Cybersecurity 101

Vanessa Copetti Cravo

Topics

- Definitions;
- Issues;
- Cybercrime;
- Cybercrime Figures;
- Major and Recent Incidents;
- Overview of Cyber Threats;
- Historical Perspective;
- Policy and Regulatory Aspects;
- Regional and International Organizations and Initiatives.

What is the first word that comes to your mind when you think of cybersecurity?

Law
Spam
Surveillance
Child
Agencies
Cybercrime
Defense
Infrastructure
Disclosure
CSIRT
IoT
Enforcement
Cybersecurity
Awareness
Human
National
Multi-stakeholders
Strategy
Backdoors
Vulnerability
Botnet
Cryptography
Cooperation
DDoS
Online
Mass
Collaboration
Critical
Rights
Protection
Privacy
Cyberdefense
Malware
Cyberwar

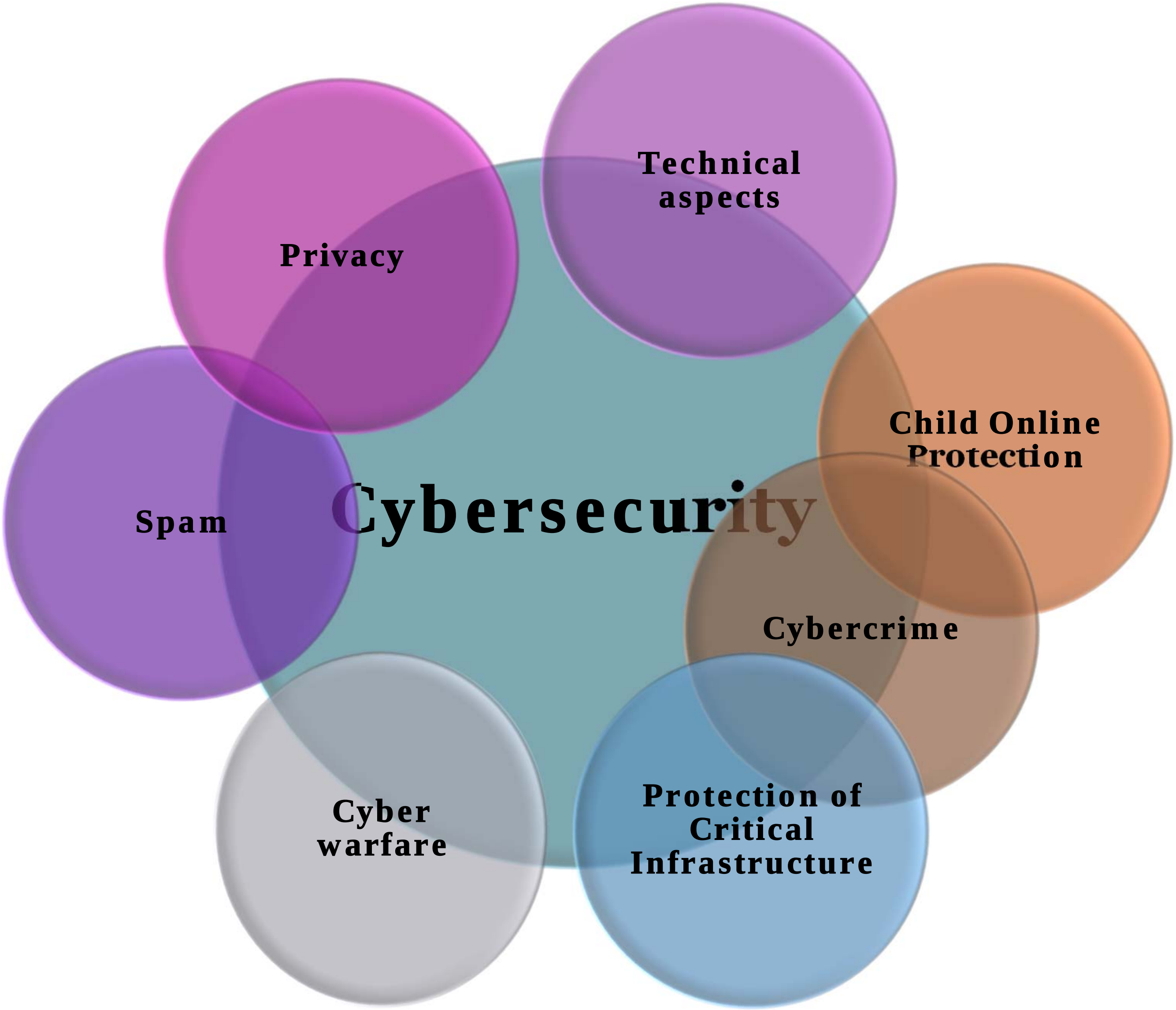
Cybersecurity definitions:

- “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; and **Confidentiality”**. (ITU-T X.1205).

- “art of assuring the existence and continuity of a Nation’s Information Society, in order to guarantee and protect its information assets and its critical infrastructures in the cyberspace” (Administrative Rule nº 45/2009 of Brazil’s Cabinet for Institutional Security);
- “preservation of confidentiality, integrity and availability of information in the Cyberspace” (ISO/IEC 27032);
- Definitions relates to the stakeholder’s perspective.

