are used
6	Control	Control personal data use. Data subjects must understand the entire process of personal data processing and be able to exercise their rights regarding wrongful use of their personal data or security levels based on the fifth strategy, "inform"
7	Enforce	The internal personal data protection policy must reflect legal and systematic duties and must be enforced
8	Demonstrate	Demonstrate compliance with legal obligations, such as the effective operation of personal data protection policies and immediate action against incidents involving data outflow

ENISA has also made suggestions for privacy and data-protection activities to be undertaken by various stakeholders. It recommends that policy-makers promote and support the development of new incentives to advance personal data protection services and that research and development groups investigate engineering methods for protecting personal data through an interdisciplinary approach and disseminate research results via policy-makers and the media. Lastly, the agency recommends that software developers provide technology that can intuitively actualize privacy properties and supports the protection of personal data in publicly and mutually established infrastructure projects.

In the United States, the Federal Trade Commission (FTC) emphasizes practical and procedural principles for privacy protection, such as privacy by design, simplified consumer choice, and substantive and procedural principles such as guaranteed transparency. The commission also stresses the protection of consumer privacy in business organization, products and all stages of service development.[161]

The Spanish Data Protection Authority (AEPD) has published a guide to privacy by design in which it underlines the need to consider privacy and the principles of data protection from the

[161] FTC. Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policy-makers. March 2012.

inception of any type of processing. The guide also presents basic principles and strategies for processing personal data.[162]

Table 4: Link between privacy goals and privacy design strategies

Privacy protection goals	Data-oriented privacy protection strategies	Process-oriented privacy protection strategies
Unlinkability	Minimize, abstract, separate, hide	
Control		Control, enforce, demonstrate
Transparency		Inform

6.3 Lessons learned and way forward

The rate of cyberattacks, data breaches and unauthorized use of personal data is growing exponentially. It is more important than ever, particularly for organizations that handle personally identifiable information, to understand the rights and obligations of individuals and organizations with regard to personal information.

This chapter presented an overview of the legal changes and technical cybersecurity measures concerning personal data protection introduced in Member States. It also covered best practices to help Member States comply with evolving data-privacy requirements and touched on the role of cybersecurity technologies in mitigating risks and supporting compliance.

The following lessons can be derived from the examination of various cybersecurity technologies and best practices used by Member States in personal information protection:

- Institutional arrangements for pseudonymization, privacy by design and other technological measures help create a more secure environment.
- Businesses that collect and use personal information need to make active efforts to introduce technical measures to protect personal information on a more fundamental level.
- Various stakeholders, including data subjects, civil society, academics and industry representatives, need to collectively discuss the use of technology and make efforts to raise awareness and improve security.

[162] *Agencia Española Protección Datos (AEPD).* A Guide to Privacy by Design. October 2019.

Chapter 7 – The future of the Question

Cybersecurity is an important issue for all stakeholders, including governments and consumers. The work carried out by ITU-D in that regard is helping to raise awareness of the risks. As rates of connectivity and Internet use around the world continue to rise, the need to protect consumers and systems remains important. Given the continued global need to share information about cybersecurity practices, the ITU-D Study Group 2 Question 3/2 management team is of the view that the Question on cybersecurity issues should remain the same for the next study cycle. The topics addressed during this study period remain relevant and should form the basis for further contributions and work during the next study period. The general framework of the Question should therefore be retained unchanged: as security issues concern all technologies, Question 3/2 continues to apply to all new and emerging technologies, which are, by nature, integrated in their design.

Annexes

Annex 1: List of contributions and liaison statements received on Question 3/2

Contributions on Question 3/2

Web	Received	Source	Title
2/407	2021-03-03	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
2/400	2021-03-01	United States	Update on Cyber Awareness Campaigns
2/385	2021-01-28	Bhutan	Survey findings on National Child Online Safety and Protection
RGQ2/278	2020-09-22	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
RGQ2/272	2020-09-22	United Kingdom	UK case study: Cyber resilience best practice for SMEs
RGQ2/268	2020-09-22	Republic of Korea	Protecting personal data in responding COVID-19 pandemic (Korea's experience)
RGQ2/261	2020-08-19	Togo	Draft text for Chapter 1 of the Final Report for Question 3/2 - Update on the status of spam and malware, including mitigation responses
RGQ2/241	2020-08-26	United Kingdom	Updated case study on securing consumer Internet of Things (IoT) devices in UK
RGQ2/235	2020-08-20	United Kingdom	UK Government Digital Service (GDS) Global Digital Marketplace Programme
RGQ2/234	2020-08-20	United Kingdom	UK case study - reporting service for phishing emails
RGQ2/216	2020-07-27	Brazil	Brazilian National Cybersecurity Strategy (E-Ciber)
RGQ2/215	2020-07-27	Brazil	#SafeConnection (#ConexãoSegura) Awareness Campaigns
RGQ2/214	2020-07-27	Brazil	Brazilian National Cyberdrill - Cyber Guardian Exercise
2/344	2020-02-11	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
2/342	2020-02-11	Republic of Korea	Korea's major amendment to data protection law and its implication
2/341	2020-02-11	Republic of Korea	Implementation plan for strengthening national cybersecurity of Korea

