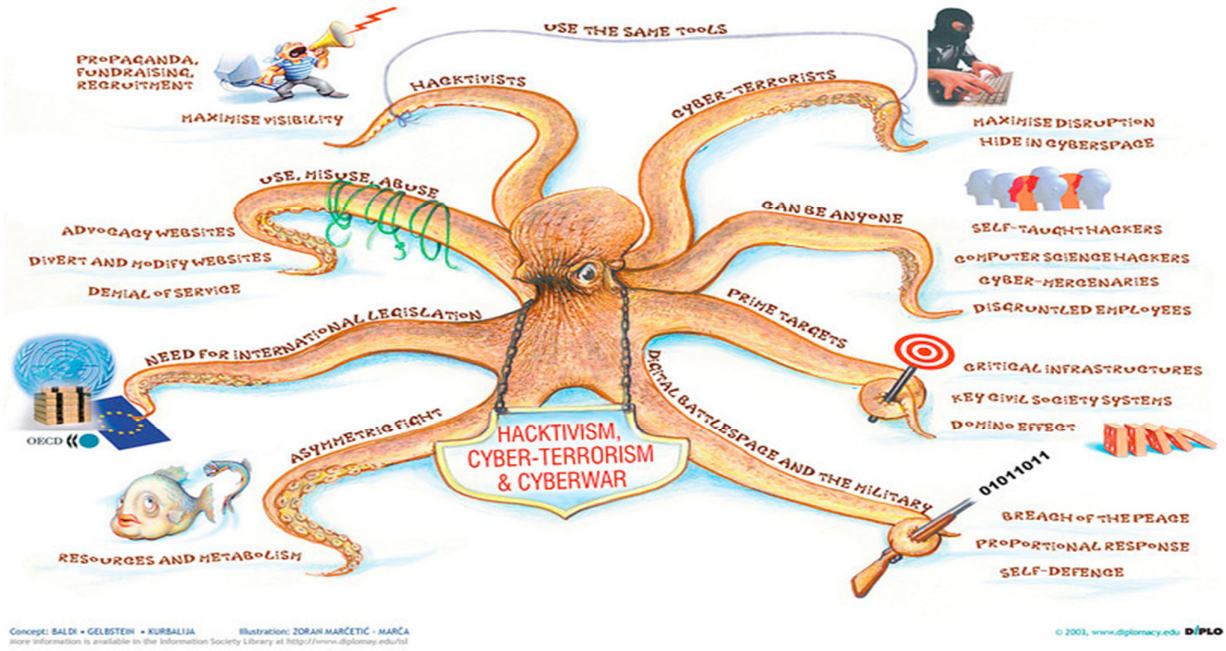
Cybersecurity: issues, actors, and challenges

Background note for the session 'Assuring cybersecurity in the Western Balkans and the rest of Europe: Roles and responsibilities of institutions, industry and users?' co-organised by DCAF and BSF at the Belgrade Security Forum 2013

Mapping the cybersecurity scene



Protection of critical information infrastructure (CIIP) which supports vital infrastructures in modern society, including communications, energy, water, and finance, is increasingly important – as is the protection of this critical society infrastructure *per se*. The vulnerability of the Internet is becoming the vulnerability of modern society.

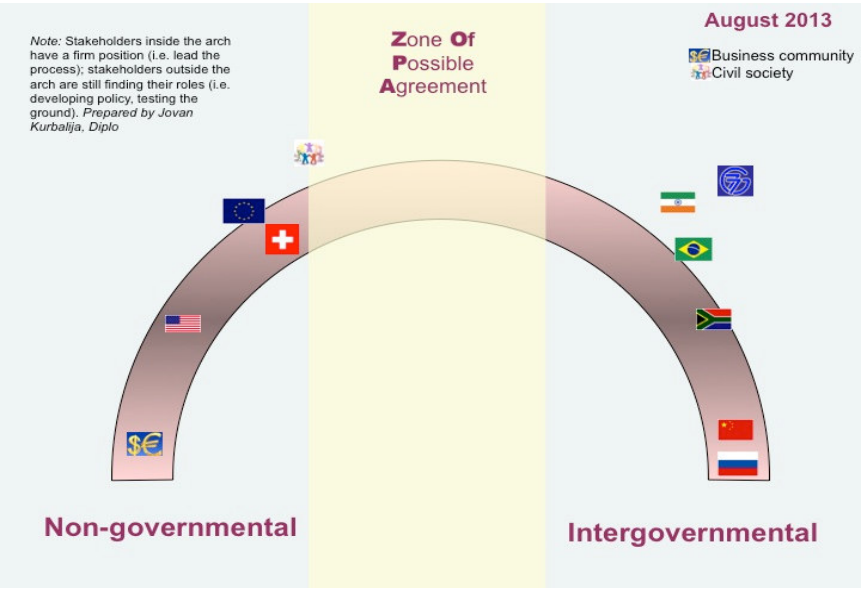
Cybercrime is crime committed via the Internet and computer systems. It includes old, i.e. traditional crimes now conducted through cyberspace (like various frauds), crimes that have evolved due to technology (e.g. credit card frauds and child abuse), new crimes that have emerged with the Internet (e.g. Denial of Service attacks and Pay per click frauds), and cybercrime tools which are used to facilitate other crimes (e.g. botnets). Combating child pornography is the most developed area of international cooperation; this cooperation is missing, however, in dismantling global cybercrime black markets which offer outsourced criminal services and easy-to-use digital weapons (e.g. viruses and botnets) to almost anyone.

