Istituto Affari Internazionali

IAI WORKING PAPERS 11 | 26 – September 2011

Ambiguous Definitions in the Cyber Domain: Costs, Risks and the Way Forward

Federica Di Camillo and Valérie Miranda

Abstract

The modern-day importance of the cyber/Information and Communication Technology (ICT) sector rests upon various considerations: it is at the basis of most of the critical infrastructures of modern societies, and can be both the direct object of attacks or incidents on Critical Information Infrastructures (CIIs) and the means of striking indirectly at the critical infrastructures whose own operations are based on it (i.e., transport networks, energy and water distribution networks, nuclear plants and banking and financial systems). This paper aims at showing that the existence of problems of definitions, and above all of their harmonisation, brings inefficiencies to various aspects of the management of the cyber sector, in particular normative production, countermeasures and law enforcement. As a way forward, it suggests some proposals for improvement at the European, transatlantic and international levels.

Keywords: *European Union / United States / Cyber-security / Information terminology*

Ambiguous Definitions in the Cyber Domain: Costs, Risks and the Way Forward

Federica Di Camillo and Valérie Miranda*

The modern-day importance of the cyber/Information and Communication Technology (ICT) sector rests upon various considerations: it is at the basis of most of the critical infrastructures of modern societies, and can be both the direct object of attacks (intentional) or incidents (unintentional) as regards Critical Information Infrastructures (CIIs) and the means of striking indirectly at the critical infrastructures whose own operations are based on it (such as transport networks, energy and water distribution networks, nuclear plants and banking and financial systems).

This implies a notable complexity with a sort of multiplying effect of the relevance of the sector and of the reach of its involvement for reasons of geography, functionality and liability. Geography, because critical infrastructures (or systems) are for the most part transnational and therefore require the involvement of several States. Functionality, because the interconnections of modern-day critical infrastructures imply an interdependency in which vulnerabilities are transmitted from one system to another: for example, the breakdown of an ICT network, public or private, can affect electrical distribution, and vice versa, i.e. a lack of electricity can interrupt the functioning of ICT networks[1]. These geographical and functional domino effects of the vulnerabilities of systems have the potential for a very high impact, and can involve both public and private subjects, the latter being fundamental as the owners of infrastructures and/or the managers of their security (this is the case on average 80% of the time in developed countries).

This is a relatively new subject which is in constant evolution, and this paper is designed to facilitate understanding of this complex theme. It is our aim to show in particular that the existence of problems of definition, and above all of the harmonization of definitions, impacts negatively on various aspects of its management, in particular normative production, countermeasures and law enforcement.

Paper prepared for the Istituto affari internazionali (IAI), September 2011.

* Federica Di Camillo and Valérie Miranda are respectively Senior Fellow and Junior Researcher in the Security and Defence Department at the Istituto affari internazionali (IAI). The authors thank Chantal Scaccabarozzi, intern at IAI, for her support to the present study and David Ashton, linguist, for the translation of the paper from Italian into English.

[1] Attacks can in fact be achieved in terms of disruptions, including partial disruptions and malfunctions, and also through intromissions which are not apparent and which are aimed at modifying data which are the object of exchange within the system - as in the case of Man-in-the-middle (MITM) attacks aimed at intercepting and manipulating information communications between two or more parties through an insertion in the flow of data which is unknown to those parties (to appreciate the seriousness of this, one can think for example of the intrusion in an air-traffic control system of erroneous coordinates).

1. Terminological variety and semantic ambiguity: European and US strategies compared [2]

Over the past decade, cyber-security has drawn the attention of the media and of experts. Although it is a global phenomenon, we will focus on a comparison of two significant situations: those of the European Union and the US. If in the latter the topic of cyber-security has already been amply treated and discussed since the 1990s, it is only from the beginning of the 2000s that it has received analogous - although not identical - treatment in the old continent.

Notwithstanding the growing interest in the problem on the part of government agencies and the proliferation of initiatives in this respect, it is interesting to note that the terms pertaining to the cyber domain are used in a rather indiscriminate and ambiguous manner without a common definition of cyber-threats having been reached at international level.

A reading of the relevant strategic documents[3] adopted by the European Union (EU) and the US in recent years offer interesting pointers in this sense.

In the European case, we will analyse five documents key to the external and internal security of the EU: the 2003 *European Security Strategy* (ESS), the 2008 report on its implementation, slightly anticipated by the Council Declaration entitled *Statement on tighter international security*, the 2010 *Internal Security Strategy* (ISS) for the European Union, followed by the European Commission's communication on the ISS in action (2010).

As is shown by Table 1, "cyber-terms", although present in European strategies, are not precisely defined. They do however show the growing awareness of the Community institutions in cyber-threats: if the 2003 EES refers only to the general danger posed by the misuse of electronic networks, the later documents treat the topic more broadly so as to arrive at the 2011 ISS and the related Commission communication, which pay particular attention to cyber-crime.

From an analysis of the main US strategic documents, i.e. the 2010 *National Security Strategy* (NSS) of the White House, the first-ever 2010 Department of Homeland Security (DHS) *Quadrennial Homeland Security Review* (QHSR), the 2010 Department of Defense (DoD) *Quadrennial Defense Review* (QDR) and the recent *International Strategy for Cyberspace* of the White House (2011), it emerges that these documents treat the topic of cyber-security in a much more extensive manner as compared to the European documents. This reflects the long-standing commitment of the US to the

[2] This chapter is based heavily on Federica Di Camillo and Valérie Miranda, "Cybersecurity: Toward EU-U.S. Cooperation?", in IAI, UI, FRS, CSIS, *EU-U.S. Security Strategies. Comparative scenarios and recommendations*, Washington, Center for Strategic and International Studies, April 2011, p. 55-67, http://www.iai.it/content.asp?langid=2&contentid=+599.

[3] These documents have been chosen because they constitute a reference point for the policies deriving from them.

sector, as epitomized by the statement of Obama that "digital infrastructure is a strategic national asset and protecting it is a national security priority".[4]

The greater attention and commitment to the sector on the part of the US agencies have not yet however been translated into a complete terminological clarity. Only the QDR contains a precise definition of cyberspace, understood as "the global domain that encompasses the interdependent networks of information technology infrastructures, including the Internet and telecommunication networks".[5] Furthermore, if it is true that all the US strategies deal with cyber-attacks in a way which is rather coherent between themselves, their nature and means of achievement, the potentially responsible entities (i.e. State or non-State actors, terrorists or organized crime), and the possible objectives are not included in a definition *tout court*, but have to be deduced from an integral reading of the entire contents of the documents.

