United Nations Inter-Parliamentary Union International Telecommunication Union

# Fourth Parliamentary Forum on Shaping the Information Society The Triple Challenge of Cyber-Security: Information, Citizens and Infrastructure

**18-20 May 2011**
**Room II - ILO Conference Center**
**International Labour Organization**
**Geneva, Switzerland**

## AIDE MEMOIRE

### Context

The last few years have seen a dramatic increase in the occurrences of Internet-related criminal activity. Reports of data and privacy breaches, as well as cyber-attacks, have become a regular feature in the media. Because of its rapid expansion, openness, and low barrier to entry, the global network is rapidly becoming a favorite playground for a host of ill-intentioned activities, such as spam, child pornography, financial frauds, and industrial espionage. Organized crime has taken a firm foothold on the Internet. For cyber-criminals, the opportunity cost is very low and the potential rewards very high. They control vast networks of computers infected with malicious software (botnets) without their owners' knowledge, which can be used anonymously to steal users' data and target more unsuspecting victims. They offer their services for hire in a thriving online black market where credit card data, bank account information, email addresses and other illicitly acquired data are traded. The underground online industry is reported to have had a double digit growth in 2010[1]. It is estimated that cybercrime globally costs corporations about €750 billion per year[2]. Although it is difficult to obtain accurate information, overall losses to society could be higher, as individual financial losses are often under-reported.

Due to the progress in broadband and mobile telecommunication, more and more users access the Internet and perform transactions using new mobile devices such as smartphones and tablets. These are in essence new computing platforms whose security features are not yet mature, providing cyber-criminals a fertile ground for accessing sensitive information and performing unauthorized transactions at the legitimate users' expenses. At the same time, voluntarily or not, citizens are disclosing a staggering amount of personal information about themselves in their regular and sustained use of social networks, literally leaving behind a virtual trail of digital breadcrumbs that can be easily pieced together for illegitimate purposes. Often unaware of the implications for their privacy, users are enticed to reveal publicly more and more about their private

[1] UPI.com: Cybercrime 'industry' sees double-digit growth, http://www.upi.com/Business_News/Security-Industry/2011/03/02/Cybercrime-industry-sees-double-digit-growth/UPI-66271299103546/

[2] Europol: Cybercrime as a business: The digital underground economy, http://www.europol.europa.eu/index.asp?page=news&news=pr110106.htm

lives, leading to a rethinking of the very concept of privacy in the Internet age. The aggregation of private data, such as Internet browsing habits, online purchases, social circle of friends, and frequented geographical locations are at the core of business models that fuel a multi-billion dollars Internet industry. Unsurprisingly, the growing Internet economy also attracts the attention of cyber-criminals.

Despite a few high profile and much publicized instances of cyber-criminals successfully apprehended, it is clear that the lack of an internationally-agreed policy and regulatory framework on cyber-security hampers governments' efforts. Recent cases[3] of dismantled child pornography networks illustrate the extent of international cooperation that is required, with several law enforcement agencies involved in tightly coordinated operations to apprehend the culprits and disrupt their criminal activities.

In this complex and rapidly evolving environment, governments are struggling to keep up with the rapid pace of illicit use of technological innovation to ensure the security of their citizens, sensitive information and infrastructure. The global nature of the Internet and the transnational character of cybercrime are particularly challenging for them as cyber-criminals could be located anywhere in the world and often collaborate online with one another without ever having met physically. Laws and regulations differ from one country to another, allowing cyber-criminals to enjoy safe havens in countries that have not enacted appropriate legislations[4].

Furthermore, the political process for negotiating international agreements and for enacting coordinated provisions on cyber security is proving slow when compared to technological evolution. Since the Convention on Cybercrime was adopted in 2001[5], Facebook, Twitter, smartphones and cloud computing, botnets and "phishing attacks" have made their apparition on the technological landscape, opening new and more challenging avenues for discussion.

In addition, while pressed to address cyber-security issues by their constituencies, governments often risk to overreact and to unsettle the delicate balance between security concerns and citizens' fundamental rights, which could be eroded by voluntary or involuntary decisions of the executive. A study published by the European Parliament confirms that ICTs offer new opportunities for protecting and advancing human rights, but at the same time, present direct threats to those same rights, by allowing the development of increasingly sophisticated censorship and surveillance mechanisms[6]. The recent wave of unrest in the Middle East well illustrates this nexus, as protest movements initially leveraged online tools to coalesce and organize, some private companies set up new platforms to evade government-imposed restrictions, and anonymous cyber-attacks were launched against government websites in support of the protesters, leading in some extreme case to a government cutting off its entire country from the Internet in an attempt, ultimately ineffective, to stifle dissent.

Against this background it is evident that addressing cyber-security has become a priority on the agenda of many governments and of the international community as the impact of online threats is pervasive and requires both national and international responses.

[3] V3.co.uk: Hacker arrested on Mariposa botnet charges, http://www.v3.co.uk/v3-uk/news/1950312/hacker-arrested mariposa-botnet-charges SV Mercury News: International child porn ring is broken up, http://www.mercurynews.com/california/ci_16857738

[4] For example, the recent attempts to prevent access to classified materials released by Wikileaks were largely ineffective as the content was replicated on hundreds of servers out of reach of international or bi-lateral agreements.

[5] In 2001 the Council of Europe adopted the Convention on Cybercrime , which came into force in 2004. It is worth noting that support for the Convention is far from unanimous.

