Cybersecurity

IN 1988, PUBLIC USE OF THE INTERNET was in its infancy, and the International Telecommunication Regulations (ITRs) compiled in that year did not contain explicit provisions on cybersecurity. But they did include (in Article 9) a reference to avoiding "technical harm," added in response to one of the first pieces of malware, the Morris worm, that was circulating at the time. In the decades since then, protecting cybersecurity has grown enormously in importance and will be considered as the ITRs are reviewed. There are proposals to add or amend articles in the treaty to include security-related elements, including measures against spam.

The number and sophistication of cyber-attacks are increasing, at the same time as our dependence grows on the Internet and other networks for critical services and information. According to the security company McAfee, 2011 saw the largest ever number of discovered threats. There are said to be at least 70 million different pieces of malware in circulation worldwide, and smartphones have become a vehicle for their dissemination. Analysts report that at least 70% of emails are spam.

Meanwhile, smart power grids, cloud computing, industrial automation networks, intelligent transport systems, e-government and electronic banking — to name just a few new types of infrastructure — are becoming interconnected. Failure in one can affect others. Alongside greater convenience and efficiency lies greater vulnerability to cyber-attack.[1]

However, there is not yet a globally accepted definition of cybersecurity. This hampers protection efforts, which must be undertaken at both national and international levels, given the borderless nature of today's networks and computer systems.

Incidents related to information and communication technologies (ICTs) are usually treated within existing national penal codes, which are often not updated or aligned to global trends. We do not yet have a common international standard of relevant offences; should they include software piracy, for example, along with dissemination of child pornography? Financial fraud, as well as denial of service attacks? The answer could be to harmonize domestic laws and establish a legal framework on which international cooperation can be delivered. Some, however, believe that this is not needed, or should only be undertaken at the regional level.

Laws are not the only — or the speediest — response to cyber-attacks. Technical solutions can be complemented by standards that achieve interoperability and conformance to security measures. This is especially significant because of the interdependence of networks in today's world. ITU's Telecommunication Standardization Sector (ITU-T) has published around 300 standards relating to cybersecurity. ITU also assists developing countries in this area, and supports the creation of computer incident response teams, or CIRTs. In its Global Cybersecurity Agenda,[2] ITU promotes international cooperation.

This work is part of ITU's mandate to lead the coordination of international efforts in "building confidence and security in the use of ICTs" — a task with which it was entrusted by world leaders at the World Summit on the Information Society held in 2003 and 2005.

---

[1] See also the WCIT Background Brief on Protection of Critical National Infrastructure.

[2] See www.itu.int/osg/csd/cybersecurity/gca/

