ITUPublications

International Telecommunication Union
Development Sector

Output Report on ITU-D Question 3/2

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

Study period 2022-2025

Output Report on ITU-D Question 3/2

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

Study period 2022-2025

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 2022-2025

ISBN 978-92-61-41101-5 (Electronic version)
ISBN 978-92-61-41111-4 (EPUB version)

Acknowledgements

The study groups of the International Telecommunication Union 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 by the World Telecommunication Development Conference (WTDC). The ITU membership, assembled at WTDC-22 in Kigali in June 2022, agreed that, for the period 2022-2025, Study Group 2 would deal with seven Questions within the overall scope of digital transformation.

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 Fadel Digham (Arab Republic of Egypt), as Chair, supported by the following Vice-Chairs: Mr Abdelaziz Alzarooni (United Arab Emirates), Ms Zainab Ardo (Federal Republic of Nigeria), Mr Javokhir Aripov (Republic of Uzbekistan), Ms Carmen-Mădălina Clapon (Romania), Mr Mushfig Guluyev (Republic of Azerbaijan), Mr Hideo Imanaka (Japan), Ms Mina Seonmin Jun (Republic of Korea), Mr Mohamed Lamine Minthe (Republic of Guinea), Mr Víctor Antonio Martínez Sánchez (Republic of Paraguay), Ms Alina Modan (Romania),[1] Mr Diyor Rajabov (Republic of Uzbekistan),[1] Mr Tongning Wu (People's Republic of China), and Mr Dominique Würges (France).

The report was developed under the leadership of the Co-Rapporteurs for Question 3/2, Ms Vanessa Copetti Cravo (Federative Republic of Brazil), Ms Nicole Darabian (United Kingdom of Great Britain and Northern Ireland), and Ms Jabin Vahora (United States of America),[1] in collaboration with the following Vice-Rapporteurs: Mr Damnam K. Bagolibe (Togolese Republic), Mr Daniel Batty (Access Partnership Limited),[1] Ms Maria Bolshakova (Russian Federation),[1] Mr Tommaso De Zan (Access Partnership Limited), Mr Idrissa Diallo (Republic of Guinea), Mr Sidy Mouhamed Fall (Republic of Senegal), Mr Álvaro García (Axon Partners Group), Mr Doğukan Ömer Gür (Republic of Türkiye), Mr Prachish Khanna (Republic of India), Mr Teng Ma (China International Telecommunication Construction Corporation), Mr Rodgers Mumelo (Republic of Kenya), Ms Uliana Stoliarova (Russian Federation), Mr Samuel Tew (Axon Partners Group),[1] Ms Xinxin Wan (People's Republic of China), Ms Kacie Yearout (United States of America), and Mr Jaesuk Yun (Republic of Korea).

Special thanks go to the chapter lead authors for their dedication, support and expertise.

This report has been prepared with the support of the ITU-D Question 3/2 focal points, editors, the publication production team and the ITU-D Study Group 2 secretariat.

[1] Stepped down during the study period.

Table of contents

List of figures and boxes

Figures

Boxes

Executive summary

The ITU-D Question 3/2 Output Report for the 2022-2025 study period represents a concerted effort to draw from national experiences and practices in cybersecurity from around the globe. The report serves as a resource that can assist countries in formulating their strategies for developing a robust cybersecurity culture. The report considers and reflects the contributions from ITU members, as well as discussions from workshops held during the study period, reflecting a diverse range of perspectives and experiences that aim to secure information and communication networks.

In an era where digital technologies are deeply intertwined into the fabric of daily life and the backbone of economies worldwide, the report acknowledges the heightened vulnerability that individuals, organizations, and nations face, against a backdrop of increasingly sophisticated cyber threats. Cybersecurity is no longer a niche concern but a foundational element for digital transformation and developments, demanding a high priority input from all stakeholders, including governments, private sector, individuals, and academia. Globally, cyber insecurity is ranked as the fourth most severe short-term risk, according to the Global Risks Report 2024, from the World Economic Forum.[2]

In addition to ITU and ITU membership initiatives and resources mentioned in this report, it is important to recognize that there are also a number of global initiatives aimed at sharing cybersecurity information and good practices. These initiatives are intended to support countries and various stakeholders in their cybersecurity journey as it can be difficult for developing countries, especially least developed countries (LDCs), to find and access cybersecurity information. In this context, two comprehensive resources, mentioned during this study cycle, and that can be of benefit to ITU Member States, should be noted: the Cyber Policy Portal from the United Nations Institute for Disarmament Research (UNIDIR),[3] and the Knowledge Portal for Cyber Capacity Building from the Global Forum on Cyber Expertise (GFCE).[4]

Another relevant resource, referred to several times in this report, is the ITU Global Cybersecurity Index (GCI),[5] which measures the commitment of countries to cybersecurity across five fundamental pillars: legal, technical, organizational, capacity development, and cooperation measures. The GCI was launched by ITU in 2015 and has been continuously improved to serve as an assessment, awareness-raising, and capacity building tool, that assists countries in their journey to develop and implement their cybersecurity capabilities.

This report is positioned as a resource that provides up-to-date thinking and practices, informed by the ever dynamic and evolving threat landscape, offering a snapshot of the current state of cybersecurity, and laying down a strategic path for future developments.

---

2 https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf
3 https://cyberpolicyportal.org/
4 https://cybilportal.org/
5 https://www.itu.int/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx

Here the structure of the report is presented, with each chapter focusing on a distinct aspect of cybersecurity:

- Chapter 1 addresses the pivotal human aspect of cybersecurity, emphasizing the pressing need for significant investments in users' awareness, and the education and training of the cybersecurity workforce. This chapter underscores the critical demand for skilled cybersecurity professionals capable of managing the complexities of contemporary digital threats, and urges countries to prioritize educational programmes and recruitment plans to cultivate a competent and resilient cybersecurity workforce, as well as to prioritize awareness as a key element to promote a culture of cybersecurity.
- Chapter 2 shifts focus to cybersecurity assurance practices which are critical in protecting networks, systems, and data from malicious activities. This chapter assesses diverse methodologies, controls, guidelines, and standards adopted across the globe that can help prevent and mitigate the risk of cyberattacks.
- Chapter 3 highlights the crucial function of cybersecurity incident response teams (CIRTs) in safeguarding vital infrastructures. It presents successful models for incident response and underscores the significance of establishing and developing CIRTs, as well as coordination between CIRTs.
- Chapter 4 evaluates the development and execution of national cybersecurity strategies. This chapter details the importance of harmonizing cybersecurity strategies with overarching digital transformation, national security and economic agendas, to bolster digital resilience.
- Chapter 5 explores efforts to secure 5G networks. Amidst the global challenges of 5G networks deployment, this chapter highlights policies, regulatory frameworks and proactive industry actions to help mitigate 5G cybersecurity threats.
- Chapter 6 investigates the increasing use of sophisticated smishing tactics by cybercriminals to deceive users via short message service (SMS), underscoring the necessity for a collective approach encompassing government regulations, industry initiatives, and heightened public awareness to protect consumers and uphold the reliability of communication networks.

Supplementing this report are annexes that provide additional resources, including detailed contributions from ITU members presented in this cycle, and a summary of ITU-D ongoing cybersecurity projects and programmes. These annexes offer invaluable insights and serve as foundational materials for stakeholders seeking to deepen their understanding of cybersecurity and its critical role in the digital age.

In essence, the ITU-D Question 3/2 Output Report for the 2022-2025 study period, is a strategic blueprint for building a high level of cybersecurity across ITU membership. It is a call to action for a unified approach to securing our digital futures, emphasizing the importance of awareness, education, strategy development, CIRTs capabilities, policies and strategies, and international cooperation to navigate and mitigate the complexities of the cybersecurity challenges towards digital transformation.

Abbreviations and acronyms

Abbreviation	Term
2G	second generation mobile technology
3G	third generation mobile technology
3GPP	Third Generation Partnership Project
4G	fourth generation mobile technology
5G	fifth generation mobile technology[6]
CI	critical infrastructure
CIRT	cybersecurity incident response team
CISA	Cybersecurity and Infrastructure Security Agency
COP	child online protection
ENISA	European Union Agency for Cybersecurity
ETSI	European Telecommunications Standards Institute
EU	European Union
FIRST	Forum of Incident Response and Security Teams
GCI	global cybersecurity index
GFCE	Global Forum on Cyber Expertise
GSMA	GSM Association
ICTs	information and communication technologies
IoT	Internet of Things
ITU	International Telecommunication Union
ITU-D	ITU Telecommunication Development Sector
ITU-R	ITU Radiocommunication Sector
ITU-T	ITU Telecommunication Standardization Sector
LDCs	least developed countries
NESAS	Network Equipment Security Assurance Scheme

[6] While care was taken in this document to properly use and refer to the official definition of IMT-generations (see Resolution ITU-R 56, "*Naming for International Mobile Telecommunications*"), parts of this document contain material provided by the membership which refers to the frequently used market names "xG". This material cannot necessarily be mapped to a specific IMT-generation, as the underlying criteria from the membership are not known, but in general, IMT-2000, IMT-Advanced, IMT-2020 and IMT-2030 are known as 3G/4G/5G/6G, respectively.

(continued)

Abbreviation	Term
NIST	National Institute for Standards and Technology
OECD	Organisation for Economic Co-operation and Development
RAN	radio access network
SDN	software-defined network
SDO	standards development organization
SG17	Study Group 17 of ITU-T
SMS	short message service
UNIDIR	United Nations Institute for Disarmament Research

Chapter 1 – Promotion of awareness-raising for users and capacity building regarding cybersecurity

Implementing robust cybersecurity skills and awareness programmes is crucial to ensure that we can continue to safely reap the benefits of digitalization. Cybersecurity initiatives not only help to mitigate the risks associated with phishing and other cyber threats but also contribute to building a skilled workforce capable of addressing the complex challenges of the digital age. This chapter explores key elements and notable examples, suggesting a way forward for countries wishing to follow the same path.

1.1 Cybersecurity awareness-raising

Human error remains a significant factor in cybersecurity breaches, with studies indicating that over 88 per cent of such incidents involve some form of human error.[7] This underscores the need for comprehensive awareness programmes that go beyond technical solutions and address the human element of cybersecurity.

Cybersecurity awareness refers to the strategic approach of educating individuals, organizations, and communities about cyber risks and good practices for protecting digital assets and information. The primary goal of cybersecurity awareness raising initiatives is to cultivate a security-conscious culture and empower people to recognize, prevent, and respond to cybersecurity risks effectively. Awareness programmes may encompass various methods and tools such as training programmes, simulated phishing exercises, gamification, and micro-learning modules. Key topics often covered in these initiatives range from social engineering and phishing awareness, to password management, data protection, and safe use of mobile devices and social media.

The impact of well-implemented cybersecurity awareness programmes can be substantial.[8] Organizations that prioritize awareness training often see significant reductions in successful phishing attacks and overall improvements in their security posture, with studies showing an up to 70 per cent decrease in successful attacks.[9] Investing in cybersecurity awareness also yields a high return on investment (ROI), with studies indicating that even the most modest training programmes can produce a seven-fold ROI.[10] Moreover, these programmes contribute to building a culture of cybersecurity that extends beyond the workplace, helping individuals also become responsible "cybercitizens" in their personal lives. Furthermore, cybersecurity awareness is essential for compliance with industry regulations and data protection laws, such as the revised "Security of network and information systems (NIS2)" Directive in the European

7 https://blog.knowbe4.com/88-percent-of-data-breaches-are-caused-by-human-error
8 https://www.sciencedirect.com/science/article/pii/S0167404823004959
9 https://keepnetlabs.com/blog/2024-security-awareness-training-statistics; https://www.knowbe4.com/press/knowbe4-analysis-finds-security-awareness-training-and-simulated-phishing-effective-in-reducing-cybersecurity-risk
10 https://blog.usecure.io/does-security-awareness-training-work; https://ostermanresearch.com/wp-content/uploads/2021/01/ORWP_0313-The-ROI-of-Security-Awareness-Training-August-2019.pdf

Union. Many sectors require organizations to implement security training programmes to meet regulatory standards and avoid potential fines or legal consequences.[11]

Data from the global cybersecurity index (GCI) indicates that 152 countries ran cybersecurity awareness campaigns targeting the general population between 2021 and 2024.[12] ITU Member States have implemented several initiatives to increase awareness about cybersecurity threats. These initiatives include comprehensive programmes targeting various segments of the population. Some projects focus specifically on cybercrime and fraud prevention, while others use a variety of online media to promote cyber hygiene practices among the population.

An example of a comprehensive programme tailored to various segments of the population is the **Russian Federation** "Cyber Hygiene Program". Launched in August 2022, this is a comprehensive three-year initiative, aimed at enhancing cybersecurity awareness among Russian Federation citizens. To enable more targeted and effective communication, the programme segmented the population into three age groups: children and adolescents (12-18 years old), adults (18-45 years old), and adults (45+). For the 12-18 age group, which receives special attention due to their vulnerability to cyber threats, two key projects were implemented:

- The "Cyberbullying" project provides advice for victims, aggressors, and observers, emphasizing the importance of responding to cyberbullying with humour and healthy indifference.
- The "Upgrade your protection skills" project focuses on educating children about scams in online gaming environments.

For adults aged 18-45, the programme includes projects such as:

- "Cyber-healthy lifestyle,"
- "Complex simple passwords," and
- "Learn your role."

These initiatives cover topics including mobile device protection, phishing prevention, password security, and telephone fraud awareness. The programme also addresses the needs of adults over 45, with a focus on protecting them from telephone fraud. Additionally, a specialized course aims to improve information security literacy among civil servants. A Russian Federation-wide study conducted in 2022, revealed an overall cyber literacy index of 48.2 out of 100, covering topics such as anti-virus protection, safe Internet use, and personal data security. The Cyber Hygiene Program is designed to be updated annually, ensuring it remains relevant to emerging digital threats and evolving population needs.[13]

In **Republic of Côte d'Ivoire**, a cybersecurity awareness programme, here with a specific focus on cybercrime, was among a number of cybersecurity awareness and training initiatives implemented through the principal Côte d'Ivoire cybersecurity institutions. The Platform for Combating Cybercrime (PLCC), conducts awareness campaigns in educational institutions, including schools and universities, as well as financial and religious institutions, publishing educational content and information about cybercriminal arrests on social media. The CI-CERT *(Côte d'Ivoire - computer emergency response team)*, the focal point of national cybersecurity, offers a specialized training programme called "DIGISEC" designed for companies and

[11] https://www.cybsafe.com/blog/7-reasons-why-security-awareness-training-is-important/
[12] https://www.itu.int/epublications/publication/global-cybersecurity-index-2024
[13] ITU-D SG2 Document 2/71 from the Russian Federation

institutions to enhance workplace digital security awareness. Another notable recent initiative, deployed during the African Cup of Nations 2024, was CyberCAN23. This cybersecurity system, managed by CI-CERT, focused on raising awareness about digital platform scams, and particularly phishing fraud. The campaign utilized social media platforms, television, and radio to disseminate cybersecurity information. The country also runs a nationwide awareness campaign called "*En ligne tous responsables*" (Online we are all responsible) across various towns and cities.[14]

Republic of Rwanda has implemented several initiatives to enhance awareness, education, and training in cybersecurity, including the National Cyber Security Awareness and Training Program, which promotes cybersecurity awareness for Internet users while also developing cybersecurity professionals to support public and private institutions in protecting critical systems against cyber threats.[15]

Focusing on cyber fraud prevention, **China** has worked to build a society-wide, multi-dimensional "anti-fraud network", encouraging the installation of the National Anti-Fraud Centre app, and raising awareness for the adoption of cyber hygiene measures across a range of targeted demographics, such as students, elderly people, farmers, etc.[16]

Finally, in **Brazil** an initiative focused on enhancing the cybersecurity hygiene practices of the population, relies on online communication tools such as 'YouTube'. Brazil has implemented cybersecurity hygiene initiatives through the national telecommunications agency, Anatel. As part of its 2023-2027 strategic planning, Anatel has created a dedicated portal for digital fraud prevention and cybersecurity hygiene, offering information about common digital threats, and prevention strategies. The agency regularly conducts awareness events with partners and maintains a specialized cybersecurity playlist on its YouTube channel. Other notable initiatives include #OctoberCyberSafe campaigns in October 2023, and October 2024, and Safer Internet Day events in February 2024, and February 2025.[17]

1.2 Capacity building in cybersecurity education and training

The Global Cybersecurity Outlook 2025, a report produced by the World Economic Forum, highlighted a growing cybersecurity skills shortage, with the cybersecurity skills gap growing by 8 per cent since the previous (Global Cybersecurity Outlook 2024) report. Two out of three organizations reported critical cybersecurity skills gaps, impeding them from meeting their security requirements. The report emphasizes the urgent need for initiatives to address this skills gap, including training, reskilling, and efforts to recruit and retain cybersecurity talent.[18]

Cybersecurity education and training can be regarded as a comprehensive process designed to equip individuals with the knowledge, skills, and abilities necessary to protect digital assets, identify and mitigate cyber threats, and ensure the security of information systems. Cybersecurity education and training encompasses a wide range of topics and approaches aimed at developing a workforce capable of addressing the evolving challenges in the cybersecurity

[14] ITU-D SG2 Document SG2RGQ/160 from the *Réseau International des Femmes Expertes du Numérique* (RIFEN)
[15] ITU-D SG2 Document 2/35 from Rwanda
[16] ITU-D SG2 Document 2/370 from China
[17] ITU-D SG2 Document SG2RGQ/165 from Brazil; https://www.youtube.com/playlist?list=PLOmVJ5Ex3R10wEUM3edKTSErojXs_07xg (cybersecurity playlist)
[18] https://www.weforum.org/publications/global-cybersecurity-outlook-2025/

landscape. Cybersecurity education and training can take various forms, including formal academic programmes, professional certifications, hands-on workshops, and continuous learning initiatives.

Cybersecurity education and training programmes are crucial in today's digital landscape as they help prevent data breaches and mitigate cyber risks, by equipping individuals and professionals with the knowledge and skills to identify and respond to potential cyber threats.[19] The Cybersecurity and Infrastructure Security Agency (CISA) of the United States, considers cybersecurity education and training as "essential to protecting our Nation's critical infrastructure"[20] underscoring the critical role that well-trained cybersecurity professionals play in safeguarding national security and economic interests.

The scale and level of cybersecurity education and training policies in different ITU Member States varies greatly, with some Member States deploying comprehensive policy tools to increase the number of cybersecurity professionals at all levels, while other Member States focus on specific cybersecurity training programmes. Some Member States have focused on graduate students by establishing tertiary-level programmes at universities, while other Member States have emphasized the need to train employees already in the workforce. Additionally, a number of international programmes run by international organizations have emerged. Regional level disparities have also been noted, with cybersecurity courses at university level being offered in 91 per cent of European countries, compared with 60 per cent of countries in the Americas region, and 61 per cent of countries in the Africa region.[21]

The **United Kingdom** offers an example of an advanced cybersecurity education and skills approach, that has implemented a variety of policies and programmes at all levels to alleviate the cybersecurity skills gap. Their strategy focuses on three main areas: cybersecurity skills for adults, cybersecurity skills for young people, and developing cybersecurity professions. For adults, the United Kingdom offers intensive bootcamp courses of 12-16 weeks duration, including the Upskill in Cyber initiative, to retrain and upskill individuals in cybersecurity. The United Kingdom also promotes apprenticeships, such as the CyberFirst Degree Apprenticeship, to provide practical, on-the-job experience. For young people, the United Kingdom has created an ecosystem of offerings under the "CyberFirst" banner. This includes a national competition for girls interested in cybersecurity careers, introductory courses during school holidays, and a recognition scheme for schools with excellent cybersecurity education programmes. The flagship learning platform for young people in the United Kingdom, Cyber Explorers, is free for all 11-14 year olds and has achieved near gender parity in participation. The United Kingdom is also working to develop the cybersecurity profession through the United Kingdom Cyber Security Council (UKCSC). This professional body aims to create clear pathways and standards in the field of cybersecurity, making it more accessible and structured for individuals at all career stages.[22]

Brazil offers an example of a well-designed cybersecurity policy with a specific intended focus and outcome. The country has launched the "Hackers do Bem" *(White Hat Hackers)* programme to address an identified cybersecurity professional shortage of 230 000 positions, by training 30 000 individuals as cybersecurity professionals to fill these positions. The programme is

---

19 https://www.forbes.com/councils/forbestechcouncil/2025/01/21/protecting-our-future-why-cybersecurity-training-is-essential-for-students/

20 https://niccs.cisa.gov/education-training

21 https://www.itu.int/epublications/publication/global-cybersecurity-index-2024

22 ITU-D SG2 Document 2/77 from the United Kingdom

implemented by Brazil's National Education and Research Network (RNP), SENAI-SP, and Softex, with support from the Ministry of Science, Technology and Innovations. The programme follows a structured five-level approach to cybersecurity education. The programme begins with a levelling phase covering basic IT concepts, then progresses through basic and fundamental cybersecurity concepts, and culminates in specialized training. The specialized level focuses on five key professional profiles: "Red Team" (security assessment), "Blue Team" (security architecture), "DevSecOps" (application security), "CSIRT" (incident response), and "GRC" (governance, risk, and compliance). The final level includes a six-month cybersecurity residency programme with professional mentoring across Brazilian states. To ensure sustainability, the programme has established a national cybersecurity hub that connects various stakeholders, including educational institutions, government bodies, companies, and students. This national cybersecurity hub aims to align industry needs with educational outcomes and expand cybersecurity training opportunities across Brazil.[23]

Some countries have been promoting cybersecurity in third-level education in an effort to upskill their populations. For example**,** the Government of **Rwanda** has introduced information security course modules into information technology (IT) and computer engineering programmes in tertiary educational institutions. Carnegie Mellon University - Africa (CMU-Africa) in Kigali, offers programmes covering cybersecurity, software engineering, and other information and communication technology (ICT) topics. These CMU-Africa programmes focus on teaching and research in cybersecurity and privacy, from securing software and network systems, to making security and privacy more usable.[24]

Alternatively, rather than targeting educational institutions, other countries have been targeting professional actors already in the workforce, especially in sectors that are more susceptible to cyber threats. Training programmes have been designed specifically for public sector employees in **Argentine Republic** covering essential topics on data security and good practices in information management. These courses aim to equip participants with essential knowledge and skills to safeguard the privacy, confidentiality, integrity, and availability of information. Specialized training is also provided for civil servants designated as cybersecurity focal points. The specialized training sessions cover topics such as new cybersecurity challenges, digital evidence, penetration testing, and hardening of computer systems.[25]

Similarly, the **Syrian Arab Republic** has organized training activities targeting government sector employees, universities, and banking sector personnel. A Centre of Excellence at the National Network Services Authority provided information security training courses, though its activities were interrupted during the war, before being relaunched in 2021.[26]

Egypt created in 2021, the Egyptian African Telecom Regulatory Training Centre (EG-ATRC), which exemplifies the power of regional cooperation by providing academic and professional training to raise human competencies across African countries in the field of securing information and networks.[27]

Another example is the Latin America and Caribbean Cyber Competence Centre (LAC4), an initiative led by the **European Union**, CyberNet, and the Government of Dominican Republic.