(continued)

Web	Received	Source	Title
2/338	2020-02-11	Co-Rapporteur for Question 3/2	Draft table of contents (V1) for the Final Report of Q3/2
2/336	2020-02-11	United Kingdom	Case study of best practices for securing customer Internet of Things in the UK
2/331	2020-02-11	Keio University (Japan)	Proposed text for consideration of security issues for ICT accessibility
2/328	2020-02-08	Deloitte (United States)	People with disabilities and the Internet of Things
2/325	2020-02-08	Democratic Republic of the Congo	La sécurité numérique en République Démocratique du Congo
2/322	2020-02-07	Welchman Keen (Singapore)	Enhancing capacity and capability for critical national infrastructure in the Pacific Island Nations
2/321	2020-01-08	Sudan	WSIS project for consideration by Question 3/2
2/305	2020-01-15	Mexico	Perception on security and trust from Mexican users on fixed and/or mobile Internet
2/287	2020-01-07	China	Forum on network security technology development and international cooperation
2/286	2020-01-07	China	National Network Security Publicity Week and network security industrial park
2/272	2020-01-02	Niger	Cybersecurity best practices: case study and recommendation
2/264	2019-12-27	Russian Federation	Protecting children from information harmful to their health and development. Experience of the Russian Federation
RGQ2/TD/13 +Ann.1 (Rev.1)	2019-10-08	Forum of Incident Response and Security Teams (FIRST)	Introduction to incident response for policy makers
RGQ2/196	2019-09-24	Silensec Africa Limited (Kenya)	Using cloud-based cyber ranges and competence frameworks for the delivery of cyber drills
RGQ2/179	2019-09-23	China	China's practice in protecting children's personal information
RGQ2/175	2019-09-19	United Kingdom	Follow up to "case study for the use of Active Cyber Defence on UK Government networks"
RGQ2/156 +Ann.1-3	2019-09-04	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
RGQ2/155	2019-08-23	United Kingdom	Case study of best practices for ransomware risk mitigation in the UK

(continued)

Web	Received	Source	Title
RGQ2/153 +Ann.1-2	2019-08-22	United States	Enhancing the resilience of the Internet and communications ecosystem against botnets and other automated, distributed threats
RGQ2/151	2019-08-22	United States	NIST Framework for Improving Critical Infrastructure Cybersecurity V1.1
RGQ2/146	2019-08-21	Senegal	Overview of the National Cybersecurity School with a regional focus
RGQ2/143	2019-08-23	Brazil	The adoption of the Brazilian General Data Protection Law
RGQ2/135	2019-07-30	Bhutan	Cybersecurity initiatives in Bhutan
RGQ2/134	2019-07-29	State of Palestine, which participates in ITU under Resolution 99 (Rev. Dubai, 2018)	Government Data Exchange
RGQ2/118	2019-06-21	Democratic Republic of the Congo	Securing information and communication networks: Best practices for developing a culture of cybersecurity
2/201	2019-03-08	Côte d'Ivoire	Survey of online activities and Internet use by children in Côte d'Ivoire
2/199 (Rev.1)	2019-03-06	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
2/174	2019-02-07	Côte d'Ivoire	Mapping of cybercrime threats in Côte d'Ivoire
2/173	2019-02-07	Côte d'Ivoire	Presentation of Platform for Combatting Cybercrime (PLCC)
2/172	2019-02-07	NRD Cyber Security (Lithuania)	National and sectorial CSIRT developments as means to strengthen cybersecurity environments, 2019 update
2/168	2019-02-07	Republic of Korea	2019 Comprehensive Cybersecurity Plan for the private sector
2/167	2019-02-07	Symantec Corporation (United States)	The importance of cyber threat intelligence in the definition of national cybersecurity strategies
2/165	2019-02-06	Mexico	Fixed and/or mobile Internet users' perception of cybersecurity
2/156	2019-02-05	China	Work experiences in personal information protection
2/155	2019-02-05	China	Design of evaluation index for network security capability

(continued)