Cyberterrorism came into sharper focus after 9/11, when an increasing number of cyberterrorist attacks were reported. Cyberweapons developed for criminal purposes are also used by cyberterrorists but to a different end. While cybercriminals are motivated mainly by financial gain, cyberterrorists want to cause major public disruption and chaos. Attempts to prevent terrorist acts in cyberspace are often challenged by possible breaches of human rights.

Cyberconflicts, often labelled as cyberwar, have high media visibility and still low policy and legal reflections. Cyberconflicts can be dissected in three main areas: *conduct of cyberconflicts* (i.e. can the existing law, mainly The Hague Conventions, be applied to cyberspace; if not, what type of new legal instruments should be developed?); *weapons and disarmament* (i.e. how to introduce cyberweapons into the disarmament process); and *humanitarian law* (i.e. how to apply Geneva conventions to cyberconflicts).

The main actors in cybersecurity

This graph presents the general position of the main actors on one of the main questions in Internet governance and cybersecurity, i.e. the roles and responsibilities of governments and other stakeholders.



Position of the main actors in global Internet governance

On one side, the USA and the business sector are arguing for the maintenance of the current, predominantly non-governmental model, with strong participation by the business sector. On the other side sit Russia and China, followed by many developing countries, arguing that the Internet should be governed at international level by inter-governmental organisations, such as the International Telecommunication Union (ITU). The rift – described by some authors as the 'digital Cold War' – widened during the ITU World Conference on International Telecommunications (WCIT) in December 2012, when the US-led block of 55 countries 'against' was outvoted by 89 countries 'in favour' of the amended International Telecommunication Regulation (ITR). One of the major amendments was the introduction of a direct reference to cybersecurity.

However, the clustering of countries around specific issues – like security, data protection, or openness – provides a more conducive space for trade-offs and possible package deals in Internet governance negotiations. The European Union, Brazil, India, Switzerland, and Norway, among others, have been trying to create a 'zone of possible agreement' in the global digital policy debate.

The closer we move towards concrete cybersecurity issues, the more we realise the specific roles of various actors and the need for a multistakeholder approach. Any of the actors alone – including the most powerful states – cannot ensure Internet security without the broader participation of many: from individuals to corporations.

On the decision-making level, **governments** need to be able to decide on policies and share operational resources, and also defend themselves (and even attack) – in accordance with international law. Nevertheless, they also have a responsibility not to militarise cyberspace by cyber-armament and exclusive policies. Instead, they need to create inclusive policy-shaping environments that define the roles and responsibilities of other stakeholders and enable them to perform their respective roles.

> ***Government actions**: Support inclusive and multistakeholder policy processes, invest in evidence-based policy-making, raise general awareness, and build capacity*

On the operational level, the role of the **business sector** is vital for cybersecurity. Most of the critical Internet infrastructure and services (cables, software, and hardware) is developed and run by private companies – the protection of which requires their active participation. Companies in the Internet industry also have huge responsibility for global cybersecurity: the financial, energy, manufacturing, and technology sectors are among the most frequent targets of cyber-attacks (most commonly for espionage activities and intellectual property theft).

Business sector actions:
Develop a system which will ensure discretion in reporting on and sharing details about cyber-attacks, and invest in awareness raising and capacity building (especially among SMEs)

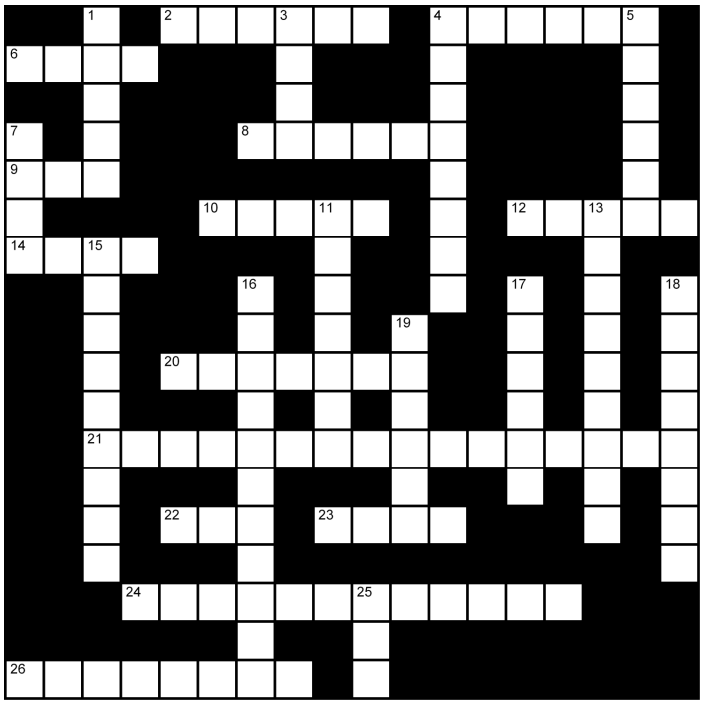
Awareness of the risks and capacity to prevent and react to incidents are the responsibility of the corporate sector, including small and medium enterprises (SMEs), which are the most vulnerable. More importantly, the corporate sector needs to be incentivised to report these incidents (thus prioritising global security over short-term risk to reputation): currently there is very little available information on the formats and effects of sustained incidents and cyber-attacks, which curbs research into protective measures.