Issues

- **Critical Information Infrastructure Protection;**
- **Cybercrime;**
- **Child Online Protection;**
- **National Strategy;**
- **CSIRTs;**
- **Technical Aspects;**
- **Spam;**
- **Awareness;**
- **Vulnerability disclosure;**
- **Privacy;**
- **International Cooperation;**
- **Collaboration.**


Privacy
Technical aspects
Spam
Cybersecurity
Child Online Protection
Cybercrime
Cyber warfare
Protection of Critical Infrastructure

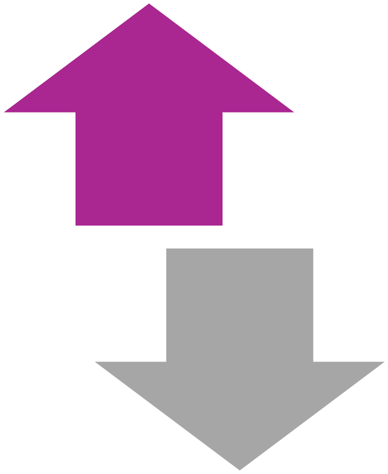
Cybercrime

- **Broad definition: ICTs are used as tools, as means to commit crimes or ICTs are the target of unlawful behavior;**

- **Transnational crimes, borderless.**

Cybercrime Figures

Annual cost to Global Economy: more than $400 billion



Maximum $575 billion

Conservative estimate

$375 billion

Source: Net Losses: Estimating the Glocal Cost of Cybercrime. Economic Impact of Cybercrime II. Intel Security and Center for Strategic and International Studies Report. June 2014.

- **The average cost for each lost or stolen record containing sensitive and confidential information - $141** (2017 Cost of Data Breach Study: Global Overview – Ponemon Institute);

- **Forecast: $6 trillion estimate costs by 2021** (Cybersecurity Ventures).

Major and Recent Incidents

- 1988 – USA *versus* Robert Tappan Morris (Cornell University's student);
- 2007 – Estonia cyber-attacks – online service of banks, government bodies and media were taken down;
- 2009 – Google China Attack;
- 2010 – Stuxnet Virus – Iran's nuclear program;
- 2013 (2016) - Yahoo massive data breaches (up to one billion user accounts compromised);
- 2014 - Anthem – 80 million patient and employee records;
- October 2016 - Dyn DDoS attack –Twitter, Amazon, Netflix, Paypal, etc;
- May 2017 - WannaCry Ransomware – more than 200,000 systems across 150 countries.

Historical Perspective

- 1992 - OECD Guidelines for the Security of Information Systems;
- 1998 – 53rd Session of General Assembly of the United Nations. Resolution 70 - Developments in telecommunications and information in the context of international security;
- 2000 – UNGA Resolution 55/63 - Combating the criminal misuse of information technologies;
- 2001 – Council of Europe Convention on Cybercrime (entered into force – 2004);
- 2002 – OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security ;
- 2002 – UNGA Resolution 57/239 - Creation of a global culture of cybersecurity;

Historical Perspective

- 2003 – WSIS 1st Phase – Geneva Plan of Action – Action Line C5 - Building confidence and security in the use of ICTs;
- 2005 – WSIS 2nd Phase – Tunis Agenda for the Information Society – ITU C5 moderator/facilitator;
- 2009 – UNGA Resolution 64/211 - Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures (self-assessment tool);
- 2011 – UNODC – 1ST session open-ended intergovernmental expert group – comprehensive study on cybercrime (UNGA Resolution 65/230);
- 2013 –Response to mass surveillance scandal – UNGA Resolution 68/167 - The right to privacy in the digital age.

Cyber Threats Overview

- Types and techniques: malware (virus and ransomware); phishing; spear phishing; whaling; DDoS; worms; scans; botnets; etc.

- Classified by targets: cyber espionage (economic, political or military advantage); cyber conflicts (national security component); and cybercrime.

Policy and Regulatory Aspects

- **National Strategy (awareness; identify lead person/institution; experts and roles; risk management process; assess and reassess);**
- **Appropriate Legislation (substantive; procedural and mutual assistance);**
- **Collaboration between Public and Private Sectors;**
- **International Cooperation Mechanisms;**
- **Technical capabilities (CSIRTs, standards, etc).**

Organizations and Initiatives

- I-STAR Organizations: ICANN, ISOC, IETF, Regional Internet Registries (LACNIC and ARIN - Americas);
- IGF – Internet Governance Forum;
- ITU – International Telecommunication Union;
- UNODC - United Nations Office on Drugs and Crime ;
- OECD – Organization for Economic Co-operation and Development - Working Party on Security and Privacy in the Digital Economy;
- World Economic Forum – Cybercrime Project and Cyber Resilience;
- IMPACT – International Multilateral Partnership Against Cyber Threats;
- FIRST – Global Forum of Incident Response and Security Teams;

Organizations and Initiatives

- Council of Europe;
- The Commonwealth Cybercrime Initiative;
- Global Forum on Cyber Expertise;
- NATO Cooperative Cyber Defense Centre of Excellence – Tallinn Manual (2013); 2.0 Tallinn Manual on the International Law Applicable do Cyber Warfare;
- OAS – Inter-American Integral Strategy to Combat Threats to Cyber Security - Inter-American Committee Against Terrorism; Inter-American Cooperation Portal on Cybercrime and the working group.

Summing Up!

- **Cybersecurity: several issues – different perspectives;**
- **Impossible to dissociate cybercrime from cybersecurity;**
- **Economic impact of cybercrime: threat to the global economy;**
- **Cybersecurity: international agenda hot topic for many years and it will continue to be;**
- **There are many organizations at regional and international levels addressing these issues, from different perspectives and approaches.**

Questions/comments
vanessac@anatel.gov.br