Web	Received	Source	Title
2/154	2019-02-05	China	Experience of Internet governance with the coordinated participation of the whole of society
2/152	2019-02-01	Benin	Cybersecurity in the era of the digital economy in Benin
2/141	2019-01-15	Chad	Digital dividend
2/140	2019-01-15	Chad	Vulnerability of connected TVs
2/136	2019-01-15	Chad	Status of cybersecurity in the Republic of Chad
RGQ2/TD/1	2018-09-24	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for ITU members
RGQ2/79	2018-09-18	Bhutan	Challenges, issues and recommendations from Bhutan: developing country perspective
RGQ2/75	2018-09-18	Namibia	Enforcement of cyber security challenged by cloud services
RGQ2/55	2018-09-10	United Kingdom	Case study for the use of Active Cyber Defence on UK government networks
RGQ2/47	2018-08-31	BDT Focal Point for Question 3/2	Information on two publications issued in 2017: regional review of national activities on child online protection in Europe; and mobile identification: implementation, challenges, and opportunities
RGQ2/39 +Ann.1	2018-08-20	High-Tech Bridge SA (Switzerland)	Cybersecurity awareness and other educative activities to members
RGQ2/32	2018-08-16	Guardtime AS (Estonia)	Towards cyber resilience - the role of national cyber exercises
RGQ2/30	2018-08-15	Brazil	Survey proposal
RGQ2/26	2018-08-14	NRD Cyber Security (Lithuania)	National and sectoral CSIRT developments as means of strengthen cybersecurity environments
RGQ2/25	2018-08-14	Proge-Software (Italy)	Data Privacy and Cloud.be compliant
2/91	2018-04-24	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
2/84	2018-04-23	Japan	Proposal for workshops in 2018-2021 study period
2/82	2018-04-23	Iran University of Science and Technology (Islamic Republic of Iran)	KOVA Project: A best practice for COP implemented in Iran

(continued)

Web	Received	Source	Title
2/75	2018-04-14	A.S. Popov Odessa National Academy of Telecommunications (Ukraine)	ITU Regional Workshop for Europe and CIS on Cybersecurity and Child Online Protection. Conclusions and Recommendations
2/74	2018-04-13	Korea Telecom (Republic of Korea)	Study topics for Question 3/2 in the current study period
2/71	2018-04-11	G3ict	Spammers and phishers who target persons with disabilities
2/66	2018-04-08	Algérie Télécom SPA (Algeria)	Proposals on the content of the (Question 3/2) final report
2/49	2018-03-15	Burundi	Current situation with regard to the Burundian Penal Code in relation to efforts to combat cybercrime
2/41	2018-02-28	Burundi	Cybersecurity, Internet Exchange point and e-commerce in Burundi

Incoming liaison statements for Question 3/2

Web	Received	Source	Title
RGQ2/242	2020-08-31	Council Working Group on Child Online Protection	Liaison statement from the Council Working Group on Child Online Protection (CWG-COP) to ITU-D SG2 on the outcome of the 15th and 16th Meetings of CWG-COP
RGQ2/174	2019-09-18	ITU-T Study Group 17	Liaison statement from ITU-T SG17 to ITU-D SG2 Q3/2 on vulnerability of TVs
2/182 +Ann.1	2019-02-11	ITU-T Study Group 17	Liaison statement from ITU-T SG17 to ITU-D Study Group 2 Question 3/2 on Cybersecurity in Africa (overview and outlook), from Democratic Republic of Congo
RGQ2/62	2018-09-14	ITU-T Study Group 17	Liaison statement from ITU-T SG17 to ITU-D SG2 Q3/2 on collaboration and liaison representative with ITU-D Question 3/2
RGQ2/43	2018-08-27	ITU-T Study Group 13	Liaison statement from ITU-T SG13 to ITU-D SG1 Q3/1 and ITU-D SG2 Q3/2 on inter-sector coordination
RGQ2/3	2018-05-11	ITU-T JCA-IMT2020	Liaison Statement from JCA-IMT2020 to ITU-D Study Groups 1 and 2 on invitation to update the information in the IMT2020 roadmap
2/73	2018-04-13	ITU-T JCA-AHF	Liaison Statement from ITU-T JCA-AHF to ITU-D Study Group 1 Q7/1 and Study Group 2 Q3/2 on JCA-AHF recent meeting reports

(continued)