---

23 ITU-D SG2 Document SG2RGQ/184 from Brazil
24 ITU-D SG2 Document 2/35 from Rwanda
25 ITU-D SG2 Document 2/150 from Argentina
26 ITU-D SG2 Document SG2RGQ/163 from the Syrian Arab Republic
27 ITU-D SG2 Document 2/329 from Egypt

LAC4 fosters regional cyber capacities through extensive knowledge exchange, training, and the development of good practices in cybersecurity and digital transformation. Located in Santo Domingo, Dominican Republic, LAC4 operates as a central hub to exchange collective experiences, assisting over 25 countries in the Latin America and the Caribbean region, to strengthen cybersecurity frameworks and encourage regional cooperation. The wide-ranging training and cyberdrill activities of LAC4, include raising awareness, managing cyber risks, protecting critical infrastructures, and shaping cybersecurity policies and laws. It also offers numerous technical training sessions aimed at enhancing the skills and knowledge of cybersecurity professionals across the region. Significantly, LAC4 places a strong emphasis on gender diversity in cybersecurity, conducting specialized training workshops aimed at empowering women in the field. These efforts are critical in building a diverse and resilient cybersecurity workforce, capable of tackling evolving challenges in the digital landscape.[28]

Cyberdrills, simulating cyberattacks, information security incidents and other types of disruption, are an important component of cybersecurity capacity building initiatives, and have been the focus of the **ITU** Telecommunication Development Bureau (BDT) efforts, as a means to enhance countries' cybersecurity readiness, protection, and incident response capabilities. ITU organizes regional and global cyberdrills, as well as national exercises, and develops materials to support these activities.[29]

As cybersecurity grows in prominence on the political agenda worldwide, international organizations have also entered the field with programmes aimed at enhancing cybersecurity skills for future generations. Notable international efforts include programmes implemented by ITU The BDT Her CyberTracks programme is a three-part project incorporating online and on-site technical training in cybersecurity policy and diplomacy, soft skills training courses, guided monthly mentorship circles, inspirational keynote presentations, as well as regional networking events, all made available as a complementary and one-stop holistic curriculum under the "Policy & Diplomacy Track" project. The objective of the project is to promote the representation and participation of women, while seeking to improve women's contribution to national and international cybersecurity policy processes.[30]

1.3 Child online protection

According to the Global Child Safety Institute (Childlight), one in eight children worldwide, or approximately 302 million young people, have been victims of non-consensual taking, sharing of, and exposure to sexual images and video in 2024.[31]

Child online protection and safety refers to the measures, practices, and strategies implemented to safeguard children and young people, from potential risks and threats in the digital environment. Child online protection encompasses a wide range of efforts to create a safer online experience for minors, including protection from various forms of online abuse, such

[28] ITU-D SG2 Document SG2RGQ/117 from the Dominican Republic
[29] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cyberdrills.aspx
[30] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Skills-Development/Her-CyberTracks.aspx
[31] https://www.ed.ac.uk/news/2024/scale-of-online-harm-to-children-revealed-in-globa

as sexual exploitation and grooming,[32] exposure to harmful and age-inappropriate content, cyberbullying, pornography, and use of online platforms for illegal activities.[33]

Child online protection and safety is crucial in today's digital age, where children are increasingly exposed to the Internet and its potential risks, making online safety education essential in empowering children to navigate the digital world responsibly. By teaching children about online risks, critical thinking, and responsible online behaviour, they can develop the skills needed to protect themselves and make informed decisions online.[34]

Contributions from Member States show that countries have taken child online protection very seriously in recent years, utilizing various instruments to ensure the safety of children online. GCI data reveals that, globally, 69 per cent of governments have implemented campaigns specifically targeting parents, educators, and children as part of child online protection efforts.[35] A number of countries have been designing comprehensive legal and policy frameworks, as well as practical programmes and tools, to safeguard the online environment for children. Empirical evidence on children's online behaviour has been collected to better understand and address some of the most challenging online safety issues. Countries have recognized the importance of multi-stakeholder solutions that bring together the right stakeholders to tackle this multifaceted problem. Finally, countries have implemented programmes that blend cybersecurity awareness with online safety, demonstrating the importance of a comprehensive approach.

Australia offers an example of a country that opted to enact a solid legal framework to tackle child online protection. In 2021, the Government established a robust framework through the Online Safety Act, which addresses cyberbullying, adult cyber abuse, and image-based abuse. In 2022, Australia also established the eSafety Youth Council, comprising 24 members aged 13-24, which provides direct input on policies and programmes, while working with major technology companies to enhance user accountability.[36]

China offers another example of a country with a comprehensive child online protection policy, and has implemented far-reaching Internet safety education programmes. Schools serve as the primary channel for delivering cybersecurity education, reaching 90.3 per cent of minors, while families serve as the second most important channel, at 61.7 per cent. Overall, 85.4 per cent of minors have received some form of Internet safety education. The "Broadband Protecting the Minors" programme was established through national telecommunication operators, and has helped to protect 160 million families with school-age children, and has the capacity to handle over 1.02 billion calls. The Government has also launched specific campaigns to address online safety concerns. China has enacted several key policies, including regulations on the network protection of children's personal information, and regulations on the Internet protection of minors. The effectiveness of these programmes is revealed in the statistics: over 70 per cent of minors can now recognize online fraud, and more than half demonstrate awareness of healthy Internet usage.[37]

---

[32] Grooming can be defined as is the intentional proposal, through information and communication technologies, of an adult to meet a child who has not reached the legal age for sexual activity, for the purpose of committing acts of sexual abuse or producing child sexual abuse material, according to Article 23 of the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse – https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=201

[33] https://www.nspcc.org.uk/keeping-children-safe/online-safety/

[34] https://www.cois.org/about-cis/child-protection/resources; https://learning.nspcc.org.uk/online-safety

[35] https://www.itu.int/epublications/publication/global-cybersecurity-index-2024

[36] ITU-D SG2 Document 2/167 from Australia

[37] ITU-D SG2 Document SG2RGQ/212 from China Mobile Communications Co. Ltd.

Other countries have also been blending cybersecurity awareness with online safety education. For example, the **Russian Federation** has implemented the "Digital Literacy Campaign" as part of its broader national "Digital Economy" programme launched in 2018. The programme delivers content through interactive animated videos covering essential cybersecurity topics including phishing detection, personal information protection, cyberbullying response, safe social media practices, and information verification. The curriculum extends to specific areas such as copyright awareness, online fraud prevention, computer virus protection, digital etiquette, and electronic money safety. To ensure effective implementation, the campaign provides teachers with methodological materials to integrate these cybersecurity lessons into computer science classes and parent-teacher meetings.[38]

A number of government administrations have established specific technological tools to protect children online. As part of a broader national strategy for the protection and empowerment of children and young people online**, Côte d'Ivoire** launched the "jemeprotegeenligne.ci"[39] (*I self-protect online*) website, offering interactive tools, search engines, and social media sites specifically designed for children. The site also includes a reporting mechanism allowing users to report abuse anonymously and discreetly. The initiative involves collaboration between various stakeholders and received the support of the Internet Watch Foundation.[40]

In addition, countries and organizations have also recognized the need to include several stakeholders in the child online protection process**.** In **Nigeria**, the "Child Online Protection Initiative" serves as a primary framework, incorporating policies into Internet service providers' terms and conditions. As one of the key policy actors in the country, the Nigerian Communications Commission (NCC) has established reporting mechanisms for child abuse content and implemented blocking measures for such material.[41] **Republic of Zambia** launched a "National Child Online Protection Strategy" in 2020, with a five-year implementation plan (2020-2024), focused on organizational structures, capacity building, legal measures, international cooperation, and technical procedures. Zambia identified several lessons learned including broader stakeholder collaboration, sustainable and sustained funding, and a robust monitoring and evaluation framework.[42] Finally, the **ITU** child online protection initiative serves as global leadership platform involving a multi-stakeholder community with proven expertise, and a successful technical assistance record, spanning over 10 years, in child online protection activities worldwide. Composed of more than 80 knowledge partners, child online protection activities include developing material for children,[43] guidelines targeting parents and educators,[44] industry[45] and policy-makers,[46] conducting online training through the ITU Academy, and offering in-person training for educators and youth.[47] The above-mentioned guidelines represent 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 and young people. These guidelines have been developed and disseminated through a translation, localization, and awareness campaign.

---

38 ITU-D SG2 Document SG2RGQ/170 from the Russian Federation
39 https://www.jemeprotegeenligne.ci/
40 ITU-D SG2 Documents 2/34 and 2/137 from Côte d'Ivoire
41 ITU-D SG2 Document SG2RGQ/20 from Nigeria
42 ITU-D SG2 Document SG2RGQ/114 from Zambia
43 https://www.itu-cop-guidelines.com/children
44 https://www.itu-cop-guidelines.com/parentsandeducators
45 https://www.itu-cop-guidelines.com/industry
46 https://www.itu-cop-guidelines.com/policymakers
47 https://www.itu-cop-guidelines.com/

Various countries have also focused on capacity building activities, as well as on the collection of empirical data to understand how children interact online**.** In **Kenya** the Communications Authority implemented the "Be the COP" and "*Huwezi Tucheza, Tuko Cyber Smart*" campaigns, aimed at parents, guardians, teachers, and youth. Kenya, in collaboration with the African Advanced Level Telecommunications Institute, has also developed educational resources and capacity-building initiatives, including a training programme on child online protection and safety measures. This programme has provided training on child online protection and safety for 951 participants across various sectors. Kenya is also conducting a national survey on child online protection and safety to gather empirical data on children's online behaviour. This national survey was expected to be completed in 2024.[48]

[48] ITU-D SG2 Document 2/119 from Kenya

Chapter 2 – Cybersecurity assurance practices

Cybersecurity assurance practices have emerged as a critical element in protecting networks, systems and data from malicious activities.[49] Cybersecurity assurance practices broadly refer to the procedures used to ensure that relevant controls are in place to protect the confidentiality, integrity, and availability of electronic devices, systems, networks, and data. Although cybersecurity assurance practices do not directly prevent cyberattacks, their goal, if correctly implemented, is to minimize the risk of such attacks. Cybersecurity assurance practices can be checked against specific security controls, guidelines and standards, and can either be imposed by regulations or voluntarily adopted by the industry. However, there is no one-size-fits-all approach, with national authorities and sector regulators often employing different practices, ranging from self-assessments and voluntary guidelines, to labelling schemes and rigid compliance checks.

While there is no one single approach to be recommended, it is evident that, in recent years, there has been a sustained shift towards the adoption of cybersecurity assurance practices worldwide, with different developments in several countries and regions. As an example of this shift towards the adoption of cybersecurity assurance practices, in December 2022, the **Organisation for Economic Co-operation and Development (OECD)** launched the Recommendation of the Council on the "Digital Security of Products and Services", which recommends the adoption of policies to enhance the digital security of products and services that are proportionate to the risk, starting with a light-touch approach based on voluntary policy measures, and then exploring the need for mandatory measures.[50] This chapter conveys the challenges faced, assesses the impact, and presents the lessons learned to date, in defining and implementing cybersecurity assurance practices.

2.1 Approaches to assessing criticality, risks and costs

When considering the implementation of cybersecurity assurance practices, it is crucial to determine first what an entity is trying to protect, and the risks faced by the identified assets. Countries and companies wanting to protect against cyberattacks should, as a priority, identify what systems and assets need protection and assess their vulnerabilities. In this regard, a framework or blueprint for conducting risk assessments is a helpful tool. One of the most well-known frameworks for conducting risk assessments is the **United States**, National Institute for Standards and Technology (NIST) Cybersecurity Framework,[51] which has been recently updated[52] and offers a widely used approach to help determine and minimize organization risks. It establishes non-regulatory guidelines allowing organizations globally to identify their own risk landscape and apply appropriate cybersecurity controls. The revised framework, published in

[49] Operational security is intricately linked to cybersecurity assurance practices, in that operational security can provide a good foundation for assurance practices. Broadcom presented the model for good conditions highlighting that it is comprised of four key elements: people and processes, knowledge, security products (exogen security) and security in assets (endogen security). See 'Reduce Risk and Protect Reputation', ITU-T SG17 Document SG17-C214 from Broadcom Corporation

[50] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0481

[51] https://www.nist.gov/cyberframework

[52] https://www.nist.gov/cyberframework/updating-nist-cybersecurity-framework-journey-csf-20

early 2024, builds upon a wide and long-term engagement with the community of stakeholders that use these guidelines, as well as continued alignment with other international standards.[53]

The NIST position as a non-regulatory agency has allowed a deeper engagement with industry stakeholders from around the world to better understand real-world challenges and receive feedback, which have been incorporated into the new guidelines.[54] These guidelines are intended to be adaptable, flexible, and applicable to all organizations and sectors. **BitSight** incorporates the NIST Cybersecurity Framework in its platform, which has been used by various government agencies responsible for cybersecurity (such as computer emergency response teams, national cybersecurity agencies, and telecommunication regulators).[55] Through the platform, countries can conduct risk assessments of their infrastructure and assets that are considered critical, and measure their risk factors.

Risk assessments can also help to determine what level of assurance is appropriate, taking into consideration the sensitivity of the data and assets being protected, the consequences of a breach, and the threat environment (i.e. whether an entity is susceptible to a cyberattack). In some cases, the levels of assurance will be dictated by regulatory requirements. The higher the level of assurance, the stricter the security controls. For example, a low level of assurance could require a system password or a firewall, whereas a higher level of assurance would require the addition of more advanced controls such as advanced encryption, and multifactor authentication.

Although cybersecurity assurance practices add to information technology budgets, the failure to put in place security controls can be even more costly. The costs of suffering a cyberattack are not measured only in financial terms, as the additional reputational cost can be far more damaging. Losing the trust of customers and citizens has a long-term effect that goes beyond money, and organizations must be able to strategically understand that. Equally, for the public sector, successful attacks may impact on the provision of public services and critical activities, and the disruption of such services and activities also cannot be measured in financial terms only, since it affects the lives of citizens.

Planning and budgeting cybersecurity investment to ensure compliance with national regulations can be a challenging task for different organizations. To support organizations in cost planning for legally required cybersecurity controls, the **Kingdom of Saudi Arabia** National Cybersecurity Authority (NCA) has developed a cost estimation tool for implementing Saudi Arabia's "Essential Cybersecurity Controls."[56] Following early trials, the NCA concluded that the cost estimation tool has proven to be effective, and provides a good estimate, especially for organizations in the early stages of implementing cybersecurity-related controls that often have no previous records of the estimated budget, time, or resources needed to implement such cybersecurity controls.

2.2 Multistakeholder approaches

It is important to benchmark initiatives against other initiatives in order to understand good practices and learn from the successes and mistakes of others during the development of an initiative. It is also important to engage with multiple stakeholders, including industry stakeholders, to gain important insights for the development of the initiative.

[53] https://www.nist.gov/cyberframework
[54] ITU-D SG2 workshop presentation Q3/2_2023_07 by the United States
[55] ITU-D SG2 workshop presentation Q3/2_2023_02 by BitSight
[56] ITU-D SG2 Document SG2RGQ/201 from Saudi Arabia

Although cybersecurity assurance practices are becoming increasingly necessary in least developed countries (LDCs), they may remain difficult to implement. The case of Cyber Defence Africa (CDA) in **Togo** can serve to explain some of the challenges experienced in local markets in providing cybersecurity assurance across essential service operators (ESOs).[57] A lack of funding, a lack of trust in the Government as a service provider, and a lack of local human capacity and facilities, were cited as some of the challenges experienced. To support ESOs in complying with newly published cybersecurity controls, the Government of Togo created a public–private partnership with a large reputable cybersecurity provider, to provide cybersecurity services in both the public and private sectors. Through this partnership model, Togo created CDA as a self-sufficient and high-quality, local cybersecurity provider to support ESOs on a non-mandatory basis. The self-sufficient model employed allowed Togo to address the many challenges mentioned above and to begin to foster local talent in cybersecurity, as well as encouraging the development of the local market. The importance of CDA was noted, as a private entity in a competitive market to ensure adaptability, high quality of services, and competitive pricing.

It is also important to foster cooperation between policymakers who may set the regulatory environment, and civil society organizations. Civil society organizations can boost the demand for security and also inform policy and regulatory development on the basis of existing identified regional and international practices. For instance, the **DiploFoundation** is an international organization delivering training programmes and capacity building expertise to governments, regulators, businesses, and civil society on topical questions related to cybersecurity, and is also involved in the "Geneva Dialogue on Responsible Behaviour in Cyberspace".[58] In 2020, the Geneva Dialogue produced a collection of good practices,[59] which include suggested definitions of secure design and vulnerability management, threat modelling, third-party and supply chain security, secure development, vulnerability management and disclosure, as well as organizational culture.

The **Global Forum on Cyber Expertise (GFCE)** is an international platform that supports the coordination of projects, promotes the sharing of knowledge and expertise, matches requests to offers of capacity-building support, and develops research projects.[60] The GFCE set up four regional hubs in the Pacific Islands, Africa, the Americas and the Caribbean, and South-East Asia. Given its global footprint and its varied support in developing countries, the GFCE is well placed to provide diverse regional views on the needs and demands of cyber capacity building. The GFCE comprises an online portal, which serves as a repository of implemented and ongoing projects in cyber capacity building, and of resources and tools. The GFCE online portal helps to reduce duplication of effort and also helps to identify gaps and patterns in capacity-building provision.[61]

2.3 Evolving regulatory approaches

In many cases, cybersecurity assurance practices are introduced on a voluntary basis before becoming mandatory. The shift to becoming mandatory usually happens when governments consider that industry is not doing enough to secure products, and that consumers do

[57] ITU-D SG2 workshop presentation Q3/2_2023_09 by Cyber Defense Africa
[58] ITU-D SG2 workshop presentation Q3/2_2023_11 by DiploFoundation
[59] https://genevadialogue.ch/goodpractices/
[60] ITU-D SG2 workshop presentation Q3/2_2023_12 by Global Forum on Cyber Expertise
[61] https://cybilportal.org/

not necessarily have the knowledge to assess if the products are safe or not. This can lead governments and national authorities to act, and to stipulate assurance practices that they expect industry to meet. Whether mandated by law or not, it is good practice to review and adapt cybersecurity assurance practices over time given the dynamic threat landscape and evolving cybersecurity risks.

In **Brazil**, the telecommunication regulator, Anatel, offers an example of an evolving approach with the creation of a system of certification bodies and testing laboratories within the country for the certification of customer premises equipment (CPEs), or home gateways. The initial approach of Anatel, was to provide non-mandatory cybersecurity guidelines for the telecommunication sector. However, by carrying out risk assessments it was found that recommendations were not enough to secure CPEs given the vulnerabilities and threats associated with this type of equipment, and that it was necessary to establish mandatory minimum safety requirements for such products. Mandatory requirements for telecommunication service providers in Brazil, were published in early 2023, and focus on vulnerabilities, such as non-secure passwords and unnecessarily enabled service parts.[62] The requirements became effective in early 2024, as part of mandatory laboratory tests for product approval.[63] Anatel explained that the evolution from a non-mandatory approach to a cybersecurity compulsory certification requirement for a specific set of equipment was only possible following a comprehensive debate with the sector.

Similarly, in **Saudi Arabia**, the National Cybersecurity Agency (NCA) highlighted an initiative to build an independent verification and validation (IV&V) ecosystem[64] to test and certify products from a cybersecurity assurance perspective at national level. The initiative also aims to identify and classify hardware and software that are highly sensitive to cyber risks and threats. Furthermore, the initiative seeks to contribute to the development of human capabilities in IV&V. The roadmap for the initiative considers beginning with a voluntary programme before making cybersecurity assurance a mandatory obligation. The agency also indicated the importance of such an ecosystem eventually becoming "self-sustaining", and this has informed the NCA approach of encouraging market stakeholders to conduct such IV&V assessments.

In the Internet of Things (IoT) security domain, the United Kingdom and Australia also provide case studies of evolving from a voluntary to mandatory cybersecurity assurance approach. In recent years, both countries have decided to mandate, through legislation, a baseline security requirement for IoT consumer products based on the European Telecommunications Standards Institute (ETSI) EN 303 645 standard,[65] the first globally applicable cybersecurity standard for consumer IoT devices.

In the **United Kingdom**, manufacturers, importers and distributors will be obliged to comply with three of the 13 ETSI security guidelines, and the law gives powers to the Government to adopt additional requirements if necessary, depending on regular threat assessments. The decision to mandate baseline security requirements followed a period of voluntary adoption. In 2018, the country formulated a voluntary code of practice[66] for consumer IoT security, but industry compliance was not as expected. Evidence gathered through consultation exercises showed

---

62 ITU-D SG2 Document SG2RGQ/58 from Brazil

63 ITU-D SG2 workshop presentation Q3/2_2023_12 by Brazil; https://informacoes.anatel.gov.br/legislacao/index.php/component/content/article?id=1505; and https://informacoes.anatel.gov.br/legislacao/atos-de-certificacao-de-produtos/2023/1850-ato-2436

64 https://nca.gov.sa/en/news?item=535

65 https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf

66 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971440/Code_of_Practice_for_Consumer_IoT_Security_October_2018_V2.pdf

that consumers value security and are willing to pay a price premium for secure products. However, cybersecurity threats are not subject to the same level of robust regulation as product safety, leading to a lack of transparency from manufacturers, and slower adoption of security policies. The evidence also found that the consumer connectable product market disincentivizes the adoption of basic security features, as consumers overwhelmingly assume that products are already secure. The Product Security and Telecommunications Infrastructure (PSTI) regime aims to address this gap by mandating elements of the code of practice to ensure that manufacturers are aware of vulnerabilities and take steps to mitigate them. The PSTI regime came into effect in April 2024 and applies to any consumer product that can connect to the Internet.[67]

Similarly in **Australia,** the Government found that there was a low uptake of its voluntary code of practice, published in 2020, 'Securing the Internet of Things for Consumers'. In 2024, the Government proposed a law that would mandate the code of practice, and the proposed law received consensus following a public consultation. The law aligns closely to United Kingdom's approach, intending to give the Minister the power to mandate specific security standards for IoT devices through secondary legislation (rules). By incorporating standards in rules rather than in primary legislation, the Government of Australia intends to update these standards quickly to ensure that consumers in Australia are protected based on international and industry good practice.[68]

In the **United Kingdom**, one of the challenges identified is the possible impact on small and micro enterprises that may encounter difficulties in complying with the new PSTI regime. The United Kingdom PSTI enforcement authority is developing guidance to mitigate any disproportionate impacts. In addition to working with the industry, the United Kingdom noted that the top three requirements to be mandated in the scheme have been identified and communicated transparently for several years. During this period, the United Kingdom has conducted a number of exercises on the regime implementation process, including password requirements, fundamental product architecture, vulnerability exposure, and security transparency requirements. The impact assessment has shown that the overall benefits of reducing the volume of cyberattacks on consumers and businesses, are expected to exceed the costs associated with the implementation of PSTI regime. As the PSTI Act (2022), is the first mandatory cybersecurity product legislation in the world, the cost of enforcing the regime is uncertain, but initial estimates suggest that the allocated funding will be sufficient.