Beyond these observations relating to the problem of definition, one can point out that analysis of the strategic documents is nevertheless useful in so far as those documents outline certain commitments that the EU and the US intend to make in the future in order to strengthen their own cyber-security. Although the US commitments are of a more operational nature, one can note an interesting convergence between the EU and US commitments for the purposes of the present analysis, in particular in the cyber-crime sector: the need for a greater degree of cooperation at the internal and international levels to harmonise (and eventually update) the existing normative frameworks and to define in a more homogenous manner the legal scenarios in order *inter alia* to render the criminal prosecution of crimes more effective.

[4] White House, *National Security Strategy*, Washington, May 2010, http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf, p. 27.
[5] US Department of Defense, *Quadrennial Defense Review Report*, Washington, February 2010, http://www.defense.gov/qdr/images/QDR_as_of_12Feb10_1000.pdf, p. 37.

Table 1. Comparing EU and US Strategic Documents

EUROPEAN UNION			
DOCUMENT	**MAIN CYBER REFERENCES**	**DEFINITIONS**	**PROPOSED ACTIONS**
A Secure Europe in a Better World. European Security Strategy (2003)	[…] European dependence on an interconnected infrastructure […] in information […]	//	//
	[…] terrorist movements are well-resourced, connected by electronic networks	//	//
Report on the Implementation of the European Security Strategy - Providing Security in a Changing World (2008)	Cyber security	"Modern economies are reliant on critical infrastructure including transport, communication and power supplies, but also the internet. […] attacks against private or government IT systems have given this a new dimension, as a potential new economic, political and military weapon […]"	More work is required in this area, to explore a comprehensive EU approach, raise awareness and enhance international co-operation.
EU Council Declaration, Statement on tighter international security (2008)	[…] use of the internet by terrorist networks	//	[…] (to update legislation) to make recruitment and incitement to terrorism via the Internet a criminal offence
	Cyber attacks	≅ intrusions against public and private bodies	[…] increase the protection and resilience of our networks, by increasing operational cooperation between Member States
Internal Security Strategy for the European Union: 'Towards a European Security Model' (2010)	Cyber-crime	Global, technical, cross-border, anonymous threat to our information systems	//
	Terrorism […] propaganda over the internet	//	//
	New risks and threats such as […] ICT break down	//	//

The EU Internal Security Strategy in Action: Five steps towards a more secure Europe (2010)	Another growing threat is cyber-crime. Europe is a key target for cyber-crime because of its advanced Internet infrastructure (…)	//	Citizens, businesses, governments and critical infrastructure must be better protected from criminals who take advantage of modern technologies
	Cyber-crime is a global phenomenon causing significant damage to the EU internal market. Jurisdiction for prosecuting cyber-crime still stops at national borders. Raise levels of security for citizens and businesses in cyberspace.	//	Action 1: Build capacity in law enforcement and the judiciary (establishment of an EU cybercrime centre by 2013; increase cooperation between Member States) Action 2: Work with industry to empower and protect citizens (ensure that people can easily report cyber-crime incidents; increase cooperation between the public and the private sector; introduce guidelines to handle illegal internet content). Action 3: Improve capability for dealing with cyber-attacks (establish at national and EU levels functioning CERTs; network together national CERTs; develop national contingency plans and undertake regular national and European exercises in incident response and disaster recovery).
UNITED STATES			
DOCUMENT	**MAIN CYBER REFERENCES**	**DEFINITIONS**	**PROPOSED ACTIONS**
National Security Strategy (2010)	Secure cyberspace: it has a quite comprehensive view, generally speaking of “cyber threats”	Threats from individual criminal hackers to organised criminal groups, from terrorist networks to advanced nation states	To Deter, prevent, detect, defend against, and quickly recover from cyber intrusions and attacks by: 1. Investing in people and technologies to a. Better protect and improve the resilience of critical government and industry systems and networks 2. To strengthen international partnerships 3. To strengthen partnerships with the Government and with the private sector

Quadrennial Homeland Security Review (2010)	Cyber attacks	Carried out by state or non state actors (individual, (terrorist) groups): -Intrusions in search of information to use against the United States -Spreading of malicious codes in an attempt to destroy, disrupt the national information infrastructure and threaten the delivery of critical service + steal money and information	
	Cyberspace	//	DHS' vision is a cyberspace that supports a secure and resilient infrastructure, that enables innovation and prosperity, and that protects privacy and other civil liberties by design
	Safeguarding and Securing Cyberspace (4th DHS mission)	//	1. Creating a Safe, Secure, and Resilient Cyber Environment 2. Promoting cybersecurity knowledge and innovation
	Cyberspace is also cited when speaking of critical infrastructures and related protection (1st DHS mission)	See above	1. Protect critical infrastructure: a. Prevent high-consequence events by securing critical infrastructure assets, systems, networks, or functions—including linkages through cyberspace—from attacks or disruption.
Quadrennial Defense Review (2010)	Cyber domain	//	"more comprehensively monitor the air, land, maritime, space, and cyber domains for potential direct threats to the United States"
	Cyberspace	Global domain within the information environment that encompasses the interdependent networks of information technology infrastructures, including the Internet and telecommunication networks	//

	Cyberspace attacks	No clear-cut definition. It is only reported that they could target command and control systems and the cyberspace infrastructure supporting weapons system platforms.	DoD mission-critical systems and networks must perform and be resilient in the face of cyberspace attacks.
	§ Operate effectively in cyberspace	See above for the definition of cyberspace	1. Develop a comprehensive approach to DoD operations in cyberspace 2. Develop greater cyberspace awareness and expertise 3. Centralize command of cyberspace operations (USCYBERCOMMAND) 4. Enhance partnerships with other agencies and governments, in particular with the DHS.
International Strategy for Cyberspace (2011)	Cyberspace Cybersecurity threats Cybercrime	//	Selected expectations/commitments: "The US will work internationally to promote an open, interoperable, secure and reliable information and communications infrastructure (…) build and sustain an environment in which norms of responsible behaviour guide states' actions, sustain partnerships and support the rule of law in cyberspace" Diplomatic objectives: Strengthening partnerships - bilateral and multilateral partnerships - international and multi-stakeholder organisations - private sector collaboration Defence objective: dissuading (at home and abroad) and deterring Development objective: building prosperity and security - building technical capacity - building cybersecurity capacity - building policy relationships Policy priorities: Economy: promoting international standards and innovative, open markets Protecting our networks: enhancing security, reliability, and resiliency