Web	Received	Source	Title
2/69	2018-04-09	ITU-T Study Group 17	Liaison Statement from ITU-T SG17 to ITU-D SG2 Q3/2 on collaboration and liaison relationship with ITU-D Study Group 2 Question 3/2
2/68	2018-04-09	ITU-T Study Group 17	Liaison Statement from ITU-T SG17 to ITU-D SG2 Q3/2 on best practices in Benin and Senegal
2/67 (Rev.1)	2018-04-09	ITU-T Study Group 17	Liaison Statement from ITU-T SG17 to ITU-D SG2 Q3/2 on new work item X.framcdc "Framework of the creation and operation for a Cyber Defense Center"
2/62	2018-04-03	ITU-T Study Group 17	Liaison Statement from ITU-T SG17 to ITU-D SG2 Question 3/2 on new work item X.framcdc "Framework of the creation and operation for a Cyber Defense Center"
2/46	2018-03-05	ITU-T JCA-IMT2020	Liaison Statement from ITU-T JCA-IMT2020 to ITU-D study groups on invitation to update the information in the IMT2020 roadmap
2/23	2017-11-24	ITU-T Study Group 17	Liaison Statement from ITU-T SG17 to ITU-D SG2 Question 3/2 on an ongoing work item on technical framework for countering telephone service scam
2/10	2017-11-22	ITU-T Study Group 20	Liaison Statement from ITU-T SG20 to ITU-D study groups on work on the combat of counterfeit ICT devices and mobile device theft

Annex 2: List of lessons learned received on Question 3/2

Web	Received	Source	Title
SG2RGQ/272	2020-09-22	United Kingdom	UK case study: Cyber resilience best practice for SMEs

The UK Government provides targeted support to small and medium-sized enterprises (SMEs) to help them navigate complicated standards to better understand how to mitigate cyberrisk. This support is designed specifically for organizations who are not aware of the cyberthreat and have limited resources, both financially and in terms of technical capability. Lessons learned include the following:

- Clear and consistent cyberrisk management messaging is crucial. Critically, **awareness campaigns** should not just explain *what* businesses need to do and *how* they can actually carry out the action by pointing to government advice, guidance and support, but should draw attention to *why* they should do it.
- **Advice and guidance** is most effective when it is non-technical, size-specific and easy to access. Government and law enforcement should use national, regional and local networks, and work in partnership with key industry bodies, to identify levers and business touchpoints that can be used to amplify messaging, and ensure advice and guidance reaching SMEs.
- The creation of a government-backed **certification scheme** can be an effective intervention to support SMEs to improve their cybersecurity. The certification scheme can:

  - be quickly and effectively delivered by a single supplier if the government can outline the technical controls and/or minimum standards that should be covered;
  - evolve to continue to meet the needs of SMEs and address the changing threat landscape;
  - better ensure organizations remain compliant through having a certification expiry date and requiring annual recertification.

Web	Received	Source	Title
SG2RGQ/235	2020-08-20	United Kingdom	UK Government Digital Service (GDS) Global Digital Marketplace Programme

Challenges

A range of interconnected challenges face governments in relation to traditional approaches to public procurement of ICTs, which is typically:

- neither understanding nor meeting the needs of users
- task oriented, risk averse and inflexible
- isolated from what happens:
    - 'before' (strategic planning, investment appraisals, early market engagement)
    - 'after' (service delivery, monitoring and evaluation, supplier relationship management)
- hidden from public scrutiny due to the poor quality, inconsistency, incompleteness and poor availability of data.

User-centred design approaches

Since GDS was established in 2011, it has incubated, embedded and mainstreamed new standards-based approaches to government transformation.

These approaches were first conceptualized by the Government Design Principles,[163] published in April 2012.

Since then, GDS and the government and UK public sector more broadly have been incrementally applying these principles to redesign and improve services, organizational structures, governance approaches, etc. This includes public procurement.

Social Purpose Digital Commissioning

Focus on culture, mindset, collaboration and capability, by:

- understanding users' needs
- being clear about the problems you are trying to overcome (e.g. legacy ICT, system vulnerabilities, capability and capacity, governance and accountability, etc.) to meet users' needs
- being outcome-oriented (rather than solution-oriented), experimental and flexible, making small incremental investments to try out different approaches to address users' problems, learning quickly and iteratively
- being multidisciplinary and collaborative coalition builders, advocating for systemic change through communities of practice
- engaging throughout the end-to-end lifecycle of delivery - the 'before' and 'after' of procurement
- being open to public scrutiny through deliberative participation of civil society, enabled by structured, quality, consistent, complete and published open data.

[163] UK Government. Guidance. Government Design Principles. April 2012.

Web	Received	Source	Title
SG2RGQ/215	2020-07-27	Brazil	*#ConexãoSegura* (#SafeConnection) Awareness Campaigns

The campaign around personal data protection on the Internet reinforced the importance of telling consumers how to protect themselves in the digital environment. The interactions of consumers on digital media and on the website revealed that many of them have a number of doubts about what is fraud or scam - especially when it involves cash prizes, in addition to not knowing what to do when they are victims of these situations. It is also important to advise people not to post or publish personal data (surprisingly many people do not know what can happen). In the next initiative, it would be interesting to expand the dissemination of materials further in order to reach a wider audience.