In some cases, the distinction as to whether a cybersecurity assurance practice is mandated or remains voluntary is dictated by the type of user or client. For example, the **Republic of Korea** launched the Cloud Security Assurance Program (CSAP), a security certification for cloud computing services.[69] In general, the CSAP certification is voluntary. However, customers in the public sector (public agencies) are required to use a cloud service that has obtained CSAP certification pursuant to the relevant regulations, and cloud service providers therefore need to obtain CSAP certification when providing cloud services to public agencies.

Regular internal audits that can help to identify gaps in controls and risk of exposure, as well as threat intelligence subscriptions, are considered good practices. Even if a product is certified, it could suffer from security flaws over its lifecycle. A certification scheme requires the submission of information at a specific time, and the process does not account for dynamic threat changes

67 ITU-D SG2 workshop presentation Q3/2_2023_03 by the United Kingdom
68 ITU-D SG2 Document 2/320 from Australia
69 https://isms.kisa.or.kr/main/csap/intro/index.jsp and ITU-D SG2 Document SG2RGQ/34 from the Republic of Korea

in the future. A recent BitSight study showed a strong correlation between poor "patching cadence" for vulnerabilities and the likelihood of experiencing a cybersecurity incident,[70] pointing to the critical importance of updating systems as soon as security patches are available, bearing in mind the reported varying distribution of patches across the globe.

Penetration testing, or "pen testing," is a security assurance exercise that helps to evaluate the security of an IT system and identify vulnerabilities that could otherwise be used to exploit systems. Ofcom, the **United Kingdom** communications regulator, runs the TBEST scheme voluntarily with telecommunication providers. This pen testing scheme aims to simulate a cyberattack in order to identify security vulnerabilities that can then be addressed through a process of remediation to improve the operators' network security posture.[71,72] More broadly, this scheme is an example of a supervisory regime approach being taken by Ofcom, which stresses the importance of building collaborative relationships with the industry that the authority regulates. To date, all United Kingdom communication providers have run the TBEST scheme voluntarily, or are doing so, and have made changes as a result. TBEST is neither a "standard" nor a certification process. The goal is to enable communication providers to gain awareness of cyberthreats and implement appropriate changes in a timely manner to improve their cyber-defence capabilities. By being aware of, and addressing such vulnerabilities and weaknesses, the operator is in a much stronger position to protect its networks.

2.4 Educating consumers and manufacturers

Efforts have been made to educate the public about the importance of cybersecurity and the benefits of choosing more secure products.

One approach to this end is the development of a cybersecurity labelling scheme, under which, as exemplified by **Republic of Singapore**, certified products can be accompanied by a label. Labelling schemes serve primarily as an information tool for consumers. In Singapore, the Cybersecurity Agency (CSA), responsible for the cybersecurity labelling scheme, aims to help consumers distinguish between more and less secure IoT devices.[73] The scheme is voluntary (with the exception of Wi-Fi routers, for which it is mandatory) and has four levels, with level 1 being the security baseline. Levels 1 and 2 are based on self-assessment by manufacturers and levels 3 and 4 involve third-party assessment by an approved laboratory. The scheme is multilevel to incentivize manufacturers to incorporate additional security measures beyond the basic requirements.

The CSA also considered the trade-offs involved in mandating cybersecurity standards, including the risk of manufacturers bypassing the market due to increased compliance costs. Instead, the goal is to change the mindset of manufacturers to view cybersecurity as an enabler and market differentiator, rather than as an extra cost. Regarding the impact of the cybersecurity labelling scheme in Singapore, the process is still in the early stages, and efforts are ongoing to encourage manufacturers to participate in the scheme and improve their cybersecurity. A public survey will be conducted in the future to assess consumer awareness and behaviour. The cost of compliance is minimized for manufacturers at levels 1 and 2, and there has been no

[70] https://www.bitsight.com/press-releases/study-finds-significant-correlation-between-bitsight-analytics-and-cybersecurity

[71] works in close partnership with the Department of Science, Innovation and Technology (DSIT) and the National Cyber Security Centre (NCSC) to run it.

[72] ITU-D SG2 Document SG2RGQ/74 from the United Kingdom

[73] ITU-D SG2 workshop presentation Q3/2_2023_05 by Singapore

significant increase in the cost of products for consumers. With the voluntary scheme in place, market forces are expected to drive improvements in cybersecurity among manufacturers.

In the **United States**, the newly established U.S. Cyber Trust Mark program is an example of a voluntary cybersecurity labelling programme for IoT products.[74] In the development of the programme, the Federal Communications Commission (FCC) highlighted that soliciting the public input and comment of all relevant stakeholders, including industry, government, and civil society, is critical for designing and administering a programme that addresses identified needs. Whilst the FCC leads the programme, the Cyber Trust Mark will be implemented alongside a variety of interagency partners requiring close cooperation with all branches of government involved.

Beyond labels, it is equally important to invest in technical controls, and to build awareness and educate the population about the cybersecurity risks that organizations and countries are facing. Currently, ransomware attacks constitute the most concerning trend. For these types of attacks, the main vector of attack, meaning the way a criminal enters a network or system, is through phishing emails.[75] In this context, cybercriminals can often bypass security controls simply when people click on a phishing email. It is therefore crucial to cybersecurity assurance that citizens and employees are made aware of such issues. The promotion of user-awareness regarding cybersecurity is considered in Chapter 1 of this report.

2.5 Approaches to international synergy/harmonization and reciprocity agreements

The existence of reciprocity agreements between cybersecurity assurance models, such as certification and labelling schemes, can be a determinant for the scaling of these practices. As stakeholders have highlighted, reciprocity agreements can help to ease compliance for industrial actors operating across multiple markets. However, considering that reciprocity agreements are a formal mechanism, may have many national conditions, and take time to be approved and signed, cybersecurity assurance practices need to find synergies with existing international approaches that are in alignment with national needs and priorities. This will reduce the regulatory burden on products and service providers with the aim of avoiding contradictory requirements.

The Cybersecurity Agency (CSA) stressed the importance of international collaboration in the development and implementation of its cybersecurity labelling scheme. **Singapore** has signed mutual recognition arrangements with Finland and Federal Republic of Germany and is working to expand its partnerships in this area. Singapore reflecting on its experience noted that governments need to be proactive in establishing recognition, though manufacturers also have an interest in supporting the process of recognition, as mutual recognition arrangements reduce the burden of repeated testing and certification, as well as helping to attain market access in different jurisdictions. The process involves bringing interested parties together to harmonize requirements and establish common standards that are realistic and not overly burdensome.

At European level, the **European Union Agency for Cybersecurity (ENISA)** has a mandate to develop three certification schemes, which would be recognized across the internal market

[74] ITU-D SG2 Document 2/196 from the United States

[75] A common tactic used by cyber-criminals to trick people to reveal sensitive information or download malware which infects the targeted system/network.

and therefore have automatic 'mutual recognition' across the European Union. These are: the *European Union common criteria scheme for ICT products*, for which the implementing regulation was adopted in early 2024; and the *cloud services scheme*, which is under discussion; and finally, the *5G scheme*, which is under development.[76]

In addition to reciprocity and considering the international markets in which the industry operates, the harmonization of baseline security requirements is also an important consideration. The ETSI standards on IoT consumer products provide an example of an attempt to harmonize baseline security requirements. The main question is to what extent different regulatory frameworks will be in alignment, and to what extent they will be connected through the same international standards. In this regard, strengthening and even finding the right place for dialogue has been noted as presenting a challenge. In the area of harmonization, ENISA activities in cybersecurity standardization and 5G, require collaboration among the European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC), ETSI, the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), the GSM Association (GSMA), the 3rd Generation Partnership Project (3GPP), and the GlobalPlatform. One of the main outputs of ENISA has been the consolidation of 5G security controls from different standards development organizations (SDOs) into a single repository.[77]

[76] ITU-D SG2 workshop presentation Q3/2_2023_10 by the European Union Agency for Cybersecurity
[77] https://www.enisa.europa.eu/publications/5g-security-controls-matrix

Chapter 3 – CIRT national coordination for the resilience of critical infrastructure and cybersecurity incident response

In today's rapidly evolving digital landscape, organizations face an ever-growing threat of cybersecurity incidents that can compromise sensitive data, disrupt operations, and undermine the trust of stakeholders. National coordination of cybersecurity incident response team (CIRT) efforts strengthen the resilience of critical infrastructure (CI). By fostering collaboration, information sharing, and standardized protocols, such initiatives aim to enhance the collective ability to detect, mitigate, and recover from cyber incidents efficiently. To achieve this objective, Member States should increase their efforts to establish and develop CIRTs, as typically the first significant step toward creating a cybersecurity culture. It should be noted that 'CIRTS' are also known as cyber security incident response teams (CSIRTs) and as computer emergency response teams (CERTs), and for the purpose of this report, considered synonyms.[78]

One task of national CIRTs is responding to threats against critical infrastructure (CI). CI refers to a collection of systems, networks, and assets that are considered essential to public safety. There is no single definition of what constitutes "critical infrastructure", as this is established nationally, based on countries' national needs and priorities, though it typically includes sectors such as transportation, energy systems, communication systems, water systems, financial systems, and healthcare. Malicious cyber activity targeting national CI continues to be a significant challenge for governments and can present risks to citizens. A 2024, report from KnowBe4 indicates that malicious cyber activity against CI have risen by 30 per cent since 2022, representing more than 420 million attacks between January 2023 and 2024. This is equivalent to 13 attacks each second.[79]

CI attacks pose the greatest threat to impacting citizens' lives. Targets often include healthcare and emergency services, impacting the ability to receive medical care, such as surgeries and prescriptions. Other target examples include energy infrastructure, such as power grids. Given the possibility of impacts on lives, coordination and response to such incidents is critical and a key function of CIRTs.

As part of the development and maturity of CIRTs, countries often develop robust cybersecurity incident response plans to effectively detect, contain, mitigate, and recover from security breaches. A proactive and well-defined cybersecurity incident response plan is essential for organizations to effectively mitigate the impact of security incidents. There are various cybersecurity incident response plan models that countries have adopted to best manage risk and mitigate malicious cyber activity. Such models generally use a holistic approach, integrating good practices, and fostering a culture of continuous improvement, to enhance resilience against cyber threats and safeguard digital assets. As the threat landscape evolves, incident

[78] For more information about terminology see ENISA publication on *"How to Setup up CSIRT and SOC"* – https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc

[79] https://www.knowbe4.com/hubfs/Global-Infrastructure-Report-2024_EN_US.pdf?hsLang=en-us

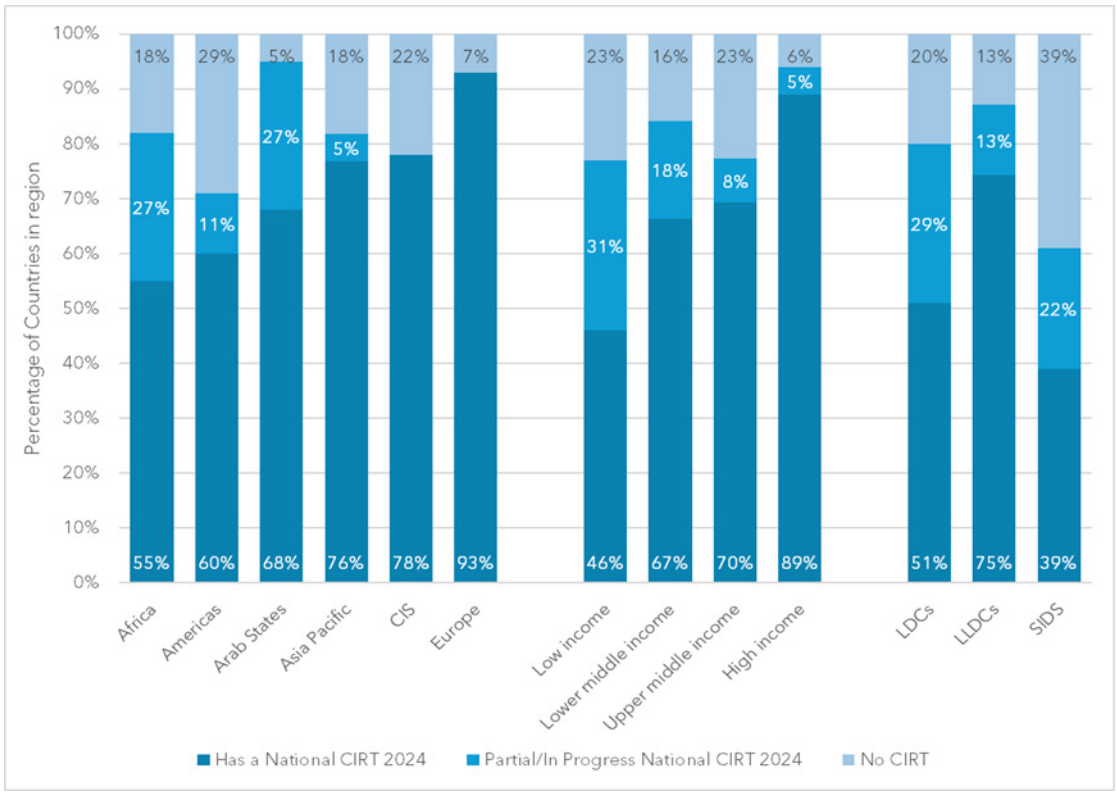
response strategies should stay ahead of cyber adversaries and protect the integrity and trust of the organization.

A more recent trend in response incident management is the establishment of national cyber coordination centres to enhance whole-of-government coordination. During a serious cyber incident, where there are often a number of government organizations involved; coordinating a quick response can be the difference between minor and major impacts. Having a centralized coordination centre or unit, can enable rapid response and overall management and control. It is worth mentioning that CI is not necessarily an infrastructure owned and managed by the public sector and therefore, ensuring coordination with the private sector is also an extremely important element when facing and responding to a cyber incident.

3.1 Establishment of CIRTs

According to the global cybersecurity index (GCI) 2024,[80] "*139 countries have a national CIRT, while 55 do not have a CIRT or national CIRT in progress*".

Figure 1: Percentage of countries with a CIRT, by region/income group/development status



Source: ITU

CIRT roles vary but one of their main functions is to detect and analyse potential threats in networks and systems and respond to mitigate the impact of incidents. The creation of a CIRT is often a significant step towards fostering a culture of cybersecurity awareness and resilience. Part of establishing a CIRT includes building the capacity and mechanisms required for CI protection.

[80] https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

The Government of **Kenya** established the National Kenya Computer Incident Response Team – Coordination Centre (National KE-CERT/CC), to coordinate national cybersecurity efforts and serve as the national point of contact on cybersecurity matters. The National KE-CERT/CC comprises a multi-stakeholder team with diverse skills to respond to and manage computer security incidents effectively. Recognizing the importance of cybersecurity in fostering a thriving digital economy, the Kenyan Communications Authority (CA) launched the CA Cybersecurity Bootcamp & Hackathon Series to build local cybersecurity capacity.[81]

With the assistance of the ITU, **Kyrgyz Republic** has been working to establish a national CIRT. The CIRT roles include identifying, managing, and responding to cyber threats along with watch-warning and incident response capabilities, building national capacity, and transferring know-how for further development in critical information infrastructure protection.[82]

ITU collaborates with Member States and global organizations, to strengthen cybersecurity through the creation and enhancement of national and regional CIRTs. Through the Telecommunication Development Bureau (BDT), ITU conducts CIRT maturity assessments, assisting to date 84 countries in evaluating their cybersecurity readiness, and establishing or improving national CIRTs. ITU has implemented 21 CIRT-related projects and is currently working on three more. CIRT maturity assessments have been conducted for Azerbaijan, Sierra Leone, and United Republic of Tanzania, with ongoing assessments for Republic of Zimbabwe, Kingdom of Bhutan, and Kingdom of Lesotho.[83] The assessments inform national CIRTs in drafting improvement operational plans. ITU also collaborates with the FIRST community to enhance the CIRT service framework and revise training materials for capacity-building in managing national CIRT operations.[84]

3.2 Role and responsibilities of CIRTs and critical infrastructure

CIRTs play a vital role in safeguarding CI across various sectors by providing real-time monitoring, incident management, threat analysis, and vulnerability assessments. CIRTs are typically responsible for ensuring the resilience of information and communication technology (ICT) systems, enabling the swift detection and resolution of cybersecurity threats, and coordinating efforts to minimize the impact of incidents on national security, public safety, and the economy. Based on the country's needs, development, and CI sectors, CIRTs take on different roles and relationships to ensure cybersecurity.

In **Republic of Lithuania**, the national CIRT operates under the broader National Cyber Security Centre (NCSC) and is specifically focused on cyber incident response and resilience coordination across CI sectors. The Government has worked to ensure that the CIRT has the necessary responsibilities and technical abilities to actively protect CI, and this work serves as a model for other countries looking to build their CIRT capabilities. The CIRT is instrumental in providing incident management services for both public and private sector stakeholders, ensuring that appropriate responses are implemented both during and after cyberattacks. One of the key aspects of the role of a CIRT in incident management, is their ability to coordinate with the affected network or system administrator, facilitating a swift recovery of operations.

---

81 ITU-D SG2 Document 2/112 from Kenya
82 ITU-D SG2 Document 2/170 from ITU BDT and ITU-D SG2 information session presentation SG2_2023_05 by ITU BDT
83 ITU-D SG2 Document 2/201 from ITU BDT
84 More details on ITU CIRT Programme: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx

During major incidents in Lithuania, CIRT specialists are deployed on-site to assist CI operators in restoring normal operations. For example, during a distributed denial of service (DDoS) attack on the Lithuania telecommunication sector, the national CIRT played a crucial role by coordinating communication between affected operators and providing technical recommendations that helped restore services swiftly.

A key part of CI protection is not just responding to malicious cyber incidents, but also through a more advanced feature of CIRTs, preventing malicious cyber incidents. Lithuania has given its CIRTs responsibility for vulnerability management, through the collection of information from public sources, closed forums, and vulnerability reporting mechanisms. The team actively scans Lithuanian digital assets to identify vulnerabilities that could be exploited by malicious actors. By disseminating information on vulnerabilities and threats, the national CIRT helps to fortify CI systems against potential cyberattacks, ensuring proactive protection across key sectors.[85]

Brazil has developed several overarching organizations to ensure that CI remains responsive, is protected, and employs the necessary cybersecurity procedures. In Brazil, two CIRTs assume national responsibilities: the Brazilian National Computer Emergency Response Team (CERT.br) and the Centre for Prevention, Treatment and Response to Government Cyber Incidents (CTIR Gov). There are also a number of sectoral CIRTs, as well as the Federal Cyber Incident Management Network (ReGIC), established in 2021, that are coordinated by the CTIR Gov centre.[86]

One example of a sectoral CIRT is the Security Incident Response Centre (CAIS) of the National Education and Research Network (RNP). Since its establishment in 1997, CAIS has been the primary CIRT for Brazil's academic network. Operating under the guidelines of the Request for Comments (RFC) 2350, CAIS is tasked with detecting, resolving, and preventing security incidents within Brazil's academic network. While CAIS does not have direct authority over the institutions in the academic sector, it plays a key coordinating role in incident handling. The activities of CAIS reflect the growing need for collaboration within specific sectors to manage cybersecurity risks effectively. The case of CAIS offers an example of a specific sector CIRT ensuring CI protection.[87]

As part of another recent effort in Brazil to augment national cybersecurity, ReGIC, the federal cyber incident response framework, enhances coordination among federal government entities for the protection of CI.

ReGIC sets mandates and expectations for federal agencies. Under ReGIC, federal agencies are required to participate in the network, which includes measures for sharing threat intelligence, cyberattack alerts, and coordination during active incidents. Another specific ReGIC role is its mandate for sectoral coordination, wherein regulatory agencies, such as the National Telecommunications Agency (Anatel), are required to establish sectoral cyber security incident response teams (CSIRTs) and to report about their sectors.

The establishing of sector-specific computer emergency response teams (CERTs), in addition to the establishment of a national CERT has also been the approach undertaken by **Tanzania**,[88] which has created TZ-Fincert for financial and banking institutions, Academia CERT for academic

[85] ITU-D SG2 Document 2/322 from NRD Cyber Security
[86] ITU-D SG2 Document SG2RGQ/182 from Brazil
[87] ITU-D SG2 Document SG2RGQ/183 from Brazil
[88] ITU-D SG2 Document 2/346 from Tanzania

institutions, and eGSoC for government ministries, departments, agencies, and authorities. These developments have enabled increased threat response effectiveness, resulting in enhanced protection, improved overall incident response, and better coordination regarding matters related to specific sectors.

CIRTs, play an indispensable role in safeguarding their own critical infrastructure against cyber threats. By coordinating incident management, sharing threat intelligence, conducting vulnerability assessments, and offering tailored guidance, CIRTs foster the cyber resilience of critical systems, ensuring swift recovery and reducing the impact of cyberattacks. Examples mentioned in this chapter highlight the importance of sector-specific responses, collaboration between public and private entities, and the need for ongoing resilience efforts to protect national infrastructure from sophisticated cyber threats. To ensure that the national CIRTs apply good practices to respond to cybersecurity incidents, and foster technical cooperation among national CIRTs, **ITU** organizes cyberdrills[89] at a regional and intra-regional level. Through cybersecurity exercises, ITU Member States build capacity that promotes readiness, protection, and better incident response.

3.3 Beyond the basics: coordinating for success across borders

As countries develop their CIRTs and deepen their cybersecurity culture, there are steps and models that enable coordination for CI protection beyond the basics. Once a country establishes a strong CIRT and domestic programmes and policies for incident handling, it is essential to look beyond national boundaries and engage in international coordination to prevent, respond to, and mitigate cyber incidents. In today's interconnected world, cyber threats often transcend borders, requiring cooperative strategies to strengthen global cybersecurity resilience. Both the United States and the European Union have developed successful models of international collaboration that demonstrate the importance of such efforts, including relationship building both domestically and internationally.