			Law enforcement: extending collaboration and the rule of law - participate fully in international cybercrime policy development - harmonize cybercrime laws internationally by expanding accession to the Budapest convention - focus cybercrime laws on combating illegal activities, not restricting access to the Internet - (…) Military: preparing for the 21st century security challenges Internet Governance: Promoting effectiveness and inclusive structures International development: building capacity, security and prosperity Internet freedom: supporting fundamental freedoms and privacy

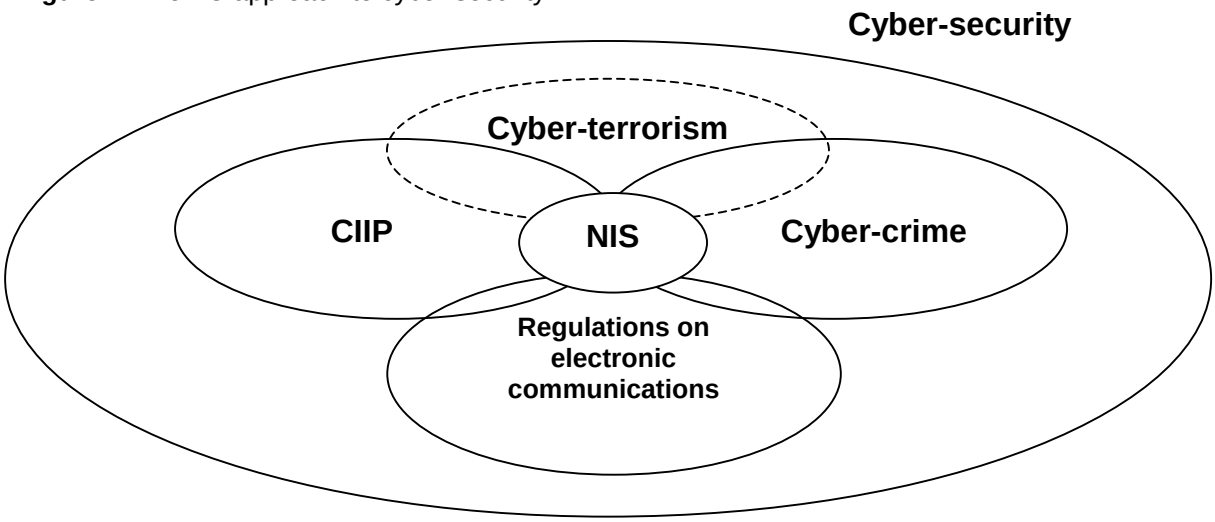
From what is set out above one can see therefore that an explicit and exhaustive definition of the term cyber-security is never once provided, even though reference is often made to the term. The impression is that it is used predominantly as a blanket term[6], with a meaning that can be deduced intuitively, in order to identify the problem and render it comprehensible even to people who are not experts in the field. On the other hand, the absence of a precise definition means that it is difficult to establish exactly the effective boundaries and scope of cyber-security, as well as the difference from other terms used with the same frequency, such as cyber-war, cyber-crime, and so on.[7] As we will see below, this is reflected negatively also in the identification of reference figures in the cyber domain who might have clearly-defined competences and responsibilities in one field rather than another.

In this vein, a univocal definition of what could be identified as subcategories or components of cyber-security, i.e. Critical Information Infrastructure Protection (CIIP) or cyber-crime and its innumerable manifestations, appears even more complex and important. At the European level, some official definitions of the latter can be identified in policy documents of a sectoral nature adopted by the EU in the second half of the 2000s. From our analysis of these documents and from consideration of the number and scope of the initiatives, one can deduce that the "priority" areas of interest and action for the EU in the broad domain of cyber-security are CIIP and the fight against cyber-crime (see figure 1).

[6] See in this regard also Hungarian Presidency of the Council of the European Union, *Cyberspace could also be war theatre*, 4 May 2011, http://www.eu2011.hu/news/cyberspace-could-also-be-war-theatre.

[7] The 18-month programme of the Polish, Danish and Cypriot Presidencies of the EU includes "cyber-crime" and "cyber-security" among its priorities without explaining their content and even at first sight as if the latter did not cover the former. Council of the European Union, *18 month programme of the Council (1 July 2011-31 December 2012)* (11447/11), Brussels, 17 June 2011, http://register.consilium.europa.eu/pdf/en/11/st11/st11447.en11.pdf.

Figure 1. The EU approach to cyber-security



Following the approach of the EU, the general objective of the initiatives in the cyber domain is Network and Information Security (NIS), defined by the Strategy for a Secure Information Society as "*the ability of a network or an information system to resist (…) accidental events or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data (…)*".[8]

The CIIP is certainly crucial to this end as it consists of "the activities of infrastructure owners and operators to ensure the performance of critical information infrastructures [namely ICT systems that are critical infrastructures for themselves or that are essential for the operation of other critical infrastructures] in case of failures, attacks or accidents above a defined minimum level of services."[9]

With respect to cyber-crime, there is not yet a univocal definition across the EU, mainly due to Member States' different domestic legislations.[10] However, in a 2007 communication, the Commission defined it as all "criminal acts committed using electronic communications networks and information systems or against such networks

[8] Commission of the European Communities, *A Strategy for a Secure Information Society - 'Dialogue, partnership and empowerment'* (COM(2006) 551 final), Brussels, 31 May 2006, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0251:FIN:EN:PDF, p. 3.

[9] Commission of the European Communities, *Green Paper on a European Programme for Critical Infrastructures Protection* (COM(2005) 576 final), Brussels, 17 November 2005, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0576:FIN:EN:PDF. The process of identifying European Critical Infrastructures launched with the Council Directive 2008/114 has focused so far on the energy and transport sectors. However, ICT will be the next priority.

[10] Europol-High Tech Crime Centre, *High Tech Crimes within the EU: Old Crimes New Tools, New Crimes New Tools. Threat Assessment 2007*, The Hague, 2007, http://57.67.199.6/publications/Serious_Crime_Overviews/HTCThreatAssessment2007.pdf. This issue is also raised by the International Telecommunication Union (ITU), which nevertheless observes that "[t]he fact that there is no single definition of 'cyber-crime' need not be important, as long as the term is not used as a legal term". International Telecommunication Union (ITU), *Understanding Cybercrime: A Guide for Developing Countries*, Geneva, April 2009, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf.

and systems."[11] Using quite an extensive approach, it further specifies three main categories: i) traditional forms of crime such as fraud and forgery, although in a cyber-crime context; ii) the publication of illegal content over electronic media; iii) crimes unique to electronic networks, namely cyber-attacks against information system, denial of service and hacking.