Web	Received	Source	Title
SG2RGQ/214	2020-07-27	Brazil	Brazilian National Cyberdrill - Cyber Guardian Exercise

The exercise started with two national critical infrastructure (NCI) sectors and evolved in its second edition to a broader and more complex exercise process. The exercise continues to evolve, and for its third edition (cancelled due to the COVID-19 pandemic) it was planned to include six NCI sectors and to add an international cooperation component to the exercise.

Web	Received	Source	Title
2/325	2020-02-08	Democratic Republic of the Congo	*La sécurité numérique en République Démocratique du Congo*

Turn cybersecurity in the Democratic Republic of the Congo into a lever for integration, protection, good governance, economic growth and social progress.

This vision will make a significant contribution to building the country's capacity in its digital transformation (circulation of information, data economy, growth economy, transparency and traceability, interoperability of information systems, etc.). It will allow digitalization to become a key driver for modernizing the State, promoting economic growth and fostering social progress.

Web	Received	Source	Title
2/336	2020-02-11	United Kingdom	Case study of best practices for securing customer Internet of Things in the UK

A significant proportion of IoT devices do not have basic cybersecurity features built into them. Following 18 months of collaboration with industry and experts at the UK's National Cyber Security Centre (NCSC), the Department for Digital, Culture, Media and Sport (DCMS) published the Code of Practice (CoP) for Consumer IoT Security in October 2018. The 13 voluntary guidelines, as outlined in the 2018 CoP, provide a much-needed baseline for IoT devices that manufacturers should embed into their products to make them 'secure by design'.

These include:

- No default passwords
- Implement a vulnerability disclosure policy
- Keep software updated
- Securely store credentials and security-sensitive data
- Communicate securely
- Minimize exposed attack surfaces
- Ensure software integrity
- Ensure personal data are protected
- Make systems resilient to outages
- Monitor system telemetry data
- Make it easy for consumers to delete personal data
- Make installation and maintenance of devices easy
- Validate input data.

These guidelines are outcome-focused as opposed to being prescriptive, which gives companies the space to come up with innovative solutions and appropriate ways to secure their products. Some devices might require enhanced security that is not included on this list and, as such, retailers and manufacturers are encouraged to secure their devices accordingly and seek solutions beyond the 13 guidelines. Action on the first three guidelines will bring largest security benefits in the short term.

Web	Received	Source	Title
2/331	2020-02-11	Keio University (Japan)	Proposed text for consideration of security issues for ICT accessibility

This document describes the consideration and implementation of cybersecurity measures for persons with disabilities, especially those with hearing difficulties, such as telecommunication relay service and remote captioning, to enhance accessibility to information and communication services.

Web	Received	Source	Title
SG2RGQ/134	2019-07-29	State of Palestine	Government Data Exchange

The central server issues certificates to security servers and provides a list of authenticated certificates to the systems connected to the Government Data Exchange. In addition, the central security server maintains encrypted activity data (hash logs) from the security servers to enable a series of e-service uses to be built subsequently, if necessary. If one of the parties to the service denies sending or receiving certain information, the service provider and user logs are compared with the encrypted copy in the central server. This method allows the integrity of security server logs to be checked, as it is impossible to change the log without it subsequently being detected.

The terms of the data-sharing process are defined by a memorandum of understanding signed by the two parties sharing the data and the Ministry of Telecommunications and Information Technology (MTIT), as third-party system operator. The memorandum includes an annex on the obligations of the parties, an annex on controls, standards and the duties and rights of each party, and an annex on the data which the two parties agree to share.

The system allows a connected ministry to determine which other connected institutions may access and read its data and the level of data that may be accessed. This is done by means of a control window on the ministry's own security server, enabling it to grant access rights to any of its services to the institutions it wishes.

Encrypted data are shared directly through secure servers from one information system to another. They do not pass through the central system and cannot be displayed there. The central system only has statistical information on the data shared.

Using this approach, the system facilitates the secure sharing of data between institutions, enabling them to share data between one another. It has also made it easier for the public to access services currently available G2G, by only going to one institution where the service involves more than one. MTIT is currently working to develop this mechanism and to provide services to the public directly via applications being developed.

Web	Received	Source	Title
SG2RGQ/146	2019-08-21	Senegal	Overview of the National Cybersecurity School with a regional focus

- Enhancing international cooperation, particularly between developed and developing countries.
- The school's regional nature helps to enhance cooperation among African countries.
- Covering all aspects of cybersecurity in both initial and continuing training.
- As cybersecurity is a prerequisite for the Digital Senegal 2025 Strategy (SN2025), classes have begun at the offices of the National School of Administration (ENA) while construction of the school's own premises is being completed at Diamniadio, 20 km from Dakar.
- The school will be the final element in the system for information system security and cybersecurity already in place.
- Boosting the fight against cybercrime in Africa.