Finally, individual Internet **users** are the pillars of cybersecurity. Yet we are often the 'weakest link' when it comes to protection from cyber-attacks: due to our negligence or ignorance, our personal computers are used to stage cyber-attacks (as part of botnets) and spread spam, viruses, and malware, among others. Unprotected access to our computers and mobile devices offers a backdoor for access to the datasets of our company or institution, and compromises many more computers.

Civil society, as a catalyst for activism, plays an important role in raising the awareness of and educating users. Equally important, however, is its role in balancing the security policies with human rights – such as freedom of expression, access to information, and openness of the Internet. Its involvement with policy-shaping processes, as well as with policy implementation, is fundamental for cybersecurity on all levels.

End-users and civil society actions:
Increase awareness, develop 'good digital hygiene' and a cybersecurity culture, and safeguard a balanced approach to security with respect to human rights

Test your cybersecurity knowledge



You can find solutions to the crossword and take a 'cybersecurity background test' at http://www.diplomacy.edu/ig/cybersecurity/

For comments and discussion on the briefing note, contact the authors: Jovan Kurbalija (jovank@diplomacy.edu) and Vladimir Radunovic (vladar@diplomacy.edu)

For more information about cybersecurity courses, consultancy, and research, consult DCAF (www.dcaf.ch) and DiploFoundation **(**www.diplomacy.edu**)**

Across

2 Cyber-operation involving a set of attacks on US corporations and government institutions in 2009, allegedly performed with the support of the Chinese army (6)

4 A remote-controlled network of hijacked personal computers – zombies – that perform directed attacks or distribute malware (6)

6 The ITU conference of December 2012 in which the amended International Telecommunication Regulation were voted for, inserting a reference to cybersecurity (4)

8 City after which the Conventions establishing the standards of international law for the humanitarian treatment of war (possibly also applicable to cyberspace) were named (6)

9 Network system that translates computer (IP) numbers into domain names (3)

10 The infamous surveillance programme instigated by the US NSA (5)

12 US-based organisation that manages Internet names and numbers; one of the most important players in global Internet governance (5)

14 Unsolicited e-mail (4)

20 Name of the country which, in 2007, suffered one of the first major cyber-attacks on its national e-infrastructure (7)

21 A policy-shaping model involving a variety of stakeholders, advanced particularly through the Internet governance process (16)

22 The main UN agency for telecommunication issues – initiator of the Global Cybersecurity Initiative (3)

23 A team of experts tasked with handling computer security incidents within a critical information infrastructure, first organised at the Carnegie Mellon University in the USA (acronym) (4)

24 One of the main legal challenges for prosecuting cyber-offenders (12)

26 Type of online scam to acquire personal information such as usernames, passwords, and credit card details (8)

Down

1 The best-known and one of the oldest types of malware (5)

3 European security organisation increasingly focusing on cybersecurity (4)

4 The city of birth of the Convention on Cybercrime of Council of Europe of 2001 (also known as the _____ Convention) (8)

5 Type of malware that performs actions that are not authorised by the user, such as data deletion, blocking, modifying, copying (6)

7 Form of cyber-attack involving multiple computers aimed at rendering a targeted server or network inaccessible for a period of time (acronym) (4)

11 Name of the virus that was used for an alleged Israeli attack on computers at Iranian nuclear facilities (7)

13 US General commanding the US Cyber Command, also a Director of the NSA, Keith _____ (9)

15 International network of hacktivists behind the publicised DDoS attacks on corporate and government websites (9)

16 One of the main challenges for applying existing international conventions on warfare to cyberspace (11)

17 Author of the science-fiction novel *Neuromancer* who coined the word 'cyberspace', William _____(6)

18 Another common name for international cyberconflict (8)

19 A skillful computer user that seeks and exploits weaknesses in a computer system or computer network (6)

25 Acronym for a multistakeholder body designated by a decision of the World Summit on the Information Society (3)