One should point out that some more detailed examples of attacks against information systems are contained in the 2005 Framework Decision of the Council of the European Union (the updating of which is currently being worked on[12]). It does not however distinguish between small- and large-scale cyber-attacks, and does not consider as a priority attacks against CIIs, which themselves are not distinguished from ordinary information systems.[13]

Still in the Community context and the case of cyber-crime, Article 83 TFEU features among the existing possibilities for a greater degree of harmonisation of definitions, providing that "*[*t]he European Parliament and the Council may, by means of directives adopted in accordance with the ordinary legislative procedure, establish minimum rules concerning the definition of criminal offences and sanctions in the areas of particularly serious crime with a cross-border dimension (…)", including also "computer crime".[14]

At the international level, an initiative worthy of note for the purposes of greater clarity and rationalisation in the field of cyber-crime is the Convention on Cybercrime of the Council of Europe (2001),[15] from which EU initiatives in the sector have drawn inspiration, such as the Council Framework Decision. Interestingly, the US is also party to the Convention. Ratification by several European countries is however awaited, as well as by all third countries (not Member States of the Council of Europe), with the exception of the US.[16]

Against this background, the general impression received is that often, with rare exceptions of legal instruments which are binding on a greater or lesser number of States, the definitions of the sectors of activity of cyber-security contained in these documents are in reality valid only and exclusively in relation to a specific field of application and for a specific normative system. The problem is particularly acute in relation to cyber-crime, whose numerous manifestations, though regulated, risk being understood differently at EU level (for example between certain of its agencies, such as

[11] Commission of the European Communities, *Towards a general policy on the fight against cyber crime* (COM(2007) 267 final), Brussels, 22 May 2007, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF, p. 2.
[12] Council of the European Union, *Proposal for a Directive of the European Parliament and of the Council on Attacks against Information Systems, replacing Council Framework Decision 2005/222/JHA* (10751/11), Brussels, 30 May 2011, http://register.consilium.europa.eu/pdf/en/11/st10/st10751.en11.pdf.
[13] Estonian Ministry of Defence, *Cyber Security Strategy*, Tallinn, 2008, http://www.mod.gov.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf, p. 18.
[14] European Union, *Treaty on the Functioning of the European Union*, consolidated version, Official Journal of the European Union, C 83/47, 30 March 2010, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0047:0200:EN:PDF.
[15] Council of Europe, *Convention on Cybercrime*, Budapest, 23 November 2001, http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm.
[16] For the state of play on the ratification of the Convention, see the Council of Europe website: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG.

Europol, which for example technically prefers the term and concept of "internet facilitated (organised) crime"[17]) and between the 27 Member States.

2. Risks and criticality of semantic ambiguities

In the opinion of some, the problem of definitions might seem a non-problem on the basis of the fact that, notwithstanding that those definitions are neither univocal nor uniform, initiatives and means of implementation for the management of the sector, including from the normative point of view, exist. At this point indeed we would like to stress that the question is one of means of implementation that could be more efficient and effective if they could be based on sure definitions harmonised at the international level, given that one is dealing with a transnational domain that therefore requires transnational answers.

It is in fact easily noticeable that terms such as cyber-security, cyber-crime, cyber-terrorism, cyber-sabotage, cyber-espionage, cyber-defence, cyber-attack, cyber-war, information warfare and so on continue to be cited and used in very many contexts in an ambiguous way, even by experts. Authoritative analyses in the world of research make this point, as expressed in a Chatham House report in which it is argued that cyber-security is a problem of an ill-defined nature, which too often is the result of an unhappy "combination of intuition and uncertainty (mixed with pessimism)" (!). This fundamental irrationality, which characterises the perception of cyber-security, contributes to the fact that analyses of evaluation of the threat are concentrated almost exclusively on events of great show but low probability, thereby diverting significant resources away from the management of more ordinary, but also more urgent, problems.[18]

The issue is also raised at the institutional level, as in the framework of the "Multinational Experiment 7 - Access to the Global Commons" sponsored by US JFCOM - J9, which, over the period 2011-12, will bring together various nations, among them European, with the concern among others of the question of "terminology/taxonomy in the Cyber Domain". This is indeed indicative, if one considers that the military environment is by definition considered to have a much more advanced level of terminological and definitional standardisation than the civilian.

It is therefore the case that from a lack of definitiveness and above all a lack of harmonisation of definitions problems of inefficiency, if not of ineffectiveness, can derive at a number of levels, including the following:

- Misleading risk assessment. As observed above in the Chatham House report, uncertainty as to the actual reach of cyber-threats favours perceptions, approaches

[17] See for instance Europol, *Threat Assessment on Internet Facilitated Organised Crime (iOCTA)*, The Hague, 7 January 2011, https://www.europol.europa.eu/sites/default/files/publications/iocta.pdf. The report uses both the terms "cyber-crime" and "internet facilitated organised crime", apparently interchangeably. The latter appears to have a predominantly technical meaning akin to "expert", and enters into the merits of which party might be guilty of a cyber-crime.

[18] Paul Cornish, Rex Hughes and David Livingstone, *Cyberspace and the National Security of the United Kingdom. Threats and Responses*, London, Chatham House, March 2009 (A Chatham House Report), http://www.chathamhouse.org/publications/papers/view/109020, p. 1.

and countermeasures based on the worst-case scenario. The risk is that resources are disproportionately allocated to events with potentially serious consequences but which are unlikely to occur, neglecting more frequently recurring problems which have a greater and direct impact on the well-being of citizens. Here we are referring to the real quantitative and social preponderance of cyber-crime, for example in the diffuse forms of telematic banking fraud and industrial espionage. Even in the case of the support given to the drafting of an initial *Trattato per il contrasto alle minacce cibernetiche statali* (Treaty against State cyber-threats),[19] it should be noted that, if on the one hand such a project has the merit of filling a normative gap, it does not, as has been seen, correspond to a preponderant problem and, in the opinion of some creditable commentators, could today have a limited impact: "A treaty, particularly an arms control treaty, makes little sense. What is a weapon in cyberspace? A child with some programming knowledge and a laptop can build and launch an attack in few weeks. Verification is impossible. A treaty based on technological constraints would be meaningless. Nor would a treaty that excludes certain targets from cyber-attacks make sense. Existing laws of war already define safeguards and limitations (but do not ban) attacks on civilian targets. We cannot expect more for cyberspace".[20]