In the **United States**, the Cybersecurity and Infrastructure Security Agency (CISA) has implemented the Pre-Ransomware Notification programme, a forward-looking initiative designed to identify and respond to ransomware threats before they can cause harm. This programme exemplifies proactive cybersecurity through early warnings, which aim to help organizations avoid critical data loss, operational disruptions, and financial impacts caused by ransomware attacks. The programme relies on two key pillars: robust partnerships, and the systematic collection of actionable intelligence.[90]

The CISA Joint Cyber Defense Collaborative (JCDC) plays a central role by filtering tips from the cybersecurity research community, infrastructure providers, and threat intelligence organizations. Strong relationships with private sector entities and researchers further ensures the timely submission of high-quality intelligence. Once a credible tip is received, JCDC leverages its national and field personnel to notify victim organizations and provide mitigation guidance.

An important part of the programme is its international reach through close coordination with foreign CIRTs. When a threat tip involves an organization outside the United States, JCDC works with its international counterparts to ensure the affected entity is alerted promptly. These CIRT-to-CIRT relationships are indispensable, particularly when swift action is required

[89] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cyberdrills.aspx
[90] ITU-D SG2 Document SG2RGQ/164 from the United States

to prevent ransomware deployment. In cases where ransomware has already been deployed, JCDC supports affected organizations by providing insights into threat actor tactics, techniques, and procedures and assisting with investigative and remediation efforts. This assistance often includes identifying exfiltrated data and offering guidance to mitigate the long-term impacts of an attack.

The **European Union** has similarly prioritized international coordination to enhance its cyber resilience. A prime example is the PESCO Cyber Rapid Response Teams and Mutual Assistance in Cyber Security (CRRT) project.[91] This programme enables the rapid deployment of cybersecurity experts across European Union Member States to respond to large-scale incidents, particularly those targeting critical infrastructure. By pooling expertise and resources, the European Union strengthens its collective ability to address cyber crises both at the national and regional levels. The initiative is also a testament to the European Union commitment to collaborative cybersecurity, as it ensures that European Union Member States can provide mutual support during emergencies.

In addition to these initiatives, both the United States and the European Union, emphasize the importance of sharing threat intelligence, fostering trust, and establishing standardized protocols for cross-border coordination.

As cyber threats continue to evolve in sophistication and scale, coordination beyond borders becomes a critical element of success. The above-mentioned models demonstrate how international collaboration can enhance incident response capabilities and strengthen global cyber protection. By prioritizing cooperation and leveraging the expertise of global partners, countries can better address the challenges of an increasingly interconnected digital landscape.

3.4 Establishing coordination centres

Both Australia and Russian Federation have established national coordination centres and have experienced the benefits of their respective models. For both governments, the national coordination centres are part of a wider, whole-of-government response to cyber incidents. The coordination centres are not CIRTs but work alongside with CIRTs.

The Government of **Australia** established the Cyber Security Response Coordination Unit (CSRCU) under the Department of Home Affairs, following the Optus and Medibank data breaches of 2022. The goal was to create central coordination for nationally significant cyber incidents.[92] The **Russian Federation** established their National Computer Incident Response and Coordination Centre (NCIRCC) following a national law to enhance critical information infrastructure. These centres perform similar tasks: coordinating incident response and communicating critical information. The NCIRCC focuses on the coordination of measures to respond to cyber incidents, and on communication with CI about the means and methods for collecting, storing, and analysing data on such incidents.[93] Both the CSRCU in Australia, and the NCIRCC are empowered to create working groups, involve relevant organizations and experts, and disseminate information and reference materials.

---

91 ITU-D SG2 Document 2/322 from NRD Cyber Security; https://www.pesco.europa.eu/project/cyber-rapid-response-teams-and-mutual-assistance-in-cyber-security/

92 ITU-D SG2 Document SG2RGQ/218 from Australia

93 ITU-D SG2 Document SG2RGQ/79 from the Russian Federation

Chapter 4 – Approaches and good practices, and collected experiences on the implementation of national cybersecurity strategies and policies

As global reliance on digital technologies deepens, the importance of robust national cybersecurity strategies and policies cannot be overstated. Cyber threats are evolving rapidly, targeting both developed and developing nations alike. To protect critical infrastructure, the digital economy, and the privacy of citizens, countries must adopt comprehensive, adaptive cybersecurity strategies. This chapter explores the various approaches and good practices that various countries are employing to build resilient cybersecurity frameworks. By analysing the experiences of different countries, this chapter aims to provide a roadmap for the design and implementation of national cybersecurity policies and strategies.

National cybersecurity policies and strategies encapsulate a broad spectrum of practices, each tailored to the distinct political, social, economic, legal, and technological contexts of different countries. The implementation of these policies and strategies is marked by a unique set of challenges and opportunities, profoundly influenced by each country's specific conditions. This section delves into the practical experiences of various countries, highlighting both the challenges and successes encountered as they work to strengthen their digital protection and resilience against a backdrop of evolving threats.

The discussion extends across critical areas such as strategic alignment, stakeholder engagement, capacity building, and continuous adaptation to the dynamic cyber threat landscape. This comprehensive exploration seeks not only to elucidate the complexities involved in effectively safeguarding national interests in the increasingly contested cyber domain, but also aims to offer strategic insights that can guide policymakers and cybersecurity professionals in enhancing their own strategies.

4.1 Strategic and leadership alignment and policy framework

Successful implementation of national cybersecurity strategies critically depends on aligning these strategies with broader digital transformation, national security, and economic policies. This alignment ensures that cybersecurity initiatives are not only supportive of, but are also integrated with, the country's overall objectives and governance frameworks. For instance, **Republic of Estonia**, widely recognized for its advanced digital society, has effectively aligned its cybersecurity strategy with its e-governance, and digital economy goals, thereby creating a resilient digital infrastructure that supports both public and private sector initiatives.[94] The strategic alignment in Estonia is facilitated through regular updates to its cybersecurity strategy, which are synchronized with changes in the broader technological and geopolitical environment.

[94] https://www.weforum.org/stories/2020/07/estonia-advanced-digital-society-here-s-how-that-helped-it-during-covid-19/

Adding to these insights, effective cybersecurity policies and strategies require alignment with broader national policies and economic objectives. This alignment ensures that cybersecurity measures not only address immediate threats but also support long-term national interests, fostering a secure and resilient digital environment conducive to growth and innovation. Such strategic alignment is necessary for the effectiveness of cybersecurity measures and supports broader national objectives, enhancing the country's capability to prevent, treat and respond to cyber incidents while supporting the growth of the domestic cybersecurity industry.

Democratic Republic of Timor-Leste[95] provides a compelling example of how important it is to emphasize cybersecurity within the context of digital transformation policies, strategies, plans and roadmaps. Timor-Leste recognized that with the digital transformation, cybersecurity risks need to be managed to prevent cyberattacks and data breaches. In this sense, least developed countries (LDC) need to prioritize cybersecurity as a fundamental pillar, reflecting an understanding of the critical role that cybersecurity plays in the digital transformation and digital transformation in the national development.

Ensuring strong and aligned leadership within organizations responsible for national cyber coordination, as an integral part of the wider government cybersecurity community, is another important element to advancing cybersecurity. A designated coordinator can facilitate and drive a whole-of-government response. In this regard, the **Australia** model includes a National Cyber Security Coordinator, whose main function is leading the management of national cyber events. This coordinator position was established in February 2023, and the designated individual reports to the Minister of Cyber Security.[96] In May 2022, the President of the **Russian Federation** issued a decree outlining stringent criteria for appointing individuals responsible for information security, emphasizing eligibility requirements including education and experience in the field, as well as organizational requirements. It also encourages professional retraining for individuals lacking a specialized background in information security.[97]

4.2 Legal frameworks and governance

The **Central African Republic**[98] and the **Democratic Republic of the Congo**[99] exemplify how tailored legislative actions and governance frameworks can significantly enhance cybersecurity capabilities. In the Central African Republic, the Government has initiated legal reforms and established dedicated cybersecurity agencies to enforce its policies, showcasing a proactive approach to strengthening digital defences. Similarly, the Democratic Republic of the Congo has adopted a comprehensive charter based on international good practices, which encompasses policy legislation, multi-level cooperation, and extensive public awareness campaigns. These measures are crucial for countries, particularly in developing regions, to secure their cyberspaces against increasing threats.

Republic of Albania[100] adds another dimension to this narrative with its recent comprehensive cybersecurity reforms. The establishment of a national CSIRT and the restructuring of its cybersecurity authority reflect Albania's commitment to aligning its cybersecurity framework with international norms and good practices. These strategic moves are designed to strengthen

[95] ITU-D SG2 Document 2/120 from Timor-Leste
[96] ITU-D SG2 Document SG2RGQ/218 from Australia
[97] ITU-D SG2 Document SG2RGQ/79 from the Russian Federation
[98] ITU-D SG2 Document 2/141 from the Central African Republic
[99] ITU-D SG2 Document 2/115 from the Democratic Republic of the Congo
[100] ITU-D SG2 Document 2/309 from Albania

Albania's national cybersecurity infrastructure by ensuring a coordinated response to cyber incidents and enhancing the governance of cybersecurity efforts. Additionally, Albania's legal reforms aim to update and fortify the existing legislative framework, ensuring it meets current cybersecurity challenges and threats. This alignment of legal, institutional, and operational elements within Albania's cybersecurity strategy serves as a model for other nations seeking to bolster their cybersecurity defences through holistic governance reforms.

Côte d'Ivoire is also pursuing a range of legislative updates as part of its policy objective of establishing digital trust by 2025.[101] Notable efforts include the enhancement of legal structures to support a trusted information society, aligning with regional standards such as those of the Economic Community of West African States, and the African Union Convention on Cybersecurity and Personal Data Protection. The Telecommunication/ICT Regulatory Authority of Côte d'Ivoire (ARTCI) plays a central role, with a specific focus on digital trust and network security, personal data protection, and the management of electronic transactions. The creation of consultative committees such as the Consultative Committee for Digital Trust, and the Consultative Committee for the Protection of Personal Data, underscores the depth of commitment to fostering a secure cyber environment. These structured efforts aim to build a trusted digital space, enhancing the digital infrastructure security of Côte d'Ivoire and fostering public confidence in the digital economy.

These examples demonstrate the importance of aligning cybersecurity strategies with national governance frameworks, which not only enhances the effectiveness of these strategies, but also ensures their sustainability, and adaptability in the face of evolving cyber threats.

4.3 International collaboration and support

The role of international organizations in supporting national cybersecurity efforts is crucial, as is illustrated by a number of **World Bank** initiatives.[102] The World Bank aids its client countries, especially those categorized as LDCs, by providing both financial and technical support in order to build strong digital foundations and accelerate digital utilization across various sectors. This support is vital for these countries to align their cybersecurity policies and strategies with global developments, ensuring they remain resilient against both current and emerging cyber threats.

The efforts of the World Bank highlight the significant impact of global partnerships, and the sharing of expertise in enhancing national cybersecurity frameworks. By facilitating the integration of cutting-edge technologies and good practices, the World Bank helps countries not only in defence against cyber threats, but also in leveraging digital transformation for economic and social growth.

In **Republic of Haiti**,[103] international partnerships, particularly with the World Bank and the Inter-American Development Bank, provide crucial financial and technical support. This support is essential for developing robust digital infrastructures and enhancing cybersecurity measures across the country.

A key initiative is the joint working group formed by the Haiti National Telecommunication Council (CONATEL), and the Haitian Institute of Statistics and Informatics (IHSI). This joint working group is tasked with developing a harmonized national cybersecurity strategy, focused on

[101] ITU-D SG2 Document SG2RGQ/29 from Côte d'Ivoire
[102] ITU-D SG2 Document 2/74 from the World Bank
[103] ITU-D SG2 Document SG2RGQ/121 from Haiti

protecting critical infrastructures and combating cybercrime. The regulatory role of CONATEL ensures compliance with security protocols, while IHSI manages cybersecurity threats and risks, enhancing the overall security of digital systems in Haiti.

These efforts are supported by international projects such as the Haiti Digital Acceleration Project, which aims to improve broadband connectivity and establish digital resilience. This comprehensive approach not only safeguards Haiti against emerging cyber threats but also supports its socio-economic growth in the digital era. Further reinforcing these efforts, Haiti conducted a comprehensive cybersecurity maturity assessment in collaboration with the Global Cyber Security Capacity Centre, and the World Bank. This assessment involved diverse stakeholders and utilized the Cybersecurity Capacity Maturity Model for Nations to identify critical areas needing strategic investment. The findings have guided targeted improvements to strengthen the cybersecurity infrastructure of Haiti.

4.4 Collaborative frameworks and stakeholder engagements

Brazil[104] has implemented a series of strategic measures aimed at bolstering its national cybersecurity infrastructure through active and inclusive stakeholder engagement. The country's approach emphasizes the importance of collaboration between government bodies, private sector entities, and academic institutions. This multi-stakeholder engagement is facilitated through various initiatives and partnerships that leverage the unique strengths and perspectives of each sector to enhance the overall cybersecurity landscape. One of the recent developments is the creation of the National Cybersecurity Committee, with the purpose of monitoring the implementation and evolution of the National Cybersecurity Policy. The committee has 25 members, 15 members represent entities and bodies of the Federal Public Administration, including Anatel, and 10 represent other organizations, such as the Brazilian Internet Steering Committee (CGI.br), while 3 seats represent civil society, with 3 seats for academia and 3 seats for the cybersecurity-related private sector.

Australia has taken steps beyond its CIRTs to ensure CI protection and resilience, which is a more advanced step in cybersecurity development. Rather than just response and protection, the Critical Infrastructure Uplift Programme (CI-UP) is designed to assist Australian CI organizations in improving their resilience against sophisticated cyberattacks. The programme, run by the Government of Australia, works hand in hand with private sector CI, to harden against attack pathways to CI assets and operational technology environments. CI-UP operates as a voluntary, nation-wide, threat-driven programme.[105]

The primary focus of CI-UP is to help CI organizations improve their cybersecurity posture in several key areas:

- Enhancing visibility and awareness: CI-UP helps entities gain better visibility into cyber incidents and raise awareness of potential vulnerabilities in their systems.
- Incident containment and response: The programme strengthens the ability of CI organizations to contain and respond to cyber incidents effectively.
- Promoting a cybersecurity culture: CI-UP further encourages the development of a cybersecurity-conscious culture across Australia's critical infrastructure sectors.

[104] ITU-D SG2 Documents SG2RGQ/57 and SG2RGQ/181 from Brazil
[105] ITU-D SG2 Document SG2RGQ/214 from Australia

This programme reflects the importance for security of multi-stakeholder collaborations between Government and private sectors. CI-UP delivers these services through a variety of engagement activities, including presentations, workshops, information exchanges, and the provision of detailed mitigation guidance. The programme also works onsite with personnel at Australia's most vital critical infrastructure entities, offering bespoke, in-depth advice, tailored to the specific needs of each organization.

Engaging a broad range of stakeholders is crucial for the effective implementation of national cybersecurity policies and strategies. This engagement includes government agencies, private sector entities, academia, and civil society, each bringing unique perspectives, needs, priorities and expertise to the table. These collaborations help in building, reviewing, improving and refining national policies, and ensure that the implemented strategies are practical and reflective of the needs and realities of all sectors.

4.5 Infrastructure development for cybersecurity

Democratic Republic of the Congo[106] has embarked on an ambitious plan to overhaul and modernize its digital infrastructure. This initiative is driven by the recognition that strong, secure digital systems are the backbone of effective cybersecurity and are essential for national development. The Government has prioritized the upgrade of critical network infrastructure, to not only withstand the growing spectrum of cyber threats, but also to support the digital demands of its expanding economy. The Democratic Republic of the Congo strategy includes the deployment of advanced cybersecurity technologies such as state-of-the-art firewalls, intrusion detection systems, and comprehensive data encryption methods. These technologies are crucial for protecting against unauthorized access, and for safeguarding sensitive information. Additionally, the Democratic Republic of the Congo is working on expanding its broadband access, which is vital for ensuring that cybersecurity measures reach all parts of the country, including remote and underserved areas.

Republic of Burundi[107] is advancing its cybersecurity infrastructure as a core component of its future national cybersecurity strategy. The Government is committed to the digital transformation and digitalization of services, recognizing the vital importance of ICTs for development. In response to escalating cyber threats, Burundi, through the Ministry for Information and Communication Technologies, has established a committee for the development of comprehensive national cybersecurity that includes enhancing legal frameworks to govern cybersecurity, promoting cybersecurity culture, building technical knowledge, and participating in regional and international efforts, and raising awareness of cybersecurity threats across sectors. This infrastructure development is implemented with data protection and security mechanisms to maintain integrity and confidence among users and service providers.

4.6 Capacity building

Building the requisite capacity to implement national cybersecurity strategies involves enhancing the skills of cybersecurity professionals, establishing technological infrastructures, and creating legal and regulatory frameworks. Ongoing investment in training and capacity building is vital for maintaining national cybersecurity. As explored in Chapter 1, by continually developing

[106] ITU-D SG2 Document SG2RGQ/104 from the Democratic Republic of the Congo
[107] ITU-D SG2 Document SG2RGQ/134 from Burundi

the skills of cybersecurity professionals and educating the public, nations can better manage and respond to cyber incidents, while supporting broader goals of economic and social development through enhanced ICT proficiency.

4.7 Continuous adaptation to the cyber threat landscape

The dynamic nature of the cyber threat landscape requires that national cybersecurity policies and strategies be inherently adaptive, as should any other cybersecurity legislation or regulation. Continuous monitoring of the evolving landscape, including the challenges posed by new and emerging technologies, as well as the assessment of policies and strategies effectiveness, and the regular updating of cybersecurity practices, are essential components of this cybersecurity adaptiveness. The necessity of adaptive cybersecurity was discussed in Chapter 2, when addressing cybersecurity assurance practices.

Chapter 5 – 5G cybersecurity challenges and approaches

The introduction of 5G technology represents a significant development in telecommunications, offering faster speeds and better connectivity with the potential to improve industries, expand IoT applications, and bring new approaches to digital communication. However, the sophisticated architecture that enables these advances, brings with it complex cybersecurity challenges that require comprehensive understanding and robust protective measures.

As 5G networks are deployed globally, establishing a secure ecosystem is imperative to ensure the integrity, availability, and confidentiality of information, as well as to protect the infrastructure that has become the backbone of the digital economy.

This chapter presents discussions on the complexities of 5G cybersecurity and aims to share information on existing practices and explore innovative solutions to emerging threats, while sharing reflections and good practices for 5G cybersecurity for public electronic networks that can be considered, and implemented by ITU Member States in their national contexts.

5.1 Overview of 5G cybersecurity

5G is characterized by its advanced software systems that enable more flexible configuration, and massive connectivity of subscribers and devices. 5G technology supports low-latency applications, such as augmented reality, telesurgery, and integrated Internet services, which rely on a robust and reliable network. One of the primary use cases of 5G is the Internet of Things (IoT), which capitalizes on the ability of 5G to connect a vast number of endpoints. 5G technology is poised to revolutionize connectivity, and this also presents new and dynamic cybersecurity risks and challenges.

In a break with previous generations of wireless technologies, 5G introduces a significant shift towards cloud-based architecture, software-defined networks (SDNs), and network function virtualization (NFV). This shift creates a more complex and dynamic cybersecurity landscape.

As 5G becomes more widespread, the telecommunications infrastructure is expected to become an even more attractive target for malicious cyber activity, necessitating advanced security measures that can adapt to evolving threats. Cybersecurity for 5G should focus on increasing the resilience of the entire ecosystem, including the infrastructure and applications. This includes protecting connected devices, data, and networks from cyber threats.

Recognizing that different organizations use different definitions of cybersecurity,[108] it should be borne in mind that the term "5G cybersecurity" in this report refers to cybersecurity in the context of 5G, with its new parameters, standards, and technology features, which need to be properly managed to safeguard the whole digital ecosystem and ensure cyber resilience.

[108] https://www.enisa.europa.eu/publications/definition-of-cybersecurity

Box 1: Definition of cybersecurity

At ITU, cybersecurity is defined in Recommendation ITU-T X.1205, as "*the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following*:

- *Availability*
- *Integrity, which may include authenticity and non-repudiation*
- *Confidentiality*."

5.2 Legacy network deployments

Telecommunication service providers tend initially to deploy 5G networks on a non-standalone (NSA) basis, leveraging existing 4G infrastructure before deploying a standalone (SA) end-to-end network.[109] 5G NSA networks inherit the legacy vulnerabilities of 4G networks, or even 2G/3G networks, which need to be managed accordingly. For some operators, this equates to a "technical debt" where managing older systems means that a set of standardized security controls needs to be developed to measure the security status of infrastructure components at various stages of generational maturity.[110]

It is important to highlight that 5G SA presents opportunities to improve cybersecurity compared to past generations of mobile technology, as it is designed to be more secured than 4G. Improvements have been noted in areas such as subscriber security and privacy, the radio access network (RAN), and network core and roaming security.[111],[112]

5.3 Standards activities in 5G security

5.3.1 SDOs active in 5G cybersecurity

Because of the complexity of 5G technology and the issues involved, there is no one standards development organization (SDO) with an exclusive mandate for 5G cybersecurity work. To

[109] Devices will connect to 5G frequencies for data transmission when needing greater bandwidth and lower latency (such as for communication between smart cars), or to reduce power draw on IoT-enabled devices, but will still rely on 4G and even 2G/3G networks for voice calls and SMS messaging. Source: https://www.gsma.com/get-involved/gsma-membership/wp-content/uploads/2019/11/5G-Research_A4.pdf

[110] https://www.itu.int/md/D22-SG02.RGQ-ADM-0019 and https://www.itu.int/md/D22-SG02.RGQ-ADM-0043

[111] https://www.cisa.gov/sites/default/files/publications/5G_Security_Evaluation_Process_Investigation_508c.pdf

[112] https://www.gsma.com/solutions-and-impact/technologies/security/securing-the-5g-era

prevent duplication, mechanisms have been developed for information sharing between SDOs, and for coordinating proposals and work items.

To help map these different activities and inform the direction of 5G-related security standardization work in the **ITU** Telecommunication Standardization Sector (ITU-T), Study Group 17 (SG17), prepared a technical report mapping existing standards and those under development to SDOs and their application in 5G networks.[113] The report identifies standards from ITU-T, 3GPP, ETSI, and the Institute of Electrical and Electronics Engineers Standards Association (IEEE SA), along with non-standards resources relevant to 5G cybersecurity.

The Study Group has published 11 Recommendations on 5G security, based on submissions drafted by operators, vendors, smartphone manufacturers, content providers, and others. These focus on security in five areas: software defined networks - network function virtualization (SDN-NFV), network slicing, mobile edge, 5G network management, and 5G services. SG17 has established liaisons with other SDOs, such as 3GPP and the Internet Engineering Task Force (IETF), and with industry groups working on specifications having relevance for 5G cybersecurity standardization.