[6] Study: Information and Communication Technologies and Human Rights, European Parliament, June 2010, EXPO/B/DROI/2009/24, www.europarl.europa.eu/activities/committees/studies.do?language=EN

As the public institution most accountable to the electorate for ensuring citizens' security, safeguarding their rights, and promoting a people-centred information society, Parliaments have a special responsibility to become actively engaged in shaping the direction of the cyber-security agenda. As legislators are tasked to ensure that laws truly benefit the constituencies they represent, it is the parliamentarians' role to strike the most judicious balance between competing needs, by fostering an information society that reaffirms and reinforces fundamental human rights while ensuring citizens' safety and the protection of information and infrastructure. In doing so, the Parliament must fully exert its oversight role over the executive branch and law enforcement agencies by carefully scrutinizing their responses to technology-based threats and challenges.

At the international level, there is much that parliaments can do to advance global coordination and harmonization of cyber-security laws and regulations, through increased cooperation and exchange among members of parliament and committees dealing with the issue.

## Objectives of the Parliamentary Forum

The Parliamentary Forum "T*he Triple Challenge of Cyber-Security: Information, Citizens and Infrastructure*" is the fourth meeting of members of parliament focusing on issues relating to the Information Society organized within the framework of the Global Centre for ICT in Parliament, a partnership initiative launched by UN/DESA and the Inter-Parliamentary Union (IPU) at the WSIS in 2005.

The Fourth Parliamentary Forum will focus on the representative, law-making and oversight responsibilities of members of parliaments in the area of cyber-security. It will address the particular challenges posed by the illicit use of information and communication technologies, such as the safeguarding of citizens in the connected environment; the protection of State information, data and infrastructures; and the transnational response to cybercrime.

The aim of the Forum is to further the dialogue among legislators on the different strategic and political priorities implemented at the national level, outline a broad perspective of different national engagements directed at responding to the challenge discussed, delineate the role and responsibilities of parliaments in their legislative and oversight functions with respect to the topic addressed, identify good parliamentary practices and draw recommendations for action by legislatures.

## Meeting venue and format

The Parliamentary Forum will take place on 18, 19 and 20 May 2011 at the Headquarters of the International Labour Organization in Geneva, Switzerland. It will start at 03:00 pm on Wednesday, 18 May, with the Opening Ceremony, and it will close at 01:00 pm on Friday 20 May 2011.

The Forum will be structured around a series of plenary sessions with presentations by high-level experts and legislators from different countries. In each session, ample time will be reserved to allow interventions from the floor, interactive dialogues and open debates among members of parliament.

## Participation

The Parliamentary Forum expects to attract 150 members of parliament with responsibilities for Information Society issues from all over the world. It is expected that the Chairs/Presidents of parliamentary Committees with responsibility for Science and Technology, Information and Telecommunication and/or security issues will lead the delegations and participate actively in the debates with peers from other countries and regions.

Other participants will include senior representatives and officials of international organizations, as well as experts from agencies, governments, the ICT industry and the academia.

### Contributions by Parliaments

To enrich the Forum with information on national experiences, delegations are strongly encouraged to submit in advance a brief report describing the different parliamentary actions implemented at the national level to address the global issues of cyber-security. The contributions should focus on the role played by parliaments, parliamentary committees and legislators in representing the electorate's views, in fostering the law- and policy-making process and in ensuring scrutiny on government-led activities.

Contributions should be submitted in English, French or Spanish following the enclosed template, also available on the web page of the Forum.

### Languages

The working languages of the meeting will be English, French and Spanish. Simultaneous interpretation will be available in the three languages.

### Organizers

The Fourth Parliamentary Forum will be co-organized by the United Nations Department of Economic and Social Affairs (UN/DESA), the Inter-Parliamentary Union (IPU) and the International Telecommunication Union (ITU), through the Global Centre for ICT in Parliament.

#### United Nations – Department of Economic and Social Affairs (UN/DESA)

The United Nations Department of Economic and Social Affairs (DESA) promotes and supports international cooperation to achieve development for all, and assists governments in agenda-setting and decision-making on development issues at the global level. DESA provides a broad range of analytical products and policy advice that serve as valuable sources of reference and decision-making tools for developed and developing countries, particularly in translating global commitments into national policies and action and in monitoring progress towards the internationally agreed development goals, including the Millennium Development Goals.

#### International Telecommunication Union (ITU)

ITU is the leading United Nations agency for Information and Communication Technology (ICT) issues, and the global focal point for governments and the private sector in developing networks and services. For nearly 145 years, ITU has coordinated the shared global use of the radio spectrum, promoted international cooperation in assigning satellite orbits, worked to improve telecommunication infrastructure in the developing world, established the worldwide standards that foster seamless interconnection of a vast range of communication systems and addressed global challenges, such as mitigating climate change and strengthening cybersecurity. ITU is based in Geneva, Switzerland, and its membership includes 191 Member States.

#### Inter-Parliamentary Union (IPU)

The Inter-Parliamentary Union is the international organization of Parliaments. It was established in 1889 and is the focal point for world-wide parliamentary dialogue and works for peace and co-operation among peoples and for the firm establishment of representative democracy. IPU's Headquarters is in Geneva, Switzerland, and it currently has 151 Members and 8 Associate Members.

#### Global Centre for ICT in Parliament

The Global Centre for ICT in Parliament is a joint initiative of the United Nations Department of Economic and Social Affairs, the Inter-Parliamentary Union and a group of national and regional parliaments established in the framework of the World Summit on the Information Society process in November 2005. Its objectives are a) to foster the role of parliaments and legislators in the promotion of the information society, and b) to reinforce parliaments' capacity to harness ICT tools to better fulfill their democratic functions and to place them at the service of the institutional process and of inter-parliamentary cooperation.