- An absence of references to certain categories, and a lack of harmonisation of definitions, with possible normative and political deadlocks. Cyber-war[21] is on the one hand vaguely and ambiguously mentioned in, or completely absent from, official EU documents, but on the other highly developed in the strategies and doctrines of the US, various nation States - each according to its own structure - and in the NATO context. It is indeed on the common ground of NATO that impasses due to the differing approaches to cyber-war have arisen: an example of this is the debate over whether or not to recognise large-scale cyber-attacks[22] such as those perpetrated against Estonia in 2007 and Georgia in 2008 as cases falling within the scope of Articles 4 and 5 of the Treaty of Washington. The question turns in fact on the "nature of the attacks" and the consequent "political evaluation", which must judge them as being relevant in order to activate the collective defence clause foreseen by the Atlantic Alliance. The issue was raised in the recommendations of the 2010 report of the group of experts, with a view to the updating of NATO strategic concept, in the following terms [italics added]: "*Cyber*

[19] As suggested for Italy by the Parliamentary Committee on the Security of the Republic: Comitato parlamentare per la sicurezza della Repubblica (COPASIR), *Relazione sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dallo spazio cibernetico*, Roma, Camera dei Deputati/Senato della Repubblica, luglio 2010 (DOC. XXXIV, N. 4), http://www.parlamento.it/service/PDF/PDFServer/DF/234494.pdf, p. 85.

[20] James A. Lewis, *The international Context for Cybersecurity*, paper presented at the Session on Cybersecurity, Annual Meeting of the Trilateral Commission, Washington, 8-10 April 2011.

[21] Not to be confused, it might not be useless to add, with electronic war, a military activity which uses the electromagnetic spectrum (made up of all possible frequencies of electromagnetic radiation, from radio waves to gamma rays) for attack, defence or observation (or the acquisition of information).

[22] Carried out in both cases in the form of a DDoS (Distributed Denial of Service). In Georgia the attacks had started in the weeks preceding the physical armed Russian attack for control of South Ossetia and Abkhazia. In the words of the Georgian ambassador to NATO, Grigol Mgaloblishvili, his country "had come under a cyber-attack coordinated with land, air and sea operations during the 2008 war with Russia, which disrupted banking and communications at a crucial time in the conflict". Security & Defence Agenda (SDA), *Cyber Security: A Transatlantic Perspective*, Brussels, April 2010, http://www.securitydefenceagenda.org/Portals/14/Documents/Publications/2010/Report_Cybersecurity_Final.pdf.

defence capabilities. The next significant attack on the Alliance may well come down a fibre optic cable. Already, *cyber attacks against NATO systems* occur frequently, but most often below the *threshold of political concern*. However, the risk of a *large-scale attack on NATO's command and control systems or energy grids* could readily warrant consultations under Article 4 and could possibly lead to collective defence measures under Article 5".[23] We have therefore "*cyber defence*", "*large-scale attacks*" against "*NATO systems*" or "*energy grids*", and the crossing of the "*threshold of political concern*", which the new strategic concept takes up and elaborates [italics added]: "[c]yber attacks are becoming more frequent, more organised and more costly in the damage that they inflict *on government administrations, businesses, economies and potentially also transportation and supply networks and other critical infrastructure; they can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability*. Foreign militaries and intelligence services, organised criminals, terrorist and/or extremist groups can each be the source of such attacks".[24] In the above references one cannot see any progress towards order on the key question of the threshold of political concern required to threaten national and Euro-Atlantic prosperity, security and stability, nor on that of which cyber-events would activate the collective defence clause. Articles 4 and 5 were not able to play a role in the cases of Estonia and Georgia, differently from the case of 11 September, which obviously did not require a harmonisation of interpretations in order to determine which were the relevant categories and the threshold of political concern which meant that it was comparable to an armed attack. The lack of harmonisation of substance regarding cyber-war has been confirmed also by a recent joint US-Russia study published by the EastWest Institute, which argues for a process to render the Geneva and Hague Conventions applicable to cyberspace. Beyond the effectiveness of such an approach,[25] the point to note is that, among the obstacles to their application, is that related to the fact that there is no clearly and internationally-shared definition of what constitutes a cyber-war [italics added]: "In fact, *there is considerable confusion. Senior government leaders from the same country have incompatible opinions about the most basic aspects of cyber war* - its existence now, its reality or likely impact in the future. *The current ambiguity is impeding policy development and clouding the application of existing Convention requirements. (…) national security stakeholders to acknowledge that the current uncertainty about the definition for cyber-war is unacceptable*. In addition, Russia, the U.S., and other interested parties, must *explore new frameworks to categorize conflict (…)*".[26]

- The previous point has its context in, and also a consequence for, the debated question of whether or not it is necessary to update or otherwise certain categorisations of public international law. If indeed one considers situations in which there is a potential hostile involvement on the part of States, it becomes necessary to study which conditions would require the movement from internal

[23] NATO, *NATO 2020: Assured Security; Dynamic Engagement. Analysis and Recommendations of the Group of Experts on a New Strategic Concept for NATO*, 17 May 2010, http://www.nato.int/strategic-concept/expertsreport.pdf.
[24] NATO, *Strategic Concept 2010*, http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf.
[25] See footnote 20.
[26] Karl Frederick Rauscher and Andrey Korotkov, *Working Towards Rules for Governing Cyber Conflict. Rendering the Geneva and Hague Conventions in Cyberspace*, New York, EastWest Institute, January 2011, http://www.ewi.info/working-towards-rules-governing-cyber-conflict.

security to the application of the law of war. It is the traditional categories of public international law (sovereignty, extraterritoriality) which are put into question, with a view to an as yet uncertain adaptation to cyberspace, an adaptation in which sovereignty cannot be tied to territoriality, but could usefully be so to the different "functions" which are carried out in cyberspace. In other words, it is a question of "functional cyber-borders", classified on the basis of the types of activity carried out in cyberspace: functional sovereignty and functional jurisdiction, for which however the possibilities of control and coercion appear uncertain. The questions in search of an answer are various, and concern not only the political-strategic evaluation of an attack, but also and above all *the placing in a legal context of the aspects which put into question the traditional boundary between internal and external security and between military and civilian competences*. For example, when is a civilian response more appropriate than a military response, and vice versa? In the case in which a State does not carry out an attack itself, but tacitly gives a private operator the authorisation to proceed, is the State in question legally liable for the acts of its citizens who believe that they are acting in its place? The question of attribution of legal liability is key in a context in which the origin of attacks might not be certain. And as concerns the need to update or otherwise certain categorisations of public international law and to answer the questions set out above, again there is no clear international consensus. On the contrary, while in different fora it has been more than open,[27] the latest official position of the US is that "[t]he development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete".[28]