Web	Received	Source	Title
SG2RGQ/151	2019-08-22	United States	NIST Framework for Improving Critical Infrastructure Cybersecurity V1.1

The recent update process to develop Version 1.1 of the Framework demonstrates an example of a good process for stakeholder engagement to ensure the Framework remains a useful tool for managing cybersecurity risk.

Web	Received	Source	Title
SG2RGQ/155	2019-08-23	United Kingdom	Case study of best practices for ransomware risk mitigation in the UK

A recent advisory on ransomware from the National Cyber Security Centre (NCSC) recommends the following risk-mitigation techniques:

- Keep devices and networks up to date (e.g. prompt updating and patching, and regular scans)
- Prevent and detect lateral movement in your enterprise network
- Segment networks
- Set up a security monitoring capability
- Whitelist applications
- Use antivirus
- Back up files.

The full advisory and detailed list of recommendations can be found at: https://www.ncsc.gov.uk/news/ongoing-threat-organisations-ransomware

Protecting your organization from ransomware: https://www.ncsc.gov.uk/guidance/protecting-your-organisation-ransomware

Mitigating malware: https://www.ncsc.gov.uk/guidance/mitigating-malware

Unfortunately, it is not a question of 'if' but 'when' a cyberattack will occur. In the event an attack does take place, cooperation between the public and private sectors is key to understanding the threat and coordinating a quick and effective response to mitigate the impact of an attack. In the event of an attack, organizations are advised to contact the National Crime Agency, NCSC's Cyber Incident Response, or Cyber Security Information Sharing Partnership (CiSP). NCSC led the UK's response to the WannaCry attack and worked in collaboration with the National Crime Agency (NCA). Over the course of an incident, NCSC publishes statements and guidance for large organizations as well as home users and small businesses. Up-to-date information is announced via the NCSC Twitter account (@NCSC).

Web	Received	Source	Title
SG2RGQ/196	2019-09-24	Silensec Africa Limited (Kenya)	Using cloud-based cyber ranges and competence frameworks for the delivery of cyber drills

This contribution recommends the use of cyberrange technology (cloud-based – public or private cloud) and competency frameworks in the development and delivery of new generation cyberdrills.

Web	Received	Source	Title
2/201	2019-03-08	Côte d'Ivoire	Survey of online activities and Internet use by children in Côte d'Ivoire

- De-dramatize prevention by banishing the anxiety-provoking approach. Internet prevention can be part of a fear culture. However, this increases the anxiety of parents who are already worried about a technology they do not understand well, thereby undermining the extraordinary learning tool that is the Internet.
- Encourage educational programmes aimed at developing best practices in content management and raising children's awareness of responsible use of the Internet.
- Put an Internet portal online in order to provide children, adolescents, parents and teachers with an educational base.
- Involve all stakeholders in community-awareness activities: government agencies, the private Internet sector, NGOs, community groups and the general public.

Web	Received	Source	Title
2/174	2019-02-07	Côte d'Ivoire	Mapping of cybercrime threats in Côte d'Ivoire

Statistics should be collected on complaints and damages (financial, moral).

Web	Received	Source	Title
2/173	2019-02-07	Côte d'Ivoire	Presentation of Platform for Combating Cybercrime (PLCC)

- Development of partnerships between bodies responsible for combating cybercrime and the police in developing countries
- Awareness-raising in schools
- Collaboration with equivalent organizations in other countries.

Web	Received	Source	Title
SG2RGQ/26 2/172	2018-08-14 2019-02-07	NRD Cyber Security (Lithuania)	National and sectoral CSIRT developments as means to strengthen cybersecurity environments (2018 +2019 update)

For national digital security success, CSIRTs should focus substantial energy on broad facilitation for developing additional independent capabilities – in industries, professional communities, education centres, research, events, meet-ups and conferences, private and internal CSIRTs.

Web	Received	Source	Title
2/167	2019-02-07	Symantec Corporation (United States)	The importance of cyber threat intelligence in the definition of national cybersecurity strategies

- Establish and adopt situation awareness and threat intelligence policies.
- Develop incident analysis and response capabilities - establish CERTs.
- Develop collaboration with the private sector and information-sharing policies (public-private partnerships).