One such industry group is the **GSM Association** (GSMA). Whilst not itself a standards body, GSMA produces specifications, convening its members and engaging with SDOs to get these specifications improved and/or adopted as a standard. GSMA has published a list of baseline security controls that mobile operators can consider, on a voluntary basis, when deploying 5G networks.[114]

Given the numerous sources of information relevant to 5G security, the **European Agency for Cybersecurity** (ENISA), has published a unified repository of technical security controls for 5G networks, the "5G Security Controls Matrix."[115] The repository is currently published as a spreadsheet, but the agency is also developing a web tool to improve usability.

As networks become ever more complex and telecommunications converge with IP networks, it is becoming harder to attribute specific areas of standardization work to individual SDOs. This increases the risk of overlapping and duplication of work, making communication and information-sharing between SDOs even more important.

5.3.2 Incorporating standards in regulatory requirements

Standards help ensure interoperability between technologies and reduce the time needed for an innovation to reach its global market. Cybersecurity standards can define an agreed common security baseline which reflects universal good practices. Standards are the result of consensus-based processes. They can be mandatory, but in most cases, they are optional, leaving vendors and operators more flexibility in their deployment decisions. In some instances, standards can become mandatory if national technical regulations incorporate a specific standard in their security requirements.

National 5G cybersecurity strategies should reflect a balance between global good practices and local operational realities. As a general rule, national regulatory requirements should draw

[113] https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-ICTS-2022-2-PDF-E.pdf
[114] https://www.gsma.com/solutions-and-impact/technologies/security/gsma_resources/fs-31-gsma-baseline-security-controls/
[115] https://www.enisa.europa.eu/publications/5g-security-controls-matrix

on international agreed standards, adapting them to local contexts and local needs in order to ensure the success of 5G deployment and cybersecurity of the networks.

5.4 Complementing standards and specifications with proactive cybersecurity measures

5.4.1 Security considerations at the vendor level

Standards and specifications are only one component of 5G cybersecurity. How vendors and operators implement those standards and configure them defines the security posture of 5G networks. Ericsson has adopted a holistic approach to 5G security, which is addressed in four layers: standards, vendor product development, network deployment, and network operations.[116] The company considers that such a comprehensive approach can ensure that mitigating measures are implemented in a way that does justice to the interdependencies between the layers as well as the specific needs at each layer.

As a concrete example of 5G security measures, the Network Equipment Security Assurance Scheme (NESAS),[117] developed by **GSMA** and **3GPP**, seeks to improve security levels of mobile network equipment by providing an assurance scheme that can be applied globally. The assurance scheme is based on an internal and independent expert audit, being a mixture of assessment between vendors processes and product evaluation, which offers accreditation. The aim of this scheme is to decrease the burden of security testing for network equipment providers which tend to operate at a global scale. Major vendors have already obtained NESAS accreditation. NESAS is also a candidate for the European Union cybersecurity certification scheme on 5G,[118] a European Union-level certification that would provide conformity across the European Union Member States. This certification would not replace the current NESAS scheme but would exist in tandem with it. Developing schemes/certification initiatives in such a way that they remain flexible and can be updated quickly is essential given the evolving threat landscape.

In the **United Kingdom**, the National Cyber Security Centre (NCSC) recommends using the vendor assessment framework[119] guidance that helps operators assess the cyber risks associated with use of the vendor equipment.

5.4.2 Security considerations at the operator level

NESAS can provide a level of assurance that an item of network equipment is secure prior to deployment. As operators deploy and operate their networks, other security considerations need to be integrated, such as attack detection and automated response. This is where operators should consider leveraging artificial intelligence (AI), threat intelligence, and analytics to help support cybersecurity. 5G cybersecurity offers benefits such as real-time security, and strategies such as zero trust which improve system visibility. However, 5G cybersecurity also has its own challenges, such as maintaining connectivity across different networks with varying security levels; working with legacy components and diverse network types; and the complexities of integrating AI into security measures. Applying strict access controls according to the "least

116 https://www.ericsson.com/en/public-policy-and-government-affairs/cyber-network-security
117 https://www.gsma.com/solutions-and-impact/industry-services/certification-services/network-equipment-security-assurance-scheme-nesas/
118 https://www.enisa.europa.eu/news/enisa-news/securing_eu_vision_on_5g_cybersecurity_certification
119 https://www.ncsc.gov.uk/report/vendor-security-assessment

privileges" principle ensures that various rights in the network, such as access rights between network functions, network administrators' rights, and configuration of virtualization, are minimized. A wealth of literature on 5G-specific cybersecurity strategies is available for operators to consider.[120]

Testing of live telecommunication networks is also essential for establishing the true cyber risk to telecommunication networks. Operators can conduct some form of security testing against their own networks and systems, either using internal resources or by employing independent external contractors. In the **United Kingdom**, TBEST is an outcome-based penetration test scheme which simulates the techniques and tactics that well-resourced cyber-attackers may use. TBEST assesses how well a communications provider can detect, contain, and respond to such an attack. The overall aim is to identify and address security vulnerabilities or other weaknesses in provider functions, processes, policies, systems, or networks that could be used together to compromise a company's critical systems before detection. By undergoing the voluntary TBEST scheme, communications providers can identify specific areas in which their security could be improved. Ofcom, the regulator, then works with the provider to help implement appropriate changes in a timely manner.[121]

A strong business case for 5G cybersecurity is essential. While operators need to see a return on their investments in 5G services, compliance with baseline security measures should be recognized as indispensable and budgeted accordingly.

Box 2: Open RAN

Open RAN is the disaggregation of the radio access network (RAN) and standardization of the interfaces connecting those disaggregated elements, making it possible to build networks with equipment from different vendors.

On the one hand, open RAN can bring further complexity to the telecommunication networks' supply chain. This architecture, which encourages vendor diversity in the RAN, requires further integration efforts throughout a network supply chain which can increase the vectors of attack. On the other hand, open RAN adds transparency to supply chains, gives operators more visibility, and allows them to monitor and detect security risks. In short, open RAN improves their understanding of network architecture and equipment and makes possible more comprehensive vulnerability scanning and management. The O-RAN Alliance, the primary source of open RAN specifications, is working on security specifications for open RAN architecture and aiming to get these specifications standardized in ETSI.

In Japan, NTT Docomo is one of the operators that have embraced open RAN architecture because of its flexibility for equipment choices. The decision raised questions from a security perspective because it is generally considered that openness means that there is more opportunity for attacks. However, the operator compared traditional RAN with open RAN and concluded there is little security difference between the two.[1]

[1] For more information on Open RAN security, see for example https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/09/enhancing-the-security-of-communication-infrastructure_79b78b4d/bb608fe5-en.pdf

[120] See for example https://www.5gamericas.org/wp-content/uploads/2020/07/Security-Considerations-for-the-5G-Era-2020-WP-Lossless.pdf and https://www.5gamericas.org/security-for-5g/

[121] ITU-D SG2 Document SG2RGQ/74 from the United Kingdom

5.5 Examples of national policies and regulations to secure 5G network

In addition to the standards and practices of vendors and operators, polices and regulations to secure 5G networks can be proposed at country level. This can take various forms, including vendor assessment, testing, certification, and the establishment of guidelines or requirements. While approaches differ depending on national contexts, these initiatives all aim to mitigate the security risks presented by 5G, including cyber-specific risks. Implementation and compliance regimes should also be considered as part of the overall framework.

The examples below offer snapshots of the actions of various countries and regions to achieve 5G network cybersecurity, and their current status:

- **Brazil**'s holistic approach to 5G cybersecurity focuses on risk management with operators. Under the terms of the 5G spectrum auction and the Cybersecurity Regulation for the Telecommunication Sector,[122] 5G operators are required to comply with the regulatory framework, which includes principles, guidelines, and *ex ante* controls to ensure cybersecurity across the sector. The controls combine cybersecurity governance, mandatory incident notification, information sharing, vulnerability assessment cycles, reporting on critical infrastructure, and other provisions. The Brazilian National Telecommunications Agency (Anatel) has also partnered with academia to conduct studies in this regard.[123]
- The Government of the **United Kingdom** developed a security framework for providers of public electronic communications networks or services through the Communications Act 2003, as amended by the Telecommunications (Security) Act 2021 (the TSA). This framework applies to 5G and all other networks: while the United Kingdom is transitioning to a 5G and full-optical fibre future for all networks, many network providers incorporate older technologies within their infrastructure. The TSA sets out new security duties for all public telecommunications providers[124] and endows the Secretary of State with new powers to make regulations and issue codes of practice, which have since been developed and informed by public consultation.[125] The TSA also includes provisions strengthening Ofcom regulatory powers to monitor and enforce how providers comply with their new duties.
- The 5G cybersecurity regulations and policies of the **Republic of Korea** are recognized as being among the most stringent globally, reflecting the nation's leading position in the adoption of 5G technology. The national Government, through the Ministry of Science and ICT (MSIT) and the Korea Internet & Security Agency (KISA), has implemented a comprehensive framework to safeguard 5G networks. The framework includes stringent cybersecurity requirements for telecommunications operators to secure network infrastructure, protect user data, and mitigate cybersecurity risks. The regulations emphasize the need for secure supply chains, advanced encryption standards, and the deployment of security-by-design principles in network architecture. Additionally, the Republic of Korea collaborates with international partners and standards organizations to ensure that its 5G security measures align with global good practices.
- The legal and technical framework set up to strengthen 5G cybersecurity in **India** includes:

---

122 https://informacoes.anatel.gov.br/legislacao/resolucoes/2020/1497-resolucao-740; https://informacoes.anatel.gov.br/legislacao/resolucoes/2024 (both in Portuguese).

123 Some of the results are available at https://www.gov.br/anatel/pt-br/assuntos/seguranca-cibernetica/estudos-e-pesquisas (in Portuguese).

124 Except micro entities.

125 https://www.legislation.gov.uk/uksi/2022/933/contents/made; https://assets.publishing.service.gov.uk/media/6384d09ed3bf7f7eba1f286c/E02781980_Telecommunications_Security_CoP_Accessible.pdf

- National security directives on the telecom sector, which provides assurance of addressing concerns and vulnerabilities in telecom supply chains and sources;
- Mandatory testing and certification of telecom equipment, which ensures compliance with essential security requirements for each 5G network function; and
- Licensing conditions for telecommunication service providers that include periodic public audits of telecommunication infrastructure security.

To support the above, a variety of institutional mechanisms have been put in place: a National Centre for Communication Security (NCCS), mandated to prepare telecom security requirements/standards (Indian Telecom Security Assurance Requirements, ITSARs), with associated security testing and certification labs; the creation of Telecom-CSIRT, a CSIRT for the national telecommunication sector; and a number of citizen-centric measures for fraud management, consumer protection, etc. With regard to security protocols and standards such as 3GPP, India considered specifications proposed by the industry standards for compliance monitoring, and further telecommunication licence conditions that include regular security audits on service providers' networks.

- In the **United Arab Emirates**, securing 5G networks is approached through a multi-pronged strategy that includes rigorous national cyberdrills and training, the establishment of a National Security Operations Centre (SOC) for real-time threat visibility and response, and the Cyber Pulse initiative, which raises awareness and trains personnel in key defence strategies. The emphasis is on collaboration and information sharing with international partners, vendors, academia, and other stakeholders to strengthen cybersecurity measures. Additionally, a resilient cybersecurity framework in line with international standards, such as those issued by ISO and NIST, has been set up to ensure compliance across the telecommunications sector. To build consumer and business confidence in 5G security the country has put in place governance policies, procedures, and laws that promote secure-by-design principles and responsible security practices among vendors. Finally, the country has adopted a people-centric approach to cybersecurity, focusing on training, awareness, and support to empower individuals and organizations in the fight against cyberthreats, thereby cementing a robust defence against potential threats to the 5G network.
- **Zimbabwe** is tackling 5G cybersecurity, focusing on the emerging importance of edge computing and exploring the adoption of open RAN technology for vendor flexibility. While there is no specific 5G security law in Zimbabwe, existing data protection legislation and an in-progress AI governance document underpin the country's approach. Zimbabwe will align its security practices with international standards such as ISO/IEC 27001 and NIST standards, ensuring that new 5G radio interfaces comply with established security protocols. The Postal and Telecommunications Regulatory Authority of Zimbabwe enforces security guidelines and raises industry awareness to maintain the integrity of the national telecom infrastructure.
- **Kenya** adopted its roadmap and strategy for 5G in mobile communications in April 2022. The strategy recognizes that security is an important aspect of 5G network architecture. The evolving nature of connected services and the expected significant increase in the number and types of devices connected, lend even greater importance to data privacy, data protection, and cybersecurity in Kenya; that includes threat detection, user authentication, and good operational practices. 5G provides better security by design, incorporating enhanced security requirements on the basis of network evolution, and adapting what has been learned from earlier technologies. The Communications Authority of Kenya has adopted an approved international standard developed by ITU and 3GPP to ensure interoperability and security of mobile systems. The Authority plans to leverage the expertise of various stakeholders and international good practices in cybersecurity to develop technical codes and implement a standardized minimum security assessment checklist so as to ensure that 5G networks meet the latest technical standards and are in line with global norms in relation to 5G security.

- Following a wide review of the cybersecurity risks to 5G networks, the **European Union** developed a toolbox of risk mitigating measures[126] with the aim of identifying a common set of measures to mitigate the main 5G cybersecurity risks and help prioritize mitigation measures in European Union-level and national-level plans. The Cybersecurity Strategy for the Digital Decade highlights the importance of safeguarding the next generation of broadband mobile network, and has a specific appendix on next steps for the cybersecurity of 5G networks.[127] The European Union Certification Framework includes the on-going development of a cybersecurity certification scheme for 5G.[128]

5.6 Implementation and compliance challenges

Policy development is essential, as is a focus on effective implementation. Reporting mechanisms, compliance with relevant standards, and practical policy and regulatory enforcement measures are necessary to ensure robust 5G network cybersecurity. New frameworks introducing changes for the security of the telecommunications networks will necessitate an ongoing compliance journey for telecommunication service providers and therefore close engagement with industry. In the **United Kingdom**, Ofcom uses a supervisory model under its telecommunications security policy and engages with the telecommunications providers' regulatory and technical teams. The regulator considers that implementation is not only about technical measures, it also demands a cultural shift in how telecommunications providers think about cybersecurity, requiring them to identify and be accountable for those parts of their networks and services they have outsourced. Engaging at the senior level and getting senior commitment and sponsorship across Government, regulators and industry is a prerequisite for success.[129]

In **Malaysia**, the Government has approved a new cybersecurity bill which provides that a single agency will manage all critical infrastructures. Telecommunications networks, including 5G networks, fall within the scope of this new cybersecurity bill. The regulator[130] is in the process of developing a set of requirements for operators to report on security compliance. As part of Q3/2 interim deliverable on 5G cybersecurity,[131] one of the country's operators highlighted that the implementation of the new policy can be challenging as it involves communicating risk and articulating minimum security requirements, which requires time-, cost- and work-intensive concertation, often impinging on shareholder considerations. For operators with shareholders, the structures, policies and regulations in respect of security are sometimes not congruent, which can pose a challenge for security teams. Accordingly, there is a need to engage all teams, including C-level officials when considering new security frameworks.

5.7 Need to prioritise investment in educating and training the workforce

According to Allied Market Research,[132] the global 5G security market is projected to reach USD 37.8 billion by 2031, with soaring demand for cybersecurity professionals, particularly those with specialized skills for protecting 5G networks. Countries, organizations, and institutions should prioritize workforce training and recruitment to ensure the advancement of 5G

126 https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures
127 https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0
128 https://certification.enisa.europa.eu/index_en
129 ITU-D SG2 Document SG2RGQ/191 from the United Kingdom
130 https://www.nacsa.gov.my/act854.php
131 https://www.itu.int/hub/publication/d-stg-sg02.03.2-2024/
132 https://www.alliedmarketresearch.com/5g-security-market-A12820

cybersecurity. The necessary specialized skills are currently difficult to find in the workforce; furthermore, achieving gender balance in hiring is a challenge. If the workforce is not ready, this will slow and complicate the transition to 5G. While countries should prioritize training and education through national programmes, the private sector can also explore training and upskilling programmes, as participation from the wider industry is required to ensure needs are met.

One example of a country that is finding solutions to the workforce challenges is **Türkiye**, with increased investment in educating and training a workforce capable of managing the complexities of 5G security. As part of this commitment, a 5G Valley open test site has been established by key institutions, including the Information and Communication Technologies Authority, Middle East Technical University, İhsan Doğramacı Bilkent University, Hacettepe University, and telecommunications operators Türk Telekomünikasyon A.Ş., Turkcell İletişim Hizmetleri A.Ş., and Vodafone Telekomünikasyon A.Ş. This site serves as a vital platform for the research, development, and testing of 5G technologies and beyond, providing opportunities for academic and industry collaboration. The 5G Valley executive board, comprising representatives from the aforementioned institutions, ensures the effective implementation of this initiative. By providing a platform where academics, researchers, doctoral students, and start-ups can engage in work related to 5G and beyond, the 5G Valley open test site not only fosters innovation but also contributes to the development of a highly skilled workforce. This initiative is integral to Türkiye's strategy to prioritize and enhance the security of 5G networks through continuous investment in education, training and research.[133]

5.8 Beyond 5G: setting the direction for 6G cybersecurity

Although 5G is still at the planning and deployment stage in many countries and regions, attention in research and development, as well as in the standardization processes, is already moving beyond 5G networks. Thus, at the end of 2023, the **ITU** Radiocommunication Sector (ITU-R) approved the framework and overall objectives of the future development of IMT for 2030 and beyond,[134] commercially known as 6G.

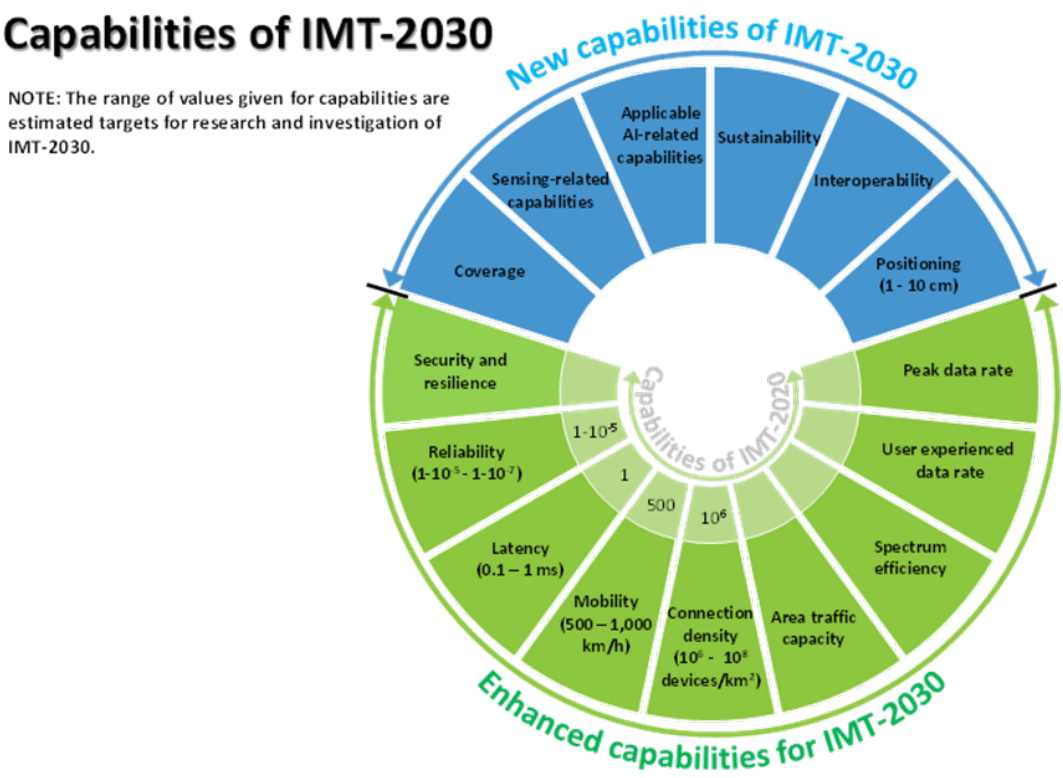
Box 3: IMT-2030

The framework highlights that IMT-2030 is expected to be an important enabler for achieving enhanced security and resiliency. It is expected to be secure by design, and to have the ability to continue operating during, and quickly recover from, a disruptive event, whether natural or man-made. The document also reaffirms that the security and resilience of IMT-2030 systems are fundamental to achieving broader societal and economic goals.

In the context of IMT-2030, security is defined by the framework as the "*preservation of confidentiality, integrity, and availability of information, such as user data and signalling, and protection of networks, devices and systems against cyberattacks such as hacking, distributed denial of service, man in the middle attacks, etc.". Resilience is defined as the "capabilities of the networks and systems to continue operating correctly during and after a natural or man-made disturbance, such as the loss of primary source of power, etc.*".

[133] https://5gtrforum.org.tr/en
[134] ITU-R Recommendation M.2160, available at https://www.itu.int/rec/R-REC-M.2160-0-202311-I/en

Figure 2: Capabilities of IMT-2030



Source: ITU

It has become clear that 6G is being envisioned, and the start of its standardization processes is being conceived, with a robust level of concern related to security and resilience, which is in contrast to the early design stages of the 5G technology, including from a standardization point of view. A comparison with the vision for IMT-2020 (commercially known as 5G) approved in 2015,[135] compellingly illustrates the shift in thinking, with the recognition of the need to properly address cybersecurity and cyber-resilience as an enabling pillar of the digital transformation and digital economy.

[135] ITU-R Recommendation M.2083, available at https://www.itu.int/rec/R-REC-M.2083-0-201509-I

Chapter 6 – Challenges and approaches to addressing smishing

Short message service (SMS) is used by malicious actors as an attack vector. Globally, there has been a significant increase of the use of SMS for spam[136] and text message scams. The latter rely on tactics to deceive users into providing their personal data, including financial data, and in downloading malware to their devices. SMS scams not only reduce user confidence in telecommunications messaging services as well as their satisfaction levels, but are also a waste of network resources.

Data form the United Stated Federal Trade Commission indicate reported losses of USD 330 million to text message scams in 2022, more than doubling that reported in 2021.[137] For the same period, in Australia, the Scamwatch programme from the National Anti-Scam Centre has received almost 80 thousand reports of text message scams that accounted for more than AUD 28 million.[138]

Although the use of SMS services varies across countries, and innovation in the telecommunications/ICT sector has delivered new ways of communicating, including through the worldwide spread of mobile messaging applications, the SMS service remains valuable to users given its simplicity and its availability on all mobile phones.

In this context, this chapter considers 'smishing', which is one of the most prevalent types of SMS incident, standards recommendations to combat smishing, and some national experiences and approaches to facing such challenges.[139]

6.1 Smishing

The term 'phishing' applies to the use of emails, messages, voice calls, or social media messages that appear legitimate but aim to deceive the recipient, usually through impersonating a trustworthy person, or entity such as a bank, government agency, employer or family member. The user is often directed to a website where they will input personal details resulting in identity theft, or the user may be induced to provide personal information such as bank or credit card information, or to make a payment to a fake account.