- Problems can also arise concerning the attribution of legal regime and of competence. If we take as an example the category of cyber-attacks against information systems/DDoS, we can say for sure that these fall within the category of Network and Information Security (NIS)/cyber-crime, as understood at EU level, but also that they potentially fall within the category of cyber-war (constituting as they do, as we have seen, a potential means of cyber-war among those used to date, and on which the debate is open). This can lead to overlaps of legal regime (security/internal law? external security/international law?) and of competent authority, which can cause inefficiency in management (duplication, wasting of resources) and implementation/countermeasures (including law enforcement).
- Overlaps of regime and competence, originating precisely *inter alia* from insecurity of definitions. Let us take the case of the European Network and Information Security Agency (ENISA). From its conception in 2004, the Agency has been responsible for NIS, with a set-up limited to ensuring economic and commercial continuity with the aim of facilitating the functioning of the internal market. This

[27] See *G8 Declaration: Renewed commitment for freedom and democracy*, Deauville, 26-27 May 2011, http://www.g20-g8.com/g8-g20/root/bank/print/1314.htm: [italics added]: "Governments have a role to play, informed by a full range of stakeholders, in helping to *develop norms of behaviour and common approaches in the use of cyberspace*." And the European Union External Action Service (EEAS) [italics added]: "introduced its recent efforts, notably with the US, India and China, to build a global compact to strengthen cyber-security and emphasised the desirability of *developing international rules and norms for cyberspace*." Hungarian Presidency of the Council of the European Union, *Closer cooperation in EU security policy*, 1 June 2011, http://www.eu2011.hu/news/closer-cooperation-eu-security-policy.

[28] See White House, *International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World*, Washington, May 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf, p. 9.

continuity concerns public and private infrastructures (and related services), i.e. functions which have a direct impact on citizens. By ensuring the economic and commercial continuity of such infrastructures, there is a positive indirect effect on citizens demonstrating the synergies between the twin economic and social dimensions of NIS, which therefore functions de facto without the need for everything to be placed in a normative framework. In other cases, instead, the European Union is rightly thinking to recognise overlaps and to regulate them formally in order to put certain policies into effect in the best way possible: the mandate of ENISA, which originally did not extend to cyber-crime and cyber-terrorism (for which in principle the Member States and Europol are responsible), is indeed supposed to be widened to include NIS-related aspects of the fight against cyber-crime.[29]

3. A way forward

The aim of this analysis has been to show that the existence of problems of definition, and above all of harmonisation of definitions, brings inefficiencies to various aspects of the management of the cyber sector, in particular normative production, countermeasures and law enforcement.

The harmonisation processes are complex, and there are no univocal and exhaustive indications as regards the ways to achieve it: it is however necessary that they involve all relevant stakeholders in the political-institutional and technical-operative fields.

As has been seen, harmonisation problems are present in an accentuated way in the framework of the EU, above all as a result of the presence of 27 cultural, legal and operative cultures which can differ greatly between themselves. It is well at this juncture to recall that the more significant responsibilities in the cyber sector, including questions of definition, rest with the Member States. The EU only intervenes in a subsidiary manner with its usual value-added in the governance - mainly directed at coordinating and harmonising national initiatives - of transnational sectors, such as, in the present case, the cyber sector. The EU has to date put into action various initiatives in the cyber sector, with particular attention being paid to cyber-crime and CIIP.

[29] Commission of the European Communities, *Proposal for a Regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA)* (COM(2010) 521 final), Brussels, 30 September 2010, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0521:FIN:EN:PDF. European Commission, *Digital Agenda: Commission proposal to strengthen and modernise European Network and Information Security Agency (ENISA) - frequently asked questions* (MEMO/10/459), 30 September 2010, http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/459: "One of the elements of the proposal is that ENISA will act as an interface between cyber-security experts and public authorities involved in the fight against cyber-crime. By bringing together law enforcers, the judiciary and privacy protection authorities, network and information security aspects of the fight against cyber-crime will be better co-ordinated." In June 2011, the Agency's mandate was extended until 2013, with the express intention of holding a debate on its reform: European Union, *Regulation (EU) No 580/2011 of the European Parliament and of the Council of 8 June 2011 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration*, Official Journal of the European Union, L 165/3, 24 June 2011, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:165:0003:0004:EN:PDF.

Measures are aimed principally at improving the EU's capacity to respond to cyber-attacks, but which aim also at providing a contribution to the process of harmonization of definitions (as provided, as we have seen, by Article 83 TFEU, and by the Council Framework Decision in the field of computer crime[30]).

A test in the near future will be the enactment of the directive on European critical infrastructures, and in particular the clarification of what actually falls within the categories of ICT set out in the directive,[31] which as is known constitute the next sector of its application. The operation will not be simple: in various opinions, including institutional opinions, it is today still difficult at the European level to come up with a shared definition not only of a European critical infrastructure, but even of an infrastructure itself (!).

The road to clarification of categories is therefore rather long, in particular for the EU, and should be embarked upon with urgency: if the categorisations are not clear and shared at EU level, how can one demand an effort at harmonisation of legal categories between Member States and with third countries? With reference to the latter, one can even see in fact the opposite: according to Europol, the preponderance of US sources is influencing the European perspective.

Cooperation on the political-institutional front must therefore be strengthened, including at the transatlantic and international levels, given the transnational and global nature of the cyber sector, with a view *inter alia* to the strengthening and improvement of existing instruments.

The progress in EU-US relations signalled by the most recent annual summits can be a good example: in 2009, "cyber-security" was recognised for the first time as a global challenge (not bilateral, nor regional), thus expressing a common intention to "identify and prioritize" areas of cooperation in the sector.[32] But do permanent dedicated contact points at appropriate levels of government exist? The 2010 summit moved in this direction with the establishment of an EU-US working group on cyber-security and cyber-crime. Its tasks include improving response capacities to cyber-incidents, with a view to a common exercise to be held by the end of 2011; intensifying the involvement of the private sector, exchanging good practices and concentrating commitment on specific sectors, such as the fight against botnets, rendering industrial plants secure and improving internet resilience; carrying out joint awareness activities, in particular with themes such as child pornography; and supporting the Convention on Cybercrime

[30] Council of the European Union, *Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems*, Official Journal of the European Union, L 69/67, 16 March 2005, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:069:0067:0071:EN:PDF.

