WSIS+20 Review
Action Lines
Milestones, Challenges and Emerging Trends beyond 2025

C5 Building Confidence and Security in the use of ICTs

Comparative Snapshot

2005

- Only 1 billion people were online.
- Mobile phones were primarily used for calls and texts.
- Mobile payments were just starting to gain traction.
- The cost of cybercrime to the global economy was $400 billion, significant for that time.
- Threat vectors, though sophisticated for their time, were very different from today's.

2024

- 5.4 billion people are online.
- Cyberattacks are increasing by 80% year-on-year. The cost of cybercrime has skyrocketed, rising more than 20 times from $400 billion in 2005 to an estimated $8-11 trillion.
- An attack occurs approximately every 39 seconds somewhere on the web.
- With our growing dependence on digital technology, cybersecurity and privacy concerns have intensified.
- Resilience now involves safeguarding a wide range of physical infrastructures such as submarine cables, satellites, and terrestrial networks, alongside implementing robust cyber resilience

The Evolution of Context

The ICT landscape has changed drastically since 2005, with ICTs now underpinning every sector of society and the bulk of critical infrastructure. Examples -

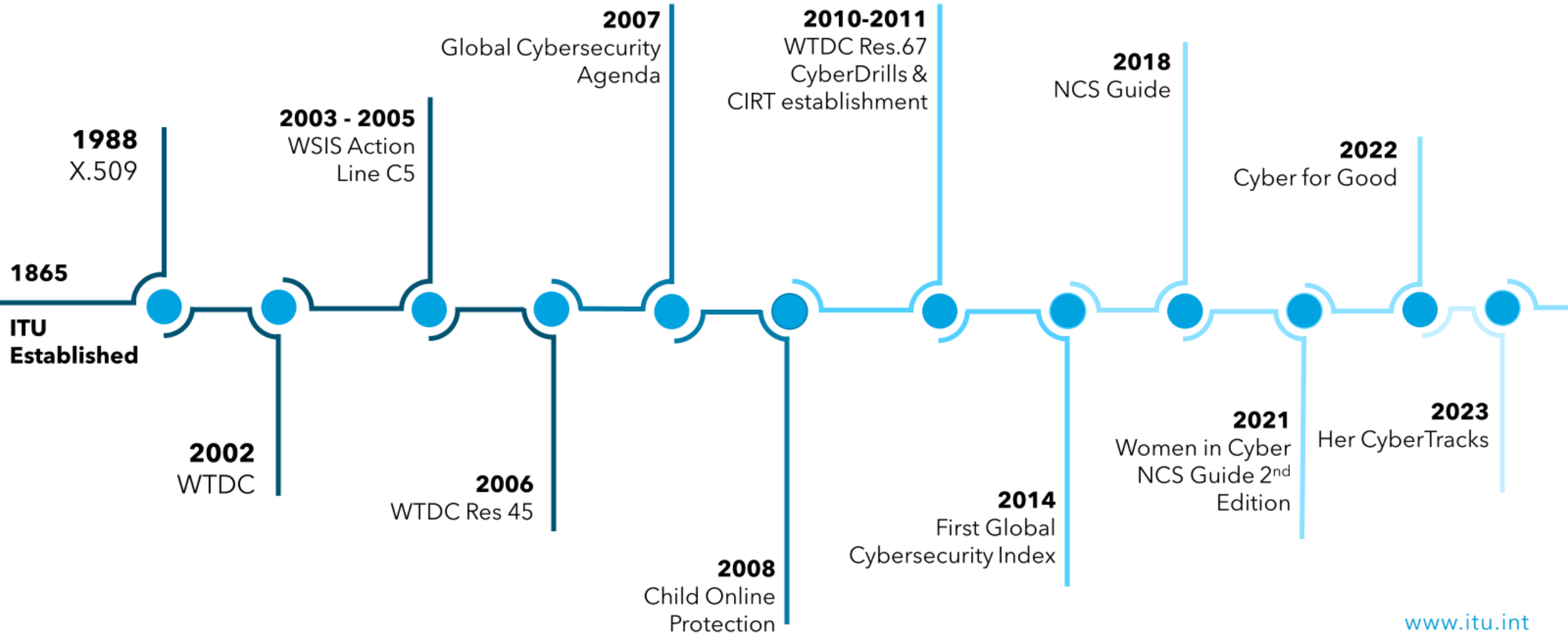
- **Emergence of Artificial Intelligence (AI)** allowing humans and machines to make more informed decisions – while raising challenges of security, trust, and safeguarding human rights.
- **Wider adoption of the Internet of Things** with billions of new interconnected devices, opening up significant new potential vulnerabilities.
- **New communication technologies and standards**, such as 5G, enabling communication at exponentially faster speeds.
- **Quantum computing,** offering computing speeds far beyond current capabilities, presenting great opportunities while also threatening current cryptographic algorithms.
- **New security technologies,** such as Distributed Ledger Technologies (e.g., blockchain), offering significantly better ways to safeguard systems and data. More countries are adopting digital identity systems.
- **Wide-scale adoption of social networks**, which have brought forth significant trust concerns.
- Emergence of the **dark web** has raised growing concerns worldwide about criminal activity in cyberspace.

The Evolution of Context

Evolution of the engagement of stakeholders

1. There has been growing recognition among all stakeholders on the diversity of urgent actions needed to advance cybersecurity, ranging from protection of critical infrastructure to safeguarding user privacy.
2. The COVID-19 pandemic highlighted the centrality of ICTs to health and safety, and the need to address rapidly evolving cybersecurity challenges.
3. The framework offered by the ITU's Global Cybersecurity Agenda (GCA) continues to offer a broad framework for international cooperation on cybersecurity within the framework of the WSIS outcome documents.
4. More than 125 countries have signed and/or ratified different cybersecurity and cybercrime conventions, declarations, guidelines or agreements.
5. A number of national, regional and international organizations, many of them multistakeholder in nature - have been set up to tackle the issue of cybersecurity.
6. Pursuant to UNGA Resolutions, groups such as the Group of Governmental Experts (GGE) and Open-ended Working Group (OEWG) have studied several issues related to the use of ICTs in the context of international security.
7. In accordance with General Assembly resolution 75/282 and General Assembly decision 78/549 the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, established by the General Assembly in its resolution 74/247, held its reconvened concluding session from 29 July to 9 August 2024 in New York where a Draft United Nations convention against cybercrime; Strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes has been agreed.

ITU and Cybersecurity: a Timeline



Challenges in implementing the Action Line

Challenge 1 Timely and sufficient resource mobilization

Challenge 2 Stakeholder participation

Challenge 3 Evolving needs and capacities

Trends and Opportunities Beyond 2025

- UN remains critical fora for cyber discussions as well as technical collaboration
- Increasing focus for the need on capacity development
- New intervention models are needed to ensure long term sustainability
- Enhanced private sector engagement
- Continuing to share best practices and engagement with standards development

Thank you!