In the cybersecurity domain, one of the most increasingly common types of scam is 'smishing', a term that combines the words 'phishing' and 'SMS' and refers to the phishing messages delivered to mobile phones through SMS texts. According to Supplement 29 to Recommendation ITU-T X.1242,[140] smishing is "*an attack in which the user is tricked into downloading a Trojan horse, virus or other malware onto his cellular phone or other mobile device*" and phishing is defined as an

[136] Spam is defined as ''*the electronic information delivered from senders to recipients by terminals such as computers, mobile phones, telephones, etc., which is usually unsolicited, unwanted, and harmful for recipients*" by Recommendation ITU-T X.1242 – https://www.itu.int/rec/T-REC-X.1242-200902-I

[137] https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/06/iykyk-top-text-scams-2022

[138] https://www.scamwatch.gov.au/research-and-resources/scam-statistics

[139] This topic has an important intersection with wide telecommunication services and online anti-fraud activities. The Final Report of Question 6/1 (Consumer information, protection and rights) has a dedicated item on online fraud.

[140] https://www.itu.int/itu-t/recommendations/rec.aspx?rec=13409

"*attack to acquire sensitive information such as usernames, passwords, and credit card details for malicious reasons, by masquerading as a trustworthy entity in an electronic communication*".

Smishing attacks have become a growing threat over recent years, and the use of artificial intelligence (AI) tools have intensified their prevalence, highlighting both the scale and increasingly sophisticated nature of this new type of cyber-attack. In 2022, more than half of personal mobile devices, and a quarter of mobile enterprise devices had encountered at least one phishing attack every quarter, with smishing, a non-email-based phishing attack, increasing by more than sevenfold in the second quarter of 2022.[141]

Sometimes it is hard for the users of communication services to identify this type of attack. By leveraging social engineering techniques, malicious actors send fake messages to mobile devices, tricking the recipients into clicking on URL links contained in these messages. Cybercriminals may use URL shortening services to hide fake login links, making it more difficult to determine whether the message is from a scammer. There are a few key signs that a message is fraudulent, such as the message having nothing to do with the recipient; the message is often imbued with a sense of urgency; the message is sent from an unfamiliar phone number; the message contains spelling and grammatical errors; and the message contains a suspicious link.

Users need to be aware of the risk and of the steps they can take to avoid becoming a victim of a smishing attack. There are also important roles for service providers to play, as well as for the public sector, that not only can work with the telecommunications sector to ensure that standards and good practices are being followed, but can also promote awareness about smishing within the population.

6.2 Approaches taken to combat smishing

6.2.1 Countries' approaches to combat smishing

During the study cycle, ITU Member States focused on developing regulation, raising awareness, collaborating with private sectors, and engaging in international cooperation to combat smishing. While there are many ongoing efforts to address the challenges posed by smishing, it is clear that there is not a one-size-fits-all solution to this problem, and that there is a need for a multifaced approach including considering these attacks as criminal offences.

This latter approach has been adopted by the **Russian Federation**[142] that qualifies the actions of telephone scammers, including smishing scammers, as a criminal offence under art. 159 of the Criminal Code of the Russian Federation. In addition, the Russian Federation administration has adopted measures to ban the renting out of virtual mobile numbers, and these measures entered into force in September 2024. The renting of virtual mobile numbers was recognized as a security threat, as malicious actors use temporary numbers to create accounts in social networks and message applications, to spread threats. Another measure adopted by Russian Federation administration was the launch of an antifraud platform to provide telephone call verification. With the help of the platform, connected telecommunication service providers verify numbers and check their authenticity, blocking suspect calls and SMS, before the can reach the recipient. Connecting to the system, which is obligatory for all telecommunication services approved to provide voice communication services is free of charge, but non-connection will

[141] https://www.lookout.com/documents/reports/Global-State-of-Mobile-Phishing-Report.pdf
[142] ITU-D SG2 Document 2/158 from the Russian Federation

lead to a fine of between RUB 600 000 and RUB 1 million. These initiatives have also been complemented by awareness campaigns to empower users.

A comprehensive approach has also been adopted by the Government of **Australia** encompassing industry and government initiatives together with awareness-raising efforts. Combatting SMS scams has been a compliance priority in recent years for the Australian Communications and Media Authority (ACMA) which unveiled a series of new rules. These rules included: requiring telecommunications providers to identify, trace and block scam calls and scam texts; mandating stronger identity verification processes before mobile numbers can be transferred between providers; and mandating stronger identity verification processes for high-risk transactions including SIM swap and account change requests, etc. The authority audits telecommunication service providers who send bulk text messages, and these enforcement actions have revealed that malicious actors have exploited vulnerabilities created by non-compliance, to send high-profile SMS scams to Australians.[143]

Other enforcement activities undertaken by the ACMA to combat telecommunications scams include: issuing consumer alerts about government agency impersonation and remote access scams; working behind the scenes with telecommunication service providers, government agencies, and well-known brands to disrupt phone scams; and undertaking international cooperation with other nations and international regulators to strengthen strategic engagement in the global fight against scams, unsolicited telemarketing, and spam.

Additionally, the Government of Australia embarked on the phased roll out of specific anti-fraud measures in 2023, including the establishment of a National Anti-Scam Centre (NASC), the development of a webpage takedown function to remove pages established for investment scams, and the introduction of a SMS sender ID registry.

Cooperation and the partnership between the involved actors has been a consistent approach employed by a number of countries and is the cornerstone of initiatives undertaken in the **Republic of Korea**. The country has facilitated the sharing of threat intelligence on smishing tactics to allow faster identification and mitigation of new attack vectors, as well as automated reporting systems to be used by users and shared with telecommunication service providers for blocking purposes.

AI tools can also help combat smishing, as is the case for example in the Republic of Korea where the Ministry of Science and ICT (MSIT) and the Korea Internet & Security Agency (KISA) implement a range of measures designed specifically to address smishing, including:

- real-time monitoring and blocking of smishing messages through an AI-based detection and filtering system that analyses SMS patterns,
- flagging of suspicious messages for blocking, and detection of malicious URLs within SMS content;
- creation of a database of malicious numbers maintained by, and shared with telecommunication service providers;
- implementation of AI-powered filtering systems; and
- creation of a national reporting hotline (118) and online portals operated by KISA.[144]

[143] ITU-D SG2 Document 2/154 from Australia
[144] ITU-D SG2 Document 2/312 from the Republic of Korea

These activities exemplify the importance of tackling several dimensions of the phenomena, with the need to engage the telecommunication service providers; to embrace new and emerging technologies to assist in analysis, filtering, and blocking; to implement necessary procedures and processes; to develop and maintain a reporting system; to make use of the reporting data; and also, to work intensively on the awareness of the population. The relevance of raising awareness of the users cannot be underestimated. Malicious actors frequently change, refine, and reinvent their methods and a well-informed, empowered, and aware user has a far higher chance of not becoming a victim.

6.2.2 Industry approaches to combat smishing

The telecommunication industry has taken positive steps to combat and mitigate the impacts of smishing, and of scams in general. In terms of technical methods, providers have introduced measures such as reporting mechanisms, SMS firewalls, blocking of known phishing site URLs, and SMS sender ID protection registries. SMS firewalls can stop large amounts of unwanted messages from reaching users, and SMS sender ID registries allow organizations to register and protect the message headers used when sending SMS to their customers, limiting the impact of smishing and spoofing. Scam reporting, when carried out in a coordinated way across multiple mobile operators, is an effective way of identifying and removing scams. The 7726 reporting service implemented in the **United Kingdom** and **Canada** allows reporting of suspicious messages for investigation.[145] The four main mobile operators in the United Kingdom in 2014, working with the United Kingdom Information Commissioner's Office, voluntarily implemented the 7726 reporting service for people to forward suspicious texts, as well as spam, free of charge. As of March 2025, 26 000 scam numbers have been removed.[146]

Authorised push payment (APP) fraud is another issue which results in significant financial loss to consumers due to criminals contacting victims through SMS or phone calls pretending to be from a legitimate organization, such as a bank, and then extracting a payment transfer. **GSMA** and **UK Finance** convened the United Kingdom mobile operators and banks to deliver 'Scam Signal', a solution that uses an application programmable interface (API) to enable banks to better identify and stop fraudulent transfers.[147]

In many Sub-Sahara African countries where mobile money services are very popular, enhancing security on these platforms is a critical focus. 'M-Pesa' in **Kenya**, and similar services in other countries, have integrated biometric authentication, improved encryption, and enhanced fraud detection systems to protect users from impersonation and phishing attacks.[148] Globally, operators across all regions are deploying various APIs such as 'Number Verify' which removes the need to use another authentication method such as one time pin (OTP) and password, and instead checks that the user is interacting with a service from a device with the pre-registered/paired mobile phone number. 'Know your customer' (KYC) processes are increasingly used to provide a safer onboarding process, including for mobile money services, by validating user contact information and mitigating identity theft.

---

145 https://www.ofcom.org.uk/phones-and-broadband/scam-calls-and-messages/7726-reporting-scam-texts-and-calls/; https://www.getcybersafe.gc.ca/en/blogs/reporting-spam-text-messages-7726

146 ITU-D SG2 Document 2/393 from the United Kingdom

147 https://www.gsma.com/newsroom/press-release/mobile-and-banking-industries-join-forces-to-fight-fraud/

148 https://www.gsma.com/solutions-and-impact/connectivity-for-good/public-policy/social-engineering-and-impersonation-fraud/; https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/wp-content/uploads/2024/05/Mobile-Money-Fraud-Typologies-and-Mitigation-Strategies-20.05.24.pdf

Telstra, the biggest telecommunication operator in Australia, operates an SMS scam filter to scan the content of messages, looking for suspicious patterns and characteristics, and then identifies and blocks any malicious messages containing suspicious links or phone numbers.[149] Telecommunication providers also partner with the banking sector to address phone scams. For example, Australia's second largest telecommunication provider, **Optus**, launched a 'Call Stop' initiative jointly with the Australian Financial Crimes Exchange, and banking members including the major banks.[150] Targeting call back scams, the programme prevents Optus customers from dialling the identified scam number, then instead forwards the call to an automated message to warn them against scam risk. Informing the users of preventive methods is also carried out by banks and telecommunication operators to consolidate efforts to combat smishing and telecommunication fraud.

The **GSMA** facilitates collaboration and intelligence sharing through the Fraud and Security Working Group (FASG)[151] and the Telecommunication Information Sharing and Analysis Center (T-ISAC).[152] Both are secure platforms to help facilitate real-time information sharing on a global scale.

Efforts to combat smishing and telecommunication scams require strong partnerships among all stakeholders. Government alone cannot disrupt scam activities. Following ACMA registration and enforcement of rules to identify and block scam calls in December 2020, and scam text messages in July 2022, telecommunication providers have reported blocking of over 1.4 billion scam calls and over 257 million scam messages to the end of June 2023.[153]

Moreover, public information campaigns about scam reporting should be considered to increase the numbers of reports. In the **United Kingdom**, some organizations, such as the National Cyber Security Centre and some local police forces have publicised the existence of the 7726 reporting service, and Ofcom, the communications regulator, has set out simple instructions in a step-by-step video format, explaining how to report both texts and calls to 7726 on most major smartphone models. Recently, the incorporation of a spam reporting button on the vast majority of smartphones in the United Kingdom market has hugely increased the rate of reported scam messages. This new functionality acts in the same way as reporting to the 7726 service, with the information being shared with mobile operators through the shared third-party database. This change has resulted in an increase in reports by about 800 per cent over one year.[154]

As measures taken to date have generated positive results, a holistic approach that spans different stakeholders including government authorities, banks and telecommunication operators, plus users, should be considered.

149 ITU-D SG2 Document 2/154 from Australia
150 *Ibid.*
151 https://www.gsma.com/get-involved/working-groups/fraud-security-group/
152 https://www.gsma.com/solutions-and-impact/technologies/security/t-isac/
153 ITU-D SG2 Document 2/154 from Australia
154 ITU-D SG2 Document 2/393 from the United Kingdom

Conclusions

The use of telecommunications/ICTs has been invaluable in fostering development and social and economic growth globally. Securing information and communication networks and developing a culture of cybersecurity are key in today's world, especially as the adoption and use of telecommunications/ICTs continues to rise. During this study period, Question 3/2 considered numerous aspects of cybersecurity, examining contributions from the ITU membership, and holding two workshops that have informed this report and its conclusions.

Chapter 1 revealed that cybersecurity awareness initiatives have ranged from wide-encompassing programmes targeting various parts of the population, to specific interventions focused on themes such as cybersecurity hygiene, and scams awareness. Similarly, Member States' cybersecurity education and training policies have revealed different levels of maturity. Some countries have implemented fully-fledged strategies aimed at mitigating the shortage of cybersecurity professionals, while others have opted for more specific training solutions targeting components of the workforce. Member States have rightly emphasized child online protection initiatives, implementing of robust legal frameworks, and developing of pragmatic tools and programmes to make the Internet safer for children.

Chapter 2 explored a wide range of cybersecurity assurance practices which have emerged as a critical element in protecting networks, systems and data from malicious activities. Although they do not directly prevent cyberattacks, their goal, if correctly implemented, is to minimize the risk of such attacks. While there is no one single approach to be recommended, the sample of initiatives have shown a sustainable shift towards the adoption of these practices worldwide, with national authorities often using different and a mix of approaches, ranging from self-assessments and voluntary guidelines, to labelling schemes and strict compliance checks.

Chapter 3 highlighted how CIRTs serve an essential role in increasing the cyber resiliency of a country. Their establishment and functioning should be further prioritized in developing countries. ITU can offer CIRT assessments and CIRT development for countries aiming to increase their CIRTs capacity for CI resilience.

Chapter 4 discussed approaches and experiences in national roadmaps that can guide the enhancement of national cybersecurity frameworks. It emphasizes that while the cyber threat landscape is continuously evolving, the foundational principles of comprehensive planning, inclusive stakeholder involvement, and proactive adaptability remain central to successful cybersecurity strategy implementation. Moving forward, it is these principles that will continue to shape the resilient cybersecurity defences necessary to safeguard national interests in an interconnected world.

Chapter 5 focused on cybersecurity measures to secure 5G networks. Standards and specifications have been developed across SDOs and industry groups, and their implementation should be complemented with proactive cybersecurity measures from vendors and operators as well as national policies and regulations. These can take various forms depending on national contexts including vendor assessment, testing, certification, and the establishment of guidelines or requirements.

Finally, Chapter 6 considered efforts to combat telecommunication scams, with a focus on smishing, and stressed the need for strong partnerships among public and private sectors.

The chapter highlighted successful examples of government and industry initiatives in tackling the rise of smishing. User awareness and education is also critical, especially as these attacks become more sophisticated and harder to detect.

As for the future of Question 3/2, as long as the global cybersecurity landscape continues to evolve, the need to share information and approaches about cybersecurity will remain vital. There are merits in retaining this topic in the next study cycle, albeit with a review of terms of reference that lend greater focus to specific cybersecurity issues reflective of the mandate and audience of the ITU-D study group.

Annexes

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

Contributions for Question 3/2

Web	Received	Source	Title
2/408	2025-04-29	RIFEN	Securing contractualization and deed production during the real estate sales process via blockchain technology and machine learning: practices and use cases
Describes the integration of blockchain technology and machine learning solutions for securing real estate transactions. Together, these technologies strengthen stakeholder confidence, while improving the efficiency of real estate transactions. This contribution takes into account existing work and provides an overview of the system we have implemented in Cameroon for the sale of real estate.			
2/405	2025-04-28	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
This contribution provides an update on the activities currently being undertaken by BDT to enhance cybersecurity in ITU Member States. It also highlights future actions envisaged and new initiatives being formulated.			
2/393	2025-04-23	United Kingdom	Scam reporting within the UK
Summarises how the largest mobile operators in the United Kingdom voluntarily provide the 7726 reporting service, as a way of identifying, removing, and preventing scams calls and messages.			
2/392	2025-04-2025	RIFEN	Developing countries: strengthening cyber-security
Describes how developing countries face multiple and complex cybersecurity challenges, but with limited means to address the question of how they can ensure that disparities in technical capabilities and funding do not hamper their efforts to enhance cybersecurity.			
2/370	2025-04-14	China	Jointly building cybersecurity: typical practices of safeguarding cyberspace security
Provides an overview of the laws and regulations enacted by China to safeguard cyberspace security, the national campaigns launched to raise people's awareness of cybersecurity, as well as the international initiatives proposed by China on cybersecurity, with the aim of providing reference practices and paths for the world to build secure cyberspaces together.			
2/350	2025-02-27	RIFEN	Artificial intelligence for the detection and reporting of online cyberbullying
Presents the challenge to combat online harassment and the opportunity to integrating artificial intelligence, particularly deep learning techniques, as a promising avenue for improving the protection of sensitive data. The contribution highlights the advantages of designing an intelligent system capable of proactively and automatically identifying threats by combining advanced analysis techniques with proactive cybersecurity strategies.			

(continued)

Web	Received	Source	Title
2/346	2025-02-04	Tanzania	Best practices for coordinating efforts and developing cybersecurity culture
Highlights good practices for coordinating efforts to promote a culture of cybersecurity in Tanzania. It outlines how various legal, technical, organizational, and capacity development measures, along with cooperation, have been vital in enabling Tanzania to achieve a "Tier 1" ranking and be recognized as a "role model" in the Global Cybersecurity Index (GCI) published by the International Telecommunication Union (ITU). It also identifies areas for continuous improvement, especially in technical and capacity development measures.			
2/TD/10 +Ann.1	2024-11-12	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
Reports on the recently conducted CIRT Maturity Assessments in Azerbaijan, Bhutan, Sierra Leone, and Tanzania, the cyberdrills carried out in 2024 to enhance incident response readiness across different regions, the launch of the 5th edition of the Global Cybersecurity Index, BDT assistance in countries and territories in the assessment of their cybersecurity strategies, the Women in Cyber Mentorship Programme and the Her CyberTracks programme, the launch of new online safety tools for children and ongoing capacity building efforts, and other initiatives.			
2/339	2024-11-07	Republic of the Congo	Online communication and transactions via new and emerging telecommunications/ICTs, such as the Internet of Things (IoT)
Outlines challenges in consumer protection with the rise of IoT technology. It highlights issues with data protection, privacy, fair business practices, and device security. Various international responses include legislation, certification, monitoring, and technical standards to safeguard consumer rights and ensure device security.			
2/329	2024-10-29	Egypt	Egypt capacity building centre for African countries (EG-ATRC)
Details Egypt's dedication to enhancing African nations' communication and information technology skills via the Egyptian African Telecom Regulatory Training Centre (EG-ATRC), providing ITU-accredited training and hosting 381 participants from 30+ countries.			
2/322	2024-10-29	NRD Cyber Security	Strengthening cyber resilience: the role of Lithuania's national CIRT in critical infrastructure protection
Presents a case study on Lithuania's National Computer Incident Response Team within the National Cyber Security Centre, highlighting its functions in critical infrastructure protection through monitoring, incident handling, threat analysis, and collaboration efforts, including European Union initiatives.			
2/320	2024-10-29	Australia	Mandating a minimum standard for consumer-grade smart devices
Describes Australia's transition to mandatory smart device security standards from voluntary security standards, prompted by poor guideline adoption. A Bill proposes enforceable Internet of Things standards, requiring compliance statements from manufacturers and suppliers, and introduces a regulatory model with update flexibility.			
2/312	2024-10-28	Republic of Korea	Challenges and approaches to addressing smishing and SMS incidents in South Korea

(continued)

Web	Received	Source	Title
Examines smishing threats in the Republic of Korea, detailing the Ministry of Science and ICT and Korea Internet & Security Agency countermeasures, challenges, and government strategies such as AI detection, awareness campaigns, and international cooperation, with recommendations for improvement.			
2/309	2024-10-25	Albania	Creation of a safer cyber ecosystem in a country: the case of Albania
Summarizes Albania's post-cyberattack cybersecurity reforms, including legal and strategic updates, new operations centres, human capital investment, and enhanced international cooperation with entities like the UN and NATO, leading to stronger legal frameworks and preparedness.			
2/301	2024-10-22	China	Mobile anonymous subscription service based on data security protection
Proposes a service for user privacy protection by using temporary numbers and anonymous IDs, with a focus on balancing privacy and digital economy growth, detailing a system architecture that ensures availability, scalability, reliability, usability, observability, and audit logs.			
2/300	2024-10-22	China	Based on anonymous data exchange network, release the value of telecommunications data
Examines the importance of telecommunications data in the digital economy and the challenges of using it, such as privacy issues and integration with Internet data. It details the China Academy of Information and Communications Technology creation of an anonymous data network, enhancing financial risk management and advertising, and supporting sustainable growth and employment in line with the United Nations Sustainable Development Goals.			
2/299	2024-10-22	China Telecommunications Corporation	Building security capabilities to alert phishing websites
Outlines the difficulties the elderly encounter with digital threats such as phishing, and details the China Telecom security tool, which shields them through gateway plug-ins, cloud engines, and a security database, serving over 10 million users in 31 provinces.			
2/276	2024-09-30	Côte d'Ivoire	Cybersecurity in action: strategies and challenges in a connected world - experience of Cote d'Ivoire
Presents the "O'KOHI" web series by a Platform for the Fight against Cybersecurity (PLCC), designed to educate on cybersecurity via videos. Funded by ARTCI and the *Ministère de l'Economie Numérique, des Télécommunications et de l'Innovation*, it addresses hacking, data protection, and cyberattacks, ensuring content accuracy through expert collaboration.			
2/273	2024-09-29	RIFEN	Machine learning-based CVE and CWE analysis
Highlights the need for machine learning to automate Common Vulnerabilities and Exposures (CVE) and Common Weakness Enumeration (CWE) analysis, improve identification and prioritization of software vulnerabilities, and overcome challenges such as data quality and model complexity through solutions including data validation and continuous learning. It advocates for collaboration to enhance cybersecurity.			
2/271	2024-09-29	RIFEN	Cybersecurity and cyberspace protection in developing countries

(continued)

Web	Received	Source	Title
Examines the Internet and information and communication technology impact on Africa's socio-economic progress, addressing cyberattack risks and the necessity for collaborative security efforts. It discusses Africa-specific challenges, infrastructure vulnerabilities, and advocates for a multi-stakeholder strategy to safeguard essential Internet resources.			
2/268	2024-09-24	RIFEN	Cybersecurity awareness for rural youth through online training organized by RIFEN-SADA
Outlines the RIFEN-SADA (Smart Africa Digital Academy) cybersecurity training, which enhanced awareness and skills in cybersecurity among young Africans through fourteen modules. It fostered a security-conscious culture, practical protection knowledge, and guided talent development, leading to certifications and improved job prospects.			
2/254	2024-09-19	Co-Rapporteur for Question 6/1; Co-Rapporteur for Question 3/2	Report of the workshop on Increasing Consumer Awareness Mechanisms to Promote Informed Consumer Decision: A joint workshop for Question 6/1 and Question 3/2 held in Brasilia from 18-20 June 2024
Presents the workshop on consumer protection in the digital age, discussing infrastructure in underserved regions, security, digital literacy, and data privacy. It stressed digital inclusion, consumer behaviour, and skill gaps, concluding with good practices for ITU deliverables.			
2/246	2024-09-16	RIFEN	Securing the contracting procedure and the production of deeds of purchase in the real estate sale process using blockchain technology and machine learning
Discusses how blockchain technology and machine learning are revolutionizing the real estate industry by enhancing security, efficiency, and decision-making in the sales process. It highlights the benefits of smart contracts and improved market analysis, while acknowledging the challenges of adoption and regulation.			
2/242	2024-09-12	Central African Republic	Operationalization of CSIRT/SOC/PKI platforms and training
Outlines the Central African Republic's cybersecurity measures post-broadband expansion, including the deployment of a Security Operations Centre - Computer Security Incident Response Team (SOC-CSIRT) and public key infrastructure (PKI) systems, and requests Union support for network security.			
RGQ2/218	2024-04-29	Australia	National Office of Cyber Security and the Cyber Security Response Coordination Unit
Presents the Cyber Security Response Coordination Unit, the National Office of Cyber Security and the National Cyber Security Coordinator, entities established by the Government of Australia within the Department of Home Affairs for central coordination, following the Optus and Medibank data breaches of 2022.			
RGQ2/214	2024-04-19	Australia	Critical Infrastructure Uplift Program (CI-UP)
Outlines the Critical Infrastructure Uplift Programme (CI-UP) in Australia, designed to enhance cyber security and resilience of critical infrastructure against cyber-attacks. It details CI-UP activities and emphasizes the voluntary and collaborative nature with industry partners.			