[31] Commission of the European Communities, *Green Paper on a European Programme for Critical Infrastructures Protection*, *cit*., Annex II: "The ICT sector includes information systems and network protection; instrumentation automation and control systems (SCADA); the internet; the provision of fixed telecommunications; the provision of mobile telecommunications; radio communication and navigation; satellite communication; and broadcasting."

[32] *EU-U.S. Summit Declaration*, Washington, 3 November 2009, http://eeas.europa.eu/us/sum11_09/docs/declaration_en.pdf.

of the Council of Europe, including by increasing the number of States party to it.[33] Evaluation of its real effectiveness will take time. Even its name, which implies a distinction between cyber-security and cyber-crime as two different fields of activity, could raise certain questions which, it is hoped, will have been clarified by the time the working group reports on its results at the 2011 summit. This instrument could also become key for the task of harmonisation (through a specification in its mandate), and it appears opportune also to consider the creation of a "US-EU Cyber-security Council", on the model of the US-EU Energy Council already established at ministerial level in the same institutional context, for the advantage of permanent political-institutional attention.

Permanent consultation initiatives regarding cyber-security, similar to the transatlantic initiative, should involve other relevant partners, such as Russia and China, for example by creating analogous working groups in the context of the partnerships which the EU has with those countries.

In the context of harmonisation of definitions, there is more than one road which could be taken. As far as cyber-crime is concerned, a broader application of the Convention on Cybercrime of the Council of Europe, which currently remains the only legal instrument in force at international level, should certainly be encouraged, in line with the recommendations of US International Strategy for Cyberspace and the tasks of the EU-US working group on cyber-security and cyber-crime. Even today, however, the ratification of various signatories, among both Member States of the Council of Europe and third countries, is still awaited. Furthermore, States such as Russia, China, India and Brazil are not party to the Convention, and it is improbable that these countries will decide to cooperate in the absence of clear agreements on military and political questions regarding cyberspace. It is inevitable that this will have a negative impact on the real effectiveness and international reach of the Convention.

It is moreover important to continue to promote dialogue on the subject also at the level of the United Nations and in particular in the context of the ITU (whose partners are both States and private entities, such as for example Microsoft, Cisco Systems, Intel Cooperation and many other companies of large, medium and small sizes from various countries around the world). From 2007 onwards, with the Global Cyber-security Agenda[34] and other complementary initiatives,[35] the ITU has tried to establish itself as a building-block for the encouragement of dialogue between States and public-private entities with a view to the creation and development of common legal and operational standards, above all in the cyber-crime sector.

[33] European Commission, *Cyber security: EU and US strengthen transatlantic cooperation in face of mounting global cyber-security and cyber-crime threats* (MEMO/11/246), Brussels, 14 April 2011, http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/246.
[34] ITU, *Global Cyber-security Agenda*, http://www.itu.int/osg/csd/cybersecurity/gca/index.html.
[35] See for example the International Multilateral Partnership Against Cyber Threats (IMPACT), which initialed a memorandum of understanding with the ITU in 2008 and which is a "public-private international initiative" which aims at improving the international community's capacities of prevention, defence and response to cyber-attacks; within the ITU, there is the Global Response Centre (GRC), which aspires to becoming the world's principal resource centre against cyber-threats, and the ITU Cybersecurity Gateway, a platform for exchanges of information between interested parties in civil society, the private sector and government and international organisations active in cyber-security, http://groups.itu.int/Default.aspx?tabid=841.

At the technical-operative level, attention should be given to Computer Emergency Resource Teams (CERTs), groups of experts which intervene in the case of cyber-incidents and which have the added value of bringing together private and public actors. CERTs seem to have a greater degree of harmonisation of categories than that seen at the political-institutional level. In this sense one could assess the opportunity of strengthening their role in various ways, thus reinforcing the "bottom up" push that this more technical-operative level can give to the creation of shared categories and policies:

- by supporting the harmonisation and raising of the standards of CERTs in Europe and the creation of a network of all national CERTs and the CERTs of the European institutions by 2012, with the gradual creation of an EU-centric governance of CERTs under the responsibility of ENISA;[36]
- by increasing and making permanent the exchanges between European CERTs and non-European (e.g. US-CERT) CERTs, with the sharing of lessons learned;
- by emphasising the experience of the few regional and international CERTs (it should be borne in mind that almost all CERTs are on a national basis, and that the EU CERT is not yet established). In particular, the case of the Forum of Incident Response and Security Teams (FIRST), which has among its objectives information sharing and the spreading of best practices, can be an example of a methodology to be used for harmonisation.

Finally, in all the possible above-mentioned initiatives, a strong involvement of private actors, the home of research and development in the ICT sector and the owners and/or principal operators and/or managers of the security of infrastructures, should always be considered. For these reasons, it is necessary to put in place appropriate public-private partnerships and to overcome - through financial incentives, dedicated research funds and appropriate normative frameworks - a mere tactical vision of commercial "business continuity" so as to take a place in a wider architecture which has as its aim ensuring the protection of the security of the State and of the citizen.

Updated: 29 July 2011

[36] ENISA supports the creation of an EU CERT to manage those ICT threats that concern the Union. CERTs are at the basis of the European Information Sharing and Alert System (EISAS) which ENISA plans to develop by 2013. See Commission of the European Communities, *Critical Information Infrastructure Protection - 'Achievements and next steps: towards global cyber-security'* (COM(2011) 163 final), Brussels, 31 March 2011, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:EN:PDF.

References

Books and Articles

Paul Cornish, Rex Hughes and David Livingstone, *Cyberspace and the National Security of the United Kingdom. Threats and Responses*, London, Chatham House, March 2009 (A Chatham House Report), http://www.chathamhouse.org/publications/papers/view/109020.

Federica Di Camillo and Valérie Miranda, "Cybersecurity: Toward EU-U.S. Cooperation?", in IAI, UI, FRS, CSIS, *EU-U.S. Security Strategies. Comparative scenarios and recommendations*, Washington, Center for Strategic and International Studies, April 2011, p. 55-67, http://www.iai.it/content.asp?langid=2&contentid=+599.

International Telecommunication Union (ITU), *Understanding Cybercrime: A Guide for Developing Countries*, Geneva, April 2009, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf.

James A. Lewis, *Thresholds for Cyberwar*, Washington, Center for Strategic and International Studies (CSIS), 1 October 2010, http://csis.org/publication/thresholds-cyberwar.

Karl Frederick Rauscher and Andrey Korotkov, *Working Towards Rules for Governing Cyber Conflict. Rendering the Geneva and Hague Conventions in Cyberspace*, New York, EastWest Institute, January 2011, http://www.ewi.info/working-towards-rules-governing-cyber-conflict.

