

Cybercrime strategies

Workshop 115

Wednesday, 28 Sep, 14h30–16h00 (WS Room 6/Conf Room 13)



Focus

Many governments are adopting cybersecurity policies and strategies but only few are developing specific policies or strategies on cybercrime. The workshop will therefore discuss the following issues:

- ▶ Cybercrime and cybersecurity strategies: concepts
- ▶ Elements of cybercrime strategies
- ▶ Stakeholders in cybercrime policies and strategies

Cybersecurity has become a policy priority of many governments. This is reflected in cybersecurity policies or strategies in all regions of the world aimed at the:

- protection of economic and other national interests and national security
- protection of the confidentiality, integrity and availability of ICT to enhance security, resilience, reliability and trust.

Priority is given to public and private sector critical information infrastructure that is to be protected against:

- non-intentional incidents (disasters, technical or human failures)
- intentional attacks by state and non-state actors

They focus on technical, procedural and institutional measures, such as risk and vulnerability analyses, early warning and response, incident management, information sharing and other measures to ensure protection, mitigation and recovery. Measures against cybercrime are often one element of cybersecurity strategies.

Cybercrime is about:

- offences against the confidentiality, integrity and availability of computer data and systems
- offences by means of computers, in particular the sexual exploitation of children, fraud or IPR offences
- electronic evidence in relation to any crime

Action against cybercrime is thus about a criminal justice response to ensure that the rule of law and human rights also apply in cyberspace.

Human rights
Rule of law
Democracy

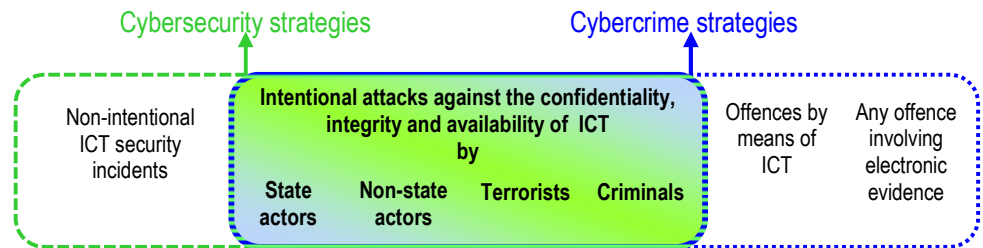




In many countries this includes for example:

- legislation (harmonised with the Budapest Convention on Cybercrime)
- preventive measures
- cybercrime reporting systems
- high-tech crime and other specialised units
- law enforcement and judicial training
- public-private cooperation
- international cooperation
- protection of children
- financial investigations and other measures against fraud and money laundering.

Cybercrime and cybersecurity strategies are not covering identical issues nor the same type of measures, but they intersect and complement each other.



However, only few governments have designed specific and consistent cybercrime strategies or have fully built the criminal justice perspective into cybersecurity strategies. The workshop will therefore discuss the following:

- ▶ Cybercrime and cybersecurity strategies: What concepts? What differences and intersection? How to ensure synergies and complementarity?
- ▶ Cybercrime strategies: Is there a need for specific cybercrime strategies? By public and private sectors? What objectives and measures?
- ▶ Stakeholders: Who is responsible for developing, managing, implementing cybercrime strategies? What role for public and private sector organisations?

Panellists:

- Markko Künnapu, Ministry of Justice of Estonia and chair of the Cybercrime Convention Committee (T-CY)
- Jayantha Fernando, Director/Legal Advisor, ICT Agency of Sri Lanka
- Monika Josi, Chief Security Advisor, Microsoft EMEA
- Bill Smith, PayPal
- Zahid Jamil, Barrister-at-law, Pakistan

Moderator: Alexander Seger, Council of Europe

www.coe.int/cybercrime

The Council of Europe is a political organisation that brings together over 800 million citizens from 47 countries, making up an entire democratic continent. Its key aim is to promote democracy, the rule of law and human rights. Its headquarters are in Strasbourg, France. www.coe.int

Human rights
Rule of law
Democracy