Web	Received	Source	Title
2/152	2019-02-01	Benin	Cybersecurity in the era of the digital economy in Benin

Benin calls on ITU-D Study Group 2 to support:

- the establishment of a national CERT in Benin to enhance the level of trust in cyberspace;
- the building up of a common African security and defence policy;
- the creation of a panel of eminent personalities to reflect on Africa's role in regard to security;
- the establishment of a CERT-AFR (for Africa) along the lines of CERT-EU (for the European Union);
- a coordinated effort to avoid disparities between the strategies adopted and means deployed by Member States in terms of military cyberdefence capabilities;
- regulators and ICT authorities as they seek to:
  - adopt measures designed to enhance the security of information systems and networks;
  - create reliable digital identities;
  - protect minors and vulnerable groups; and
  - foster transparency.

Web	Received	Source	Title
SG2RGQ/25	2018-08-14	Proge-Software [*SME pilot*] (Italy)	Data Privacy and Cloud - be compliant

General Data Protection Regulation (GDPR)

General Data Protection Regulation (GDPR) (EU) 2016/679 governs data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). It also addresses the export of personal data outside the EU and EEA. The GDPR aims primarily to give control to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying regulation within the EU. Superseding Data Protection Directive 95/46/EC, the regulation contains provisions and requirements pertaining to the processing of personally identifiable information (personal data) of individuals (formally called data subjects in the GDPR) inside the European Union, and applies to an enterprise that is established in the EU or – regardless of its location and the data subjects' citizenship – that is processing the personal data of people inside the EU. Controllers of personal data must put in place appropriate technical and organizational measures to implement the data-protection principles. Severe penalties are applied to violators.

Cloud computing

In computer science, cloud computing describes a type of outsourcing of computer services, similar to the way in which electricity supply is outsourced. Users can simply use it. They do not need to worry where the electricity is from, how it is made, or how it is transported. Periodically they pay for what they have consumed. The idea behind cloud computing is similar: The user can simply use storage, computing power or specially crafted development environments without having to worry how these work internally. Cloud computing is usually Internet-based computing. According to a paper published by IEEE Internet Computing in 2008, "*Cloud computing is a paradigm in which information is permanently stored in servers on the Internet and cached temporarily on clients that include computers, laptops, handhelds, sensors, etc.*".

Web	Received	Source	Title
SG2RGQ/32	2018-08-16	Guardtime AS [*SME pilot*] (Estonia)	Towards cyber resilience – the role of national cyber exercises

Cyberexercises are essential to achieving sustainable cyberresilience. Cyberexercises are different from training, and must be customized, realistic and engaging. Governments should consider developing a programme to govern cyberresilience, covering education, training and cyberexercises ranging from localized events to customized national-scale exercises conducted on a regular basis.

Web	Received	Source	Title
2/71	2018-04-11	G3ict	Spammers and phishers who target persons with disabilities

1. Contact the service provider to inform it of the highjacking of your e-mail address.
2. Try to give information on the spammer's/hacker's contact details with an example e-mail, e.g. by forwarding the suspect e-mail to its fraud section.
3. Ask to have your violated e-mail blocked.
4. Change your e-mail address.
5. Let your friends and contacts know you have been hacked and give them the new address.
6. Do not click on any web addresses unless you have verified it is in fact from a known source.

Web	Received	Source	Title
2/41	2018-02-28	Burundi	Cybersecurity, Internet exchange point and e-commerce in Burundi
Security of IT data and of communication networks in order to ensure high-quality services is the pillar of ICT-sector development. A legal and regulatory framework for cybersecurity in our country is an essential tool for implementing all aspects of data security. The introduction of an Internet exchange point facilitates local communications and reduces latency times and associated costs. Lastly, domain name management provides facilities for investors. Data security will thus enable us to ensure reliable e-transactions and retain our customers.			

Office of the Director
International Telecommunication Union (ITU)
Telecommunication Development Bureau (BDT)
Place des Nations
CH-1211 Geneva 20
Switzerland

Email: bdtdirector@itu.int
Tel.: +41 22 730 5035/5435
Fax: +41 22 730 5484

Office of Deputy Director and Regional Presence
Field Operations Coordination Department (DDR)
Place des Nations
CH-1211 Geneva 20
Switzerland

Email: bdtdeputydir@itu.int
Tel.: +41 22 730 5131
Fax: +41 22 730 5484

Digital Networks and Society (DNS)

Email: bdt-dns@itu.int
Tel.: +41 22 730 5421
Fax: +41 22 730 5484

Digital Knowledge Hub Department (DKH)

Email: bdt-dkh@itu.int
Tel.: +41 22 730 5900
Fax: +41 22 730 5484

Partnerships for Digital Development Department (PDD)

Email: bdt-pdd@itu.int
Tel.: +41 22 730 5447
Fax: +41 22 730 5484

Africa

Ethiopia

International Telecommunication
Union (ITU) Regional Office
Gambia Road
Leghar Ethio Telecom Bldg. 3rd floor
P.O. Box 60 005
Addis Ababa
Ethiopia