Security & Defence Agenda (SDA), *Cyber Security: A Transatlantic Perspective*, Brussels, April 2010, http://www.securitydefenceagenda.org/Portals/14/Documents/Publications/2010/Report_Cybersecurity_Final.pdf.

Stein Schjolberg, *An International Criminal Court or Tribunal for Cyberspace (ICTC)*, A paper for the EastWest Institute (EWI) Cybercrime Legal Working Group, May 2011, http://www.cybercrimelaw.net/documents/International_Criminal_Court_or_Tribunal_for_Cyberspace_(ICTC).pdf.

Eneken Tikk, "Ten Rules for Cyber Security", in *Survival*, Vol. 53, No. 3, (June-July 2011), p. 119-132, http://www.ccdcoe.org/articles/2011/Tikk_TenRulesForCyberSecurity.pdf.

Documents

1. European Union

Commission of the European Communities, *Critical Information Infrastructure Protection - 'Achievements and next steps: towards global cyber-security'* (COM(2011)

163 final), Brussels, 31 March 2011, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:EN:PDF.

Commission of the European Communities, *The EU Internal Security Strategy in Action: Five steps towards a more secure Europe* (COM(2010) 673 final), Brussels, 22 November 2010, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:EN:PDF.

Commission of the European Communities, *Green Paper on a European Programme for Critical Infrastructures Protection* (COM(2005) 576 final), Brussels, 17 November 2005, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0576:FIN:EN:PDF.

Commission of the European Communities, *Proposal for a Regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA)* (COM(2010) 521 final), Brussels, 30 September 2010, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0521:FIN:EN:PDF.

Commission of the European Communities, *A Strategy for a Secure Information Society - 'Dialogue, partnership and empowerment'* (COM(2006) 551 final), Brussels, 31 May 2006, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0251:FIN:EN:PDF.

Commission of the European Communities, *Towards a general policy on the fight against cyber crime* (COM(2007) 267 final), Brussels, 22 May 2007, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF.

Council of the European Union, *Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems*, Official Journal of the European Union, L 69/67, 16 March 2005, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32005F0222:EN:NOT.

Council of the European Union, *18 month programme of the Council (1 July 2011-31 December 2012)* (11447/11), Brussels, 17 June 2011, http://register.consilium.europa.eu/pdf/en/11/st11/st11447.en11.pdf.

Council of the European Union, *Internal Security Strategy for the European Union: 'Towards a European Security Model'* (5842/2/10 REV 2), Brussels, 25 February 2010, http://register.consilium.europa.eu/pdf/en/10/st05/st05842-re02.en10.pdf.

Council of the European Union, *Proposal for a Directive of the European Parliament and of the Council on Attacks against Information Systems, replacing Council Framework Decision 2005/222/JHA* (10751/11), Brussels, 30 May 2011, http://register.consilium.europa.eu/pdf/en/11/st10/st10751.en11.pdf.

Council of the European Union, *Report on the Implementation of the European Security Strategy - Providing Security in a Changing World* (S407/08), Brussels, 11 December 2008,

http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/EN/reports/104630.pdf.

Council of the European Union, *A Secure Europe in a Better World. European Security Strategy*, Brussels, 12 December 2003, http://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf.

Council of the European Union, *Statement on tighter international security* (16751/08), Brussels, 3 December 2008, http://register.consilium.europa.eu/pdf/en/08/st16/st16751.en08.pdf.

European Union, *Regulation (EU) No 580/2011 of the European Parliament and of the Council of 8 June 2011 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration*, Official Journal of the European Union, L 165/3, 24 June 2011, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:165:0003:0004:EN:PDF.

European Union, *Treaty on the Functioning of the European Union*, consolidated version, Official Journal of the European Union, C 83/47, 30 March 2010, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0047:0200:EN:PDF.

Europol, *Threat Assessment on Internet Facilitated Organised Crime (iOCTA)*, The Hague, 7 January 2011, https://www.europol.europa.eu/sites/default/files/publications/iocta.pdf.

Europol-High Tech Crime Centre, *High Tech Crimes within the EU: Old Crimes New Tools, New Crimes New Tools. Threat Assessment 2007,* The Hague, 2007, http://57.67.199.6/publications/Serious_Crime_Overviews/HTCThreatAssessment2007.pdf.

Hungarian Presidency of the Council of the European Union, *Closer cooperation in EU security policy*, 1 June 2011, http://www.eu2011.hu/news/closer-cooperation-eu-security-policy.

Hungarian Presidency of the Council of the European Union, *Cyberspace could also be war theatre*, 4 May 2011, http://www.eu2011.hu/news/cyberspace-could-also-be-war-theatre.

2. Others

Comitato parlamentare per la sicurezza della Repubblica (COPASIR), *Relazione sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dallo spazio cibernetico*, Roma, Camera dei Deputati/Senato della Repubblica, luglio 2010 (DOC. XXXIV, N. 4), http://www.parlamento.it/service/PDF/PDFServer/DF/234494.pdf.

Council of Europe, *Convention on Cybercrime*, Budapest, 23 November 2001, http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm.

Estonian Ministry of Defence-Cyber Security Strategy Committee, *Cyber Security Strategy*, Tallinn, 2008, http://www.mod.gov.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf.

G8, *G8 Declaration: Renewed commitment for freedom and democracy*, Deauville, 26-27 May 2011, http://www.g20-g8.com/g8-g20/root/bank/print/1314.htm.

NATO, *NATO 2020: Assured Security; Dynamic Engagement. Analysis and Recommendations of the Group of Experts on a New Strategic Concept for NATO*, 17 May 2010, http://www.nato.int/strategic-concept/expertsreport.pdf.

NATO, *Strategic Concept 2010*, http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf.

US Department of Defense, *Quadrennial Defense Review Report*, Washington, February 2010, http://www.defense.gov/qdr/images/QDR_as_of_12Feb10_1000.pdf.

US Department of Homeland Security, *Quadrennial Homeland Security Review Report, A Strategic Framework for a Secure Homeland*, Washington, February 2010, http://www.dhs.gov/xlibrary/assets/qhsr_report.pdf.

White House, *International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World*, Washington, May 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

White House, *National Security Strategy*, Washington, May 2010, http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

Istituto Affari Internazionali

Latest IAI Working Papers

11 | 25 N. Mikhelidze, The 2012 Presidential Elections in Russia: What Future for the Medvedev-Putin Tandem?

11 