(continued)

Web	Received	Source	Title
RGQ2/212	2024-04-18	China Mobile Communications Co. Ltd.	China's initiatives to protect the cyber-security rights and interests of minors
Presents the critical nature of cybersecurity for Chinese minors, addressing their high online presence, urban-rural digital divide, and exposure to risks such as addiction and privacy violations. It underscores China's advancements in safeguarding minors' Internet use and the collective role of government, industry, and society in bolstering cyber-security education and safety.			
RGQ2/201	2024-04-16	Saudi Arabia	Cost estimation tool for cybersecurity controls
Outlines the National Cybersecurity Authority (NCA) development of the "ECC Cost Estimation Tool" to aid Saudi organizations in budgeting for cybersecurity compliance. It details the creation process, including research, implementation and testing phases.			
RGQ2/191	2024-04-16	United Kingdom	Considerations in implementing a new and significant regulatory security framework for the telecoms sector: an example from the UK's Telecoms Security Act (TSA)
Outlines the United Kingdom new telecoms security framework under the Telecommunications Security Act 2021, detailing enhanced security duties for providers, a tiered approach based on turnover, and the Ofcom role in ensuring compliance and fostering a collaborative security culture.			
RGQ2/184	2024-04-15	Brazil	Creating cybersecurity capabilities: Hackers do Bem
Describes Brazil's "Hackers do Bem" ("White Hat Hackers") initiative, aiming to train 30 000 students in cybersecurity through a five-level curriculum, with government support, to build a national hub, boost employability, and strengthen the cybersecurity ecosystem.			
RGQ2/183	2024-04-15	Brazil	Cybersecurity in Brazilian National Research and Education Network: CAIS
Outlines the work of the Brazilian National Research and Education Network (RNP), which created the first network security centre in Brazil in 1995 (CAIS). CAIS serves as CSIRT for the Brazilian academic network, being the focal point for security incident notifications and providing coordination and support for the incident handling.			
RGQ2/182	2024-04-15	Brazil	Brazilian Federal Cyber Incident Management Network
Presents the Brazilian Federal Cyber Incident Management Network (ReGIC), presenting the two CSIRTs with national responsibilities, such as the Brazilian National Computer Emergency Response Team (CERT.br) and the Centre for Prevention, Treatment and Response to Government Cyber Incidents (CTIR Gov), as well the CSIRT ecosystem in Brazil.			
RGQ2/181	2024-04-15	Brazil	Brazilian National Cybersecurity Policy
Summarizes Brazil's National Cybersecurity Policy and the formation of the National Cybersecurity Committee, detailing its principles, goals, and tasks like promoting cybersecurity, resilience, education, and global collaboration, with diverse members overseeing policy execution.			
RGQ2/170	2024-04-04	Russian Federation	Implementation of the educational project "Digital Literacy Campaign" in the Russian Federation

(continued)

Web	Received	Source	Title
Outlines the Russian Federation's "Digital Economy" programme for human capital and economic growth by 2024, including "Digital Literacy Campaign" with partners like Kaspersky Lab to educate children on digital safety through animated videos.			
RGQ2/165	2024-04-02	Brazil	Meaningful connectivity
Summarizes the Anatel 2023 Strategic Planning, highlighting digital transformation and meaningful connectivity, which encompasses a cyber safety perspective. It details cyber hygiene initiatives, including the launch of a dedicated page to combat digital scams and frauds.			
RGQ2/164	2024-03-29	United States	U.S. Pre-Ransomware Notification capability
Details the CISA Pre-Ransomware Notification programme to pre-empt ransomware attacks. It emphasizes early warnings, international cooperation, and the success of the #StopRansomware campaign in averting threats in 2023.			
RGQ2/163	2024-03-26	Syrian Arab Republic	A paper on digital development in Syria and the current reality
Summarizes the Syrian Arab Republic digital transformation strategy for government services, detailing a phased approach from 2021 to 2030, encompassing e-government services, citizen centres, and cybersecurity. It includes strategic axes, programmes, and annexes on Internet capacity and security.			
RGQ2/160	2024-03-26	RIFEN	Initiatives to strengthen digital trust in Côte d'Ivoire
Highlights Côte d'Ivoire's National Digital Development Strategy 2021-2025, aiming to transform the nation into West Africa's digital hub by improving digital skills, cybersecurity, and women's tech inclusion, and by creating a national data centre.			
RGQ2/155	2024-03-26	RIFEN	Building a resilient security culture: a comprehensive approach to cybersecurity enhancement
Highlights the need for a robust cybersecurity culture in organizations, advocating for comprehensive strategies such as employee training, simulations, incident response teams, access control, encryption, and continuous monitoring to combat cyber threats.			
RGQ2/149	2024-03-15	Democratic Republic of the Congo	Development of cybersecurity in the Democratic Republic of Congo: issues and strategies for the protection of ICT infrastructures and digital actors
Outlines the Democratic Republic of the Congo's cybersecurity challenges, including its vulnerability to cyberattacks and the lack of a national strategy, legal framework, and incident reporting. It mentions a workshop for creating a national CIRT and ITU strategy support.			
RGQ2/140	2024-03-11	RIFEN	Internet and ICT: development levers and cybersecurity challenges in developing countries
Highlights the importance of Internet and ICTs for development, stressing security against cyberthreats. It combines research with expert opinions, identifies vulnerabilities, and addresses Africa's connectivity issues, advocating for information sharing, legislation, and collaboration to protect digital infrastructure.			

(continued)

Web	Received	Source	Title
RGQ2/134	2024-03-05	Burundi	Implementation of a national cybersecurity strategy
Outlines the significance of information management and ICTs for a country's progress, emphasizing the necessity of cybersecurity measures in light of rising cybercrime. It details Burundi's efforts, supported by ITU, to create a national cybersecurity strategy by 2040, concentrating on legal structures, infrastructure security, and skill development.			
RGQ2/130	2024-02-29	RIFEN	Côte d'Ivoire's cybersecurity initiatives
Outlines Côte d'Ivoire's cybersecurity strategies, including the Platform for Combating Cybercrime and CI-CERT, stressing public awareness and education to foster a cybersecurity culture and safeguard the online space, particularly during events like the African Cup of Nations.			
RGQ2/128 +Ann.1	2024-02-29	Syrian Arab Republic	Cybersecurity strategy in Syria
Summarizes the Syrian Arab Republic cybersecurity strategy, focusing on creating a strong infrastructure, handling threats, legal development, capability enhancement, research, governance, and international collaboration via six programs, while stressing the importance of multi-layered protection.			
RGQ2/121	2024-02-29	Haiti	Taking control of cybersecurity in Haiti
Outlines Haiti's Haitian Institute for Statistics and Information and the CONATEL partnership to create a national cybersecurity strategy, aided by the World Bank and Inter-American Development Bank, including forming a working group, evaluating cybersecurity maturity, and establishing a CERT to enhance digital security.			
RGQ2/117 +Ann.1	2024-02-28	Dominican Republic	Cyberskills Center for Latin America and the Caribbean LAC4: Knowledge exchange, training and training in best practices at LAC4
Describes how the Latin America and Caribbean Cyber Competence Centre has enhanced cybersecurity in over 25 Latin American and Caribbean countries through workshops, legal framework support, and promoting regional cooperation, including empowering women and raising cyber awareness.			
RGQ2/114 +Ann.1	2024-02-27	Zambia	The role of the Authority in Child Online Protection in Zambia: A Zambia case study on the implementation of the National COP Strategy - Lessons learnt
Summarizes Zambia's dedication to child online safety by adopting ITU Resolution 179 and executing a national child online protection strategy, focusing on legal frameworks, education, combating exploitation, stakeholder cooperation, and ensuring effective oversight.			
RGQ2/104	2024-01-24	Democratic Republic of the Congo	Making Congolese cybersecurity a lever for integration and socio-economic growth
Describes the Democratic Republic of the Congo's strategy for using cybersecurity to enhance integration, governance, and growth, focusing on infrastructure, cybercrime, and digital services. It advocates for expert capacity building and ITU partnership for a secure digital transformation.			
2/212	2023-10-31	Republic of Korea	Misuse of Personally Identifiable Information

(continued)

Web	Received	Source	Title
Presents the Republic of Korea's data protection mechanism that has been updated to address concerns related to the misuse and abuse of personal identifiable information (PII). The Personal Information Protection Act (PIPA) amended the existing PII Anonymization Guidelines on 28 April 2022, which aim to offer six step-by-step guidelines for the treatment (de-identification) of personal information. The Republic of Korea highlighted the challenge of crafting guidelines that guard against the abuse and misuse of PII without jeopardizing the benefits of new technologies.			
2/201	2023-10-17	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
Discusses ongoing efforts to improve cybersecurity in ITU Member States, including future plans and new initiatives as well as how the Global Cybersecurity Agenda, launched in 2007, promotes international cooperation, and how BDT works with Member States and global organizations to establish national and regional CIRTs, measures cybersecurity commitments, supports strategy development, encourages diversity, and works to protect children online through the child online protection initiative.			
2/199	2023-10-17	United Kingdom	Building local capacity to adopt secure connected place technology: the UK's Secure Connected Places Playbook
Recognizes the benefits that connected places ("smart cities") technology can bring societies and local areas. However, it also recognizes that this interconnectivity creates cyber vulnerabilities and the potential for cyberattacks. Through its National Cyber Strategy 2022, the United Kingdom has been developing a 'Secure Connected Places Playbook'. This product, currently in alpha phase, has been developed in partnership with a diverse set of local government authorities and an industry consortium. The Playbook provides guidance on: i) governance; ii) procurement and supply chain management; and iii) risk and threat analysis. The United Kingdom has identified several good practices, including: i) working hand-in-hand with intended beneficiaries; ii) using a "test and iterate" approach; and iii) co-developing and testing with local government authorities. The United Kingdom has now begun beta testing, working with 13 local authorities.			
2/196	2023-10-17	United States	U.S. proposed Cyber Trust Mark Program: certifying that IoT products meet U.S. cyber standards
Presents the proposed Cyber Trust Mark program, by the United States Federal Communications Commission (FCC), a voluntary cybersecurity labelling initiative for IoT products. The programme aims to help consumers make informed decisions, differentiate trustworthy products, and encourage manufacturers to meet higher cybersecurity standards. The FCC seeks input on various aspects of the programme, including eligible devices, oversight, security standards, and consumer education. Certified products could be available for purchase by the end of 2024.			
2/187	2023-10-16	Republic of Korea	Privacy by Design certification in South Korea
Shares its contribution on Privacy by Design (PbD), a proactive approach to embedding privacy into the design and operation of information technologies and systems. The Personal Information Protection Committee (PIPC) of the Republic of Korea is piloting a PbD certification system to strengthen the safety of personal information collection devices. The certification helps organizations demonstrate their commitment to user privacy, increasing consumer trust and reducing the risk of privacy breaches.			
2/167	2023-10-11	Australia	eSafety Youth Council

(continued)

Web	Received	Source	Title
Presents the eSafety Youth Council, established in April 2022, that consists of 24 members aged 13-24 from diverse backgrounds in Australia. It aims to involve young people in decision-making processes for policies and programmes impacting them. The Council is informed by the Western Sydney University Youth Engagement Report and follows six good practice principles. Members engage in various activities, including conferences, resource launches, and discussions with technology companies. The Council priorities include collaboration, improved reporting processes, age-appropriate content access, and increased engagement on online safety.			
2/158	2023-10-09	Russian Federation	Challenges and approaches to addressing smishing and SMS incidents. Combating illegal use of virtual mobile numbers
Contextualize smishing as a type of phishing attack that uses SMS messages to trick users into downloading malware or revealing personal information. The rise of mobile services and the pandemic have increased its popularity. To combat smishing, users should be cautious of unexpected messages, use anti-spam settings, and report suspicious messages. Governments, banks, and telecommunication operators are also working together to fight smishing through regulations, public awareness campaigns, and technological solutions.			
2/154	2023-10-05	Australia	Combating telecommunications scams
Presents the Australian Communications and Media Authority (ACMA) work to combats scams through regulatory powers, new rules, and international cooperation. Initiatives include varying the telecommunications numbering plan, registering the Reducing Scam Calls and Scam SMS Code, and mandating stronger identity verification processes. ACMA also collaborates with other nations and industries to fight scams. Despite progress, SMS scams remain a significant issue. A holistic approach involving industry, government, and consumer awareness is needed.			
2/150 +Ann.1	2023-09-29	Argentina	Promoting cybersecurity in Argentina: challenges, strategies and advances in the digital era
Presents the growing reliance on ICT for essential services highlighting the need for governments to prioritize cybersecurity. Challenges include fostering a cybersecurity culture and promoting safe cyberspace usage. Efforts include a National Cybersecurity Awareness Campaign, a joint publication on cybersecurity issues, training programmes for civil servants, strengthening legal frameworks, and addressing the gender gap in ICT access and use through national and international initiatives.			
2/141	2023-09-28	Central African Republic	Criminal aspects of physical protection of information and communication network infrastructures
Central African Republic shares the implementation of legislative reforms and creation of agencies to control and secure information systems. However, the country faces vandalism and theft on its new fibre optic network. Proposed solutions include adopting laws against theft, fraud, and vandalism in public information networks and establishing a national CIRT team to coordinate incident management.			
2/137	2023-09-14	Côte d'Ivoire	Cybercrime: Continuing campaign on child online protection

(continued)

Web	Received	Source	Title
Discusses the digital knowledge challenge facing Côte d'Ivoire, that is hindering its development in the digital world. To address this, public and private sectors, along with international organizations, have launched an awareness campaign for middle and high school students. The campaign aims to educate and raise awareness about online risks, promote responsible digital behaviour, and provide support for reporting abuse. Over 1 000 students participated in the campaign, which emphasizes the importance of a safer digital environment for all citizens.			
2/120	2023-09-07	Timor-Leste	Advancing cybersecurity for Timor-Leste's digital transformation
Presents Timor-Leste digital transformation journey, focusing on improving government services, inclusivity, and crucial sectors such as healthcare, education, and agriculture. However, as a least developed country (LDC), it faces significant cybersecurity challenges, including weak frameworks, limited awareness, and inadequate resources. To enhance digital resilience, Timor-Leste must invest in infrastructure, capacity building, legal frameworks, public-private partnerships, awareness, incident response, and international cooperation. Addressing these challenges is crucial for sustainable development and economic growth in the digital era.			
2/119	2023-09-06	Kenya	The Authority's Child Online Protection and Safety Programme in Kenya: A case study on the implementation of the ITU's Guidelines on Child Online Protection
Shares the implementation of child online protection initiatives since 2011, by the Communications Authority of Kenya (CA), focusing on raising awareness and promoting responsible Internet usage. The CA has launched two campaigns, "Be The COP" and "*Huwezi Tucheza, Tuko Cyber Smart*," targeting parents, guardians, teachers, and children. The authority collaborates with various stakeholders, including government agencies, industry players, and NGOs, to implement the ITU Guidelines on Child Online Protection. Initiatives include legal and regulatory frameworks, reporting mechanisms, research and surveys, national strategies, industry initiatives, educational resources, capacity building, and national awareness campaigns.			
2/115	2023-09-04	Democratic Republic of the Congo	Digitalization of public services in the Democratic Republic of the Congo: key challenges and requirements for information security and cyberdefence
Presents the implementation of cybersecurity measures, including the enactment of Law No. 20/017 in 2020, and the adoption of a digital code in 2023. The country is working on creating a computer incident response team (CIRT) and improving its broadband infrastructure with a planned 50 000 km of optical fibre network. Cooperation and public awareness-raising are also essential components of their cybersecurity strategy.			
2/112	2023-08-21	Kenya	CSIRT/CIRT approaches and experiences towards the resilience of critical infrastructure in Kenya
Introduces the establishment of the National Computer Incidents Response Team (KE-CIRT) by the Communications Authority of Kenya to mitigate cyber threats and ensure a safer cyberspace. The country has a legal framework defining critical infrastructure and has adopted a cybersecurity framework supported by policy and operational frameworks. Challenges faced include a rapidly evolving threat landscape, lack of international cooperation, insufficient expertise, limited resources, balancing privacy and security, coordination and information sharing, technological advancements, insider threats, public-private collaboration, and public awareness and education.			
2/98	2023-07-25	Australia	Australia's national online safety awareness campaign

(continued)

Web	Received	Source	Title
Introduces the Online Safety Act 2021, to keep pace with new technology and emerging online threats. The Online Safety campaign aimed to raise public awareness of the Online Safety Act and the strengthened laws for online safety. The campaign targeted various audience groups and successfully drove traffic to the eSafety Commissioner website.			
RGQ2/85	2023-05-18	Beihang University	Development of policies and legislation to protect consumer rights and interests in China in the digital era
China attaches great importance to the protection of consumer rights and interests. Firstly, in terms of policy guidance, the goal is to improve the consumer environment, strengthen consumer rights protection, and achieve social fairness and justice, adhering to the equal emphasis on development and regulation; Secondly, in terms of the legal system, China has steadily promoted the formulation and implementation of laws, regulations, and standards related to consumer rights protection. It has continuously strengthened the protection of consumers' digital rights and focused on the special protection of vulnerable consumers, gradually forming a comprehensive and three-dimensional legal system for consumer rights protection to adapt to the new development and needs of consumer rights protection. The content of this paper is based on the policy and legislative protection of consumer rights in China's new development pattern, so as to provide assistance for the international consumer rights protection cause.			
RGQ2/80	2023-05-10	Russian Federation	Information sharing practices to protect children from disruptive online content - Award "For a Safe Digital Childhood"
Presents its contribution which contained information on some practices on the exchange of information between two Russian Federation federal executive bodies to protect children from destructive online content, as well as information about the award "For a Safe Digital Childhood" by Alliance for the Protection of Children in the Digital Environment, aimed at supporting projects to develop a safe digital environment throughout the Russian Federation.			
RGQ2/79	2023-05-10	Russian Federation	National computer incident response and coordination centre - information security leaders
Presents a contribution on the operation of its National Computer Incident Response & Coordination Centre (NCIRCC) to ensure a stable critical infrastructure, as well as approaches regarding the appointment of leaders in the field of information security. In response to questions received during the meeting, the Russian Federation clarified that NCIRCC is not the only such centre, and the main criteria for leaders in the field of information security is not only their professional degree, but also wide-ranging experience and relevant professional skills.			
RGQ2/74	2023-05-09	United Kingdom	TBEST: an example of outcome-based pen-testing for communications providers to help improve their network security posture

(continued)

Web	Received	Source	Title
Contribution on the TBEST scheme, an example of cybersecurity assurance practice that Ofcom, the United Kingdom regulator, runs voluntarily with communications providers. TBEST is a penetration testing that aims to stimulate a cyber-attack in telecommunications networks in order to identify security vulnerabilities which can then be, through a process of remediation, addressed to improve the operators' network security posture. The contribution provides an overview of the process, and the various stakeholders involved. More broadly, this scheme is an example of supervisory policy approach that Ofcom is taking, which stresses the importance of building collaborative relationships with the industry that Ofcom regulates. To date, all communications providers in the United Kingdom have already or are undergoing the TBEST scheme voluntarily and have implemented changes as a result. TBEST is not a "standard" nor a certification process. The goal is to enable communications providers to gain awareness of cyber threats and implement appropriate changes in a timely manner to improve their cyber defence capabilities. By being aware of, and addressing such vulnerabilities and weaknesses, the operator is in a much stronger position to protect their networks.			
RGQ2/66	2023-05-10	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
Provides an update on the activities currently being undertaken to enhance cybersecurity in ITU Member States. It also highlights future actions envisaged and new initiatives being formulated. The presentation addressed the ITU cybersecurity mandate, and through BDT, work on the national CIRT programme, regional and national cyberDrills, the Global Cybersecurity Index (GCI), national cybersecurity strategy (NCS) assistance, Women in Cyber, Her CyberTracks, child online protection, partnerships and collaboration, and Cyber for Good. The document emphasizes the importance of collaboration, partnerships, and resource mobilization to allow ITU to fulfil its mandate, considering the extensive list of tasks that membership have requested BDT to undertake. BDT also presented information about the 5th edition of the Global Cybersecurity Index.			
RGQ2/58	2023-04-27	Brazil	Cybersecurity assurance practices - Brazil experience
Introduces the contribution referring to the efforts of the Brazilian National Telecommunications Agency (ANATEL) regarding the establishment of cybersecurity minimum requirements for telecommunication equipment. ANATEL initially adopted a non-mandatory approach (Act 77/2021), which evolved into a cybersecurity compulsory certification requirement for a specific set of equipment (Act 2436/2023). This evolution was only possible with a comprehensive debate within the sector.			
RGQ2/57	2023-07-27	Brazil	Brazilian cybersecurity-related policies and regulations
Presents an overview on the cybersecurity-related policies and regulations that have been developed in Brazil in recent years, including the National Information Security Policy, the National Cybersecurity Strategy, the Cybersecurity Regulation for the Telecommunication Sector, the Federal Cyber Incident Management Network, and the 5G Spectrum Auction Notice. There were questions about the modular approach adopted by the National Information Security Policy, and the Brazilian delegation explained that in Brazil cybersecurity is one of the elements of Information Security.			
RGQ2/53	2023-04-25	Mexico	Privacy reports on user information in the use of digital platforms

(continued)

Web	Received	Source	Title
Presents the Privacy Reports, which purpose is to make available in a clear, simple and transparent manner the privacy policies of operating systems, terminal equipment, social networks, and digital platforms that enable the provision of services such as: online commerce, transport and entertainment. These reports published by the Federal Telecommunications Institute help users to learn about the information that is collected by the platforms, and how this information is treated, and helps users make responsible use of such platforms. The Reports also empower users by providing transparent information about privacy policies.			
RGQ2/51	2023-04-25	Mexico	Internet of Things Devices Catalog
The *Internet of Things Devices Catalogue* is an electronic tool that allows users of telecommunication services to know the main characteristics of IoT devices, as well as the privacy policies defined by the manufacturers. The IoT devices published are those that are marketed in Mexico and have been certified by the Federal Telecommunications Institute. The tool allows users to be empowered with transparent information about privacy policies and the characteristics of terminal equipment that comply with technical regulations, for informed decision-making and for the proper use of IoT equipment.			
RGQ2/48	2023-04-25	Access Partnership Limited	Cybersecurity assurance practices - international standards and satellite communications
Contains information related to developing cybersecurity assurance practices for commercial satellite operators, as well as highlighting some of the existing general cybersecurity assurance practices which may be adopted by any commercial satellite operator, including ISO 27001. The contribution noted some of the unique cybersecurity threats which need to be overcome in satellite operations, including the cross-jurisdictional nature of satellite operations, and the vulnerabilities of ground stations. The contribution explained specific technical standards including the ETSI technical standard 103 732 and its measures to protect consumer mobile devices, as an example of standards towards specific technology which could inform the further development of standards for commercial satellite operators.			
RGQ2/44	2023-04-24	South Africa	The domain name cybersecurity culture
Provides a contribution concerning the security of the country code top-level domain name (.za). The South African Domain Name Authority (ZADNA) manages the .za domain namespace under the mandate of the Electronic Communications and Transactions Act (ECTA). Its policy framework was designed to ensure a secure, resilient, and efficiently managed domain namespace, promoting stakeholder engagement, growth of the namespace, policy compliance, and entrance of new Internet service providers. ZADNA also addresses cybersecurity threats through education and awareness programmes, alternative dispute resolution (ADR) workshops and regulations, and DNS training courses. Additionally, it adheres to international standards for dispute resolution, working in line with the World Intellectual Property Organization (WIPO) and organizations such as the South African Institute of Intellectual Property Law (SAIIPL) and the Arbitration Foundation of Southern Africa.			
RGQ2/38	2023-04-13	Australia	Sharing advice from Australia on securing smart places

(continued)

Web	Received	Source	Title
Shares information on the lessons learned by the Australian Cyber Security Centre in response to risks identified for smart places. The contribution defined smart places as those designed to provide enhanced services through the use of smart information and ICT enabled systems and devices. The contribution noted that the highly connected nature of smart places makes them vulnerable to intrusions. This is exacerbated when the system scales. The contribution gave examples of Australian policies used to protect the various aspects of smart cities including IoT, supply chains, operational technology and cloud computing. The contribution also raised several examples of strategies which may be employed to mitigate security risks as well as ensuring operational redundancy.			
RGQ2/34	2023-04-06	Republic of Korea	Cloud Security Assurance Program (CSAP) in South Korea
Introduces the Cloud Security Assurance Programme (CSAP), a security certification for cloud computing services that meet security certification standards to improve and guarantee information protection levels. The purpose of the CSAP is to provide private cloud services with proven safety and reliability to national and public institutions. Also, it aims to implement an objective and fair security certification system for cloud services to address user security concerns and secure competitiveness of cloud services. The CSAP provides a number of benefits. By certifying the security level of a cloud system, CSAP helps to improve the cyber resilience of national and public institutions. This can also help to ensure that sensitive information is protected and that cloud services are reliable.			
RGQ2/29	2023-03-30	Côte d'Ivoire	Policy and strategy of Côte d'Ivoire for building a trusted digital space
Shares the initiatives taken by Côte d'Ivoire in its efforts to build digital trust, which concerns all economic sectors that use ICTs, such as media and communication, transport, health, industry, telecommunications and computing, distribution of goods and consumption, construction, finance and insurance, tourism, agriculture and e-commerce. To consolidate the freedom of online public communication and ensure interactions are secure, Côte d'Ivoire has enhanced the means for combating cybercrime and protecting personal data in order to build trust in cyberspace. Cybersecurity has become an issue of privacy, competitiveness and national sovereignty. A capacity to anticipate, build trust and protect personal data is essential. In this sense, the country has updated its legal and institutional framework, setting a visionary policy to enhance digital trust by 2025. The country has established a Consultative Committee for Digital Trust (CCCN) and a Consultative Committee for the Protection of Personal Data (CCDCP).			
RGQ2/20	2023-03-22	Nigeria	Child Online Protection practices in Nigeria
Presents its efforts in regard to child online protection through the Nigerian Communications Commission (NCC), the independent national regulatory authority for the telecommunication industry, in collaboration with the Office of the National Security Adviser in Nigeria who works with other stakeholders to ensure child protection in Nigeria's cyber space. It was decided by the meeting to liaise with the Council Working Group on Child Online Protection (CWG-COP) to share the relevant experiences shared by Nigeria.			
2/80	2022-11-24	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
Provides an update on the activities currently being undertaken by BDT and new initiatives to enhance cybersecurity in ITU Member States: CIRT programme, regional and national cyberdrills, national cybersecurity strategy (NCS) , work related to Bridge the Cybersecurity Divide: Cyber for Good project, work on promoting a diverse and inclusive cybersecurity community through the Women in Cyber Mentorship Programme and Youth4Cyber initiative, child online protection, and partnerships and collaboration initiatives.			

(continued)

Web	Received	Source	Title
2/77	2022-11-22	United Kingdom	Sharing experience from the UK on promoting and developing cybersecurity skills
Outlines the country's policy approach to address the cyber skills gap which, in addition to the final report of the study cycle, can also be included in a future repository of good practices as agreed through Resolution 130 (Rev. Bucharest, 2022) of the Plenipotentiary Conference. The United Kingdom's initiatives are focused in three areas: (1) cyber skills for young people, (2) cyber skills for adults, and (3) developing the cyber profession.			
2/74	2022-11-18	World Bank	World Bank Study Group 2 Submission: Digital transformation
Highlights their readiness to support the least developed client countries with a special emphasis on fragility, conflict and violence (FCV) and small island developing states (SIDS). Through the analytical work programme and strategic partnerships, the World Bank is working closely with client countries on issues related to the SG2 Questions' scopes. Relevant examples from the World Bank around using ICT services and applications for the promotion of transformative and sustainable development are provided in the contribution. For instance, one relating to cybersecurity is the Cybersecurity Multi-Donor Trust Fund, being a part of the broader Digital Development Partnership umbrella programme, aims at systematically incorporating cybersecurity in the development agenda as well as in World Bank operational programmes. Work includes building global knowledge to better define the cybersecurity development agenda, and country-specific technical assistance.			
2/71 (Rev.1)	2022-11-18	Russian Federation	New practices of the Russian Federation in the field of creating a culture of cybersecurity
Presents the Russian Federation Cyber Hygiene Program, launched in August 2022. The programme is planned for a three year period and includes various activities aimed at attracting the attention of citizens of the Russian Federation to the issues of cybersecurity and the training in skills on safe behaviour on the Internet. Large-scale information campaigns are one part of the programme. Citizens were segmented into age groups, and their online behaviour and the type of digital content consumed were taken into account. Based on this segmenting approach, more specifically targeted means of information dissemination could be applied for the 3 segmented groups of population (12-18 / 18-45 / 45+ years old). The contribution also covers the means of improving the information security literacy of civil servants, as well as the results of an all-Russian Federation study of the citizens' information security literacy.			
2/35	2022-10-12	Rwanda	National cybersecurity initiatives: current status
Highlights the programmes and initiatives put in place to guarantee the security and resilience of Rwanda's cyberspace. To support national economic growth and social mobility, the Government of Rwanda (GoR) is actively deploying various information technologies and has made major investments in ICT infrastructure and applications. GoR established the National Cybersecurity Authority (NCSA) as the authority to spearhead the implementation of National Cyber Security policies and strategies. Additionally, GoR established a law relating to protecting personal data and privacy and passed the prevention and punishment of cybercrimes law. NCSA roles include: coordinating national cybersecurity functions across the private and public sectors; promoting national education programmes and fostering awareness of cybersecurity good practices amongst the Rwandan population; operating the Rwanda Computer Security Incident Response Team (Rw-CSIRT); and overseeing the implementation of the Protection of Personal Data and Privacy Law. Furthermore, the Rwanda Utilities Regulatory Authority (RURA), Regulation No. 010/R/CR-CSI/RURA/020 OF 29/05/2020), Rwanda Information Society Authority (RISA), and capacity building collaborations and initiatives have been put in place to ensure preparation in preventing and responding to evolving cyber threats.			

(continued)

Web	Received	Source	Title
2/34	2022-10-12	Côte d'Ivoire	Initiatives to support children and young people, national strategy for the protection and empowerment of children and young people online: the experience of Côte d'Ivoire
Presents an initiative undertaken by Côte d'Ivoire to protect children against the dangers and threats of using ICTs. The initiative, www.jemeprotegeenligne.ci is a website targeted at children between 5 and 19 years old as well as teachers and parents with the goal of educating children and young people and raising awareness.			
2/30	2022-10-11	Côte d'Ivoire	Proposal for State actions and initiatives to foster a culture of cybersecurity and ensure that information and communication networks are secure: the case of Côte d'Ivoire
Contextualizes cyberattacks and threats as a major concern for governments in this increasingly connected world, particularly in developing countries. Cybersecurity is now the priority issue for many States. This contribution gives an overview of the cybersecurity situation in developing countries, notably Côte d'Ivoire, and highlights strategies for raising user awareness and experience-sharing among Member States.			

Incoming liaison statements for Question 3/2

Web	Received	Source	Title
2/410 +Ann.1	2025-04-30	ITU-T Study Group 17	Liaison statement form ITU-T Study Group 17 to ITU-D Study Group 2 Question 3/2 LS on update on the work of the Correspondence Group on Child online protection (CG-COP)
2/409	2025-04-30	ITU-T Study Group 17	Liaison statement form ITU-T Study Group 17 to ITU-D Study Group 2 Question 3/2 on request to update security contacts and to provide information on security-related Recommendations or other texts under development
2/241	2024-09-11	ITU-T Study Group 17	Liaison statement from ITU-T Study Group 17 to ITU-D Study Groups 1 and 2 on SG17 update on the work of the Correspondence Group on Child online protection (CG-COP)
RGQ2/151	2024-03-18	ITU-T Study Group 17	Liaison statement from ITU-T Study Group 17 to ITU-D Study Group 1 Question 6/1 and ITU-D Study Group 2 Question 3/2 on Establishment of the Correspondence Group on Child online protection (CG-COP)
RGQ2/107	2024-02-12	Chairman, ITU Council Working Group on COP	Liaison statement from ITU Council Working Group on COP to ITU-D Study Group 2 Question 3/2 on child online protection
RGQ2/83	2023-03-08	ITU-T Study Group 17	Liaison statement from ITU-T Study Group 17 to ITU-D Study Group 2 Question 3/2 on status of security studies in ITU-T SG17
2/20	2022-06-16	ITU-T Study Group 17	Liaison statement from ITU-T Study Group 17 to ITU-D Study Group 2 Question 3/2 on request to update security contacts and to provide information on security-related Recommendations or other texts under development

Annex 2: List and summary of BDT on-going cybersecurity activities

Activity type	Activity	Targeted / invited countries	Partners	Outputs
Data	Global Cybersecurity Index v5	ITU Member States	GCI Expert Group	Global Cybersecurity Index report and country reports. Link
Governance	Capacity-building sessions for the cybersecurity ecosystem in Guinea-Bissau	Guinea-Bissau	Government of Guinea-Bissau	Capacity-building sessions for the cybersecurity ecosystem in Guinea-Bissau with the aim to empower Guinea-Bissau's cybersecurity ecosystem by guiding key national stakeholders in developing strategic approaches to CIRT implementation and enhancing cybersecurity in Guinea-Bissau
Governance	Mauritania's Cybersecurity Governance Development	Mauritania	Government of Mauritania	Sessions to enhance of a national cybersecurity governance framework to enable Mauritania to strengthen the protection of the critical information systems of official institutions and vital operators, the fight against cybercrime, awareness raising, training, confidence-building in digital, more effective regional and international integration through cooperation.
Governance	National cyber risk assessment	Lesotho	Ministry of Communications Science and Technology	Workshop to enhance strategic thinking on cybersecurity governance among key national stakeholders, thereby advancing the objectives of Lesotho's National Cybersecurity Strategy.
Governance	Strengthening Critical Information Infrastructure Resilience	Cambodia	Ministry of Post and Telecommunications Cambodia (MPTC, Japan International Cooperation Agency (JICA)	Workshops on technical incident response, national cybersecurity strategy, and crisis management for critical information infrastructure stakeholders
Governance	Tabletop Exercise and a Cybersecurity Incident Simulation Exercise	ITU Arab States region Member States	CSC UAE	Tabletop exercise centred around cyber-attack directed at a financial institution.
Incident Response	13th Event of Cyber Capacity Building in America - Andino	ITU Americas region Member States	Ministry of Popular Power for Science and Technology of Venezuela, National Commission of Information Technologies (CONATI), Superintendency of Electronic Certification Services (SUSCERTE)	Incident response trainings, discussions, and information sharing for cybersecurity professionals. Link
Incident Response	Americas Regional Cyber-Drill	ITU Americas region Member States	INICTEL-UNI, Peruvian Ministry of Transportation and Communications, General Secretariat of the Andean Community	Incident response trainings, discussions, and information sharing for cybersecurity professionals. Link
Incident Response	CIRT Establishment in Bahamas	Bahamas	Government of Bahamas	Building and deploying the technical capabilities and related training necessary to develop Bahamas national cybersecurity strategy and to establish its National Cybersecurity Incident Response Team (CIRT). Link

(continued)

Activity type	Activity	Targeted / invited countries	Partners	Outputs
Incident Response	CIRT Maturity Assessment	Timor-Leste	ANC	Conducted Maturity Assessment of country CIRT through series of workshops, discussions, and inventories, providing recommendations for the Timor-Leste computer security incident response team (TLCSIRT) in collaboration with the Autoridade Nacional de Comunicações (ANC) to ensure TLCSIRT can enhance its cybersecurity maturity level. Link
Incident Response	Cyber 100x Global Cyber-Drill 2024	ITU Member States	Cyber Security Council United Arab Emirates	Incident Response trainings, discussions, and information sharing for cybersecurity professionals. Link
Incident Response	CyberQ	ITU Member States	United Arab Emirates Cybersecurity Council	Incident Response trainings, discussions, and information sharing for cybersecurity professionals. Included specific trainings for women. Link
Incident Response	Cybersecurity Forum and CyberDrill for Europe and the Mediterranean	ITU Europe region and Arab States region Member States	Ministry of Transport and Communications of Bulgaria, Ministry of Electronic Governance of Bulgaria	Cybersecurity forum featuring trends and challenges, CSIRTs capacity-building training, and two days of cyberdrill exercises with emerging attack scenarios and collaborative learning sessions. Link
Incident Response	ITU National CyberDrill for Armenia	Armenia	Ministry of High-Tech Industry of Armenia	Incident response trainings, discussions, and information sharing for cybersecurity professionals. Link
Incident Response	ITU Regional Asia-Pacific CyberDrill	ITU Asia and the Pacific region Members States	Cyber Security Brunei (CSB)	Incident Response trainings, discussions, and information sharing for cybersecurity professionals. Link
Incident Response	ITU Regional Cybersecurity Readiness Exercise	ITU Arab States region Member States	Directorate General for Information Systems Security (DGSSI) Morocco	Incident response trainings, discussions, and information sharing. Link
Incident Response	National CIRT Establishment in Gambia	Gambia	Ministry of Information and Communication Infrastructure (MOICI)	Assist MOICI in building and deploying the technical capabilities and related trainings necessary to establish its national CIRT. Link
Incident Response	National Computer Incident Response Team (CIRT) Implementation – Suriname	Suriname	e-Government Directorate, Cabinet of the President of Suriname	Support for operationalization of Computer Incident Response Team. Link
Incident Response	Regional Cybersecurity Week	ITU Arab States region Member States	ARCC Oman	Regional Cybersecurity Conference focusing on "Cybersecurity as an enabler for the Digital Economy", the FIRST Organization Seminar, and the Regional and OIC-CERT Cyber Drill. Link
Incident Response	Rwanda National CyberDrill	Rwanda	Rwanda National Cyber Security Authority, Ministry of Foreign Affairs of the Czech Republic	Incident Response trainings, discussions, and information sharing for cybersecurity professionals. Link

(continued)

Activity type	Activity	Targeted / invited countries	Partners	Outputs
Incident Response	Twelfth Edition of the Regional Cyberdrill for Africa Region (ITU-INTERPOL CyberDrill)	ITU Africa region Member States	Ghana's Cyber Security Authority (CSA), INTERPOL	Incident Response trainings, discussions, and information sharing for cybersecurity professionals. Link
Partnerships	Cyber for Good	Least developed countries (LDCs)	Axon Consulting, BitSight Technologies, CTM360, DreamLab Technologies, ImmuniWeb, WelchmanKeen	Tools, trainings, and services offered for free to Least Developed Countries. Link
Skills Development	Child Online Protection National Assessment - Andorra	Andorra	SWGfL/UK Safer Internet Centre	Child Online Protection National Assessment with the national stakeholder consultation event
Skills Development	Child Online Protection Train the Trainers and Cybersecurity briefings - Maldives	Maldives	National Centre for Information Technology (NCIT)	Trainings on Child Online Protection as well as briefings on key topics. Link
Skills Development	Creating a Safe and Prosperous Cyberspace for Children	ITU Member States	CTO, CNIL, Council of Europe, European Commission, EC-Council, EBU, Europol, ILO, Interpol, MICITT, NCA KSA, OECD, United Nations Human Rights Special Procedures, UNICRI, UNESCO, UNICEF, UNODC, WIPO, World Bank, UC Berkley, LSE, Middlesex University London, Western Sydney University, Youth and Media, BBC, Disney, Ericsson, worldwide Group, Facebook, IBM, IEEE, Microsoft, Sony, TIM, Privately, Tencent, TrendMicro, Twitter, ASCSA, ACOPEA, 5Rights Foundation, ASDRA, Child Helpline International, Child Rights Connect, Family Online Safety Institute, Childhood, ChildOnline Africa, DeafKidz International, DISC Foundation, Families Europe, Halley Movement, End Violence Against Children, DOInstitute, ecpat, Fard Digital, HABLATAM, Cuber Coluntarios.org, Global Kids Online, GSMA, iKeepSafe, Inclusion international, InHope, Ins@fe, International Centre for Missing & Exploited Children, International Disability Alliance, Internet Matters, Internet Watch Foundation (IWF), Human Trafficking Front, ParentZone, Plan International, RNW media, Save the Children, Paniamor, Stiftung digitale chancen, SWGfL, Tech Coalition, terre des hommes suisse, United Kingdom Safer Internet Centre, WeProtect Global Alliance, Wise Kids, World Economic Forum, YouthIGF, Together Against Cybercrime	Advocacy, research, and in-country programmes related to Child Online Protection. Link

(continued)

Activity type	Activity	Targeted / invited countries	Partners	Outputs
Skills Development	Her CyberTracks 2024	Algeria, Angola, Bahrain, Benin, Botswana, Burkina Faso, Burundi, Cameroon, Cabo Verde, Central African Republic, Comoros, Chad, Côte d'Ivoire, Democratic Republic of the Congo, Djibouti, Egypt, Equatorial Guinea, Eritrea, Eswatini, Ethiopia, Gabon, Gambia, Ghana, Guinea, Guinea-Bissau, Iraq, Jordan, Kenya, Kuwait, Lebanon, Lesotho, Liberia, Libya, Madagascar, Malawi, Mali, Mauritania, Mauritius, Morocco, Mozambique, Namibia, Niger, Nigeria, Oman, Qatar, Republic of the Congo, Rwanda, São Tomé and Príncipe, Saudi Arabia, Senegal, Seychelles, Sierra Leone, Somalia, South Africa, South Sudan, State of Palestine*, Sudan, Syrian Arab Republic, Tanzania, Togo, Tunisia, Uganda, United Arab Emirates, Yemen, Zambia, Zimbabwe	GIZ, Microsoft	Her CyberTracks provides specialized, targeted training, maintaining the essential mentorship and role modelling aspects. The programme is poised to propel the next generation of women in cybersecurity into roles of leadership, ensuring that their voices and expertise shape the future of this critical field through training, mentorship, and inspiration across three tracks: Policy & Diplomacy, Incident Response, and Criminal Justice (implemented by UNODC). Link
Skills Development	Translation of Child online protection guidelines and capacity building activities - Albania	Albania	National Authority on Electronic Certification and Cyber Security	Child online protection guidelines translated into Albanian and the roll out of capacity-building activities
Skills Development	Translation of Child online protection guidelines and capacity building activities - Malta	Malta	SWGfL/UK Safer Internet Centre	Child online protection guidelines translated into Maltese and the roll out of capacity-building activities

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 du Méridien Président
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
USAF POTRAZ Building
877 Endeavour Crescent
Mount Pleasant Business Park
Harare
Zimbabwe

Email: itu-harare@itu.int
Tel.: +263 242 369015
Tel.: +263 242 369016

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
4th floor NBTC Region 1 Building
101 Chaengwattana Road
Laksi,
Bangkok 10210,
Thailand

Email: itu-ro-asiapacific@itu.int
Tel.: +66 2 574 9326 – 8
+66 2 575 0055

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

Email: bdt-ao-jakarta@itu.int
Tel.: +62 21 380 2322

India
International Telecommunication Union (ITU) Area Office and Innovation Centre
C-DOT Campus
Mandi Road
Chhatarpur, Mehrauli
New Delhi 110030
India

Email:
Area Office: itu-ao-southasia@itu.int
Innovation Centre: itu-ic-southasia@itu.int
Website: ITU Innovation Centre in New Delhi, India

CIS

Russian Federation
International Telecommunication Union (ITU) Regional Office
4, Building 1
Sergiy Radonezhsky Str.
Moscow 105120
Russian Federation
Email: itu-ro-cis@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 978-92-61-41101-5

Published in Switzerland
Geneva, 2025

Photo credits: Adobe Stock