Email: itu-ro-africa@itu.int
Tel.: +251 11 551 4977
Tel.: +251 11 551 4855
Tel.: +251 11 551 8328
Fax: +251 11 551 7299

Cameroon

Union internationale des
télécommunications (UIT)
Bureau de zone
Immeuble CAMPOST, 3e étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé
Cameroon

Email: itu-yaounde@itu.int
Tel.: + 237 22 22 9292
Tel.: + 237 22 22 9291
Fax: + 237 22 22 9297

Senegal

Union internationale des
télécommunications (UIT)
Bureau de zone
8, Route des Almadies
Immeuble Rokhaya, 3e étage
Boîte postale 29471
Dakar - Yoff
Senegal

Email: itu-dakar@itu.int
Tel.: +221 33 859 7010
Tel.: +221 33 859 7021
Fax: +221 33 868 6386

Zimbabwe

International Telecommunication
Union (ITU) Area Office
TelOne Centre for Learning
Corner Samora Machel and
Hampton Road
P.O. Box BE 792
Belvedere Harare
Zimbabwe

Email: itu-harare@itu.int
Tel.: +263 4 77 5939
Tel.: +263 4 77 5941
Fax: +263 4 77 1257

Americas

Brazil

União Internacional de
Telecomunicações (UIT)
Escritório Regional
SAUS Quadra 6 Ed. Luis Eduardo
Magalhães,
Bloco “E”, 10º andar, Ala Sul
(Anatel)
CEP 70070-940 Brasilia - DF
Brazil

Email: itubrasilia@itu.int
Tel.: +55 61 2312 2730-1
Tel.: +55 61 2312 2733-5
Fax: +55 61 2312 2738

Barbados

International Telecommunication
Union (ITU) Area Office
United Nations House
Marine Gardens
Hastings, Christ Church
P.O. Box 1047
Bridgetown
Barbados

Email: itubridgetown@itu.int
Tel.: +1 246 431 0343
Fax: +1 246 437 7403

Chile

Unión Internacional de
Telecomunicaciones (UIT)
Oficina de Representación de Área
Merced 753, Piso 4
Santiago de Chile
Chile

Email: itusantiago@itu.int
Tel.: +56 2 632 6134/6147
Fax: +56 2 632 6154

Honduras

Unión Internacional de
Telecomunicaciones (UIT)
Oficina de Representación de
Área
Colonia Altos de Miramontes
Calle principal, Edificio No. 1583
Frente a Santos y Cía
Apartado Postal 976
Tegucigalpa
Honduras

Email: itutegucigalpa@itu.int
Tel.: +504 2235 5470
Fax: +504 2235 5471

Arab States

Egypt

International Telecommunication
Union (ITU) Regional Office
Smart Village, Building B 147,
3rd floor
Km 28 Cairo
Alexandria Desert Road
Giza Governorate
Cairo
Egypt

Email: itu-ro-arabstates@itu.int
Tel.: +202 3537 1777
Fax: +202 3537 1888

Asia-Pacific

Thailand

International Telecommunication
Union (ITU) Regional Office
Thailand Post Training Center
5th floor
111 Chaengwattana Road
Laksi
Bangkok 10210
Thailand

Mailing address:
P.O. Box 178, Laksi Post Office
Laksi, Bangkok 10210, Thailand

Email: ituasiapacificregion@itu.int
Tel.: +66 2 575 0055
Fax: +66 2 575 3507

Indonesia

International Telecommunication
Union (ITU) Area Office
Sapta Pesona Building
13th floor
Jl. Merdan Merdeka Barat No. 17
Jakarta 10110
Indonesia

Mailing address:
c/o UNDP – P.O. Box 2338
Jakarta 10110, Indonesia

Email: ituasiapacificregion@itu.int
Tel.: +62 21 381 3572
Tel.: +62 21 380 2322/2324
Fax: +62 21 389 5521

CIS

Russian Federation

International Telecommunication
Union (ITU) Regional Office
4, Building 1
Sergiy Radonezhsky Str.
Moscow 105120
Russian Federation

Email: itumoscow@itu.int
Tel.: +7 495 926 6070

Europe

Switzerland

International Telecommunication
Union (ITU) Office for Europe
Place des Nations
CH-1211 Geneva 20
Switzerland
Email: eurregion@itu.int
Tel.: +41 22 730 5467
Fax: +41 22 730 5484

International Telecommunication Union
Telecommunication Development Bureau
Place des Nations
CH-1211 Geneva 20
Switzerland

ISBN 978-92-61-34101-5

9 789261 341015

Published in Switzerland
Geneva, 2021
Photo credits: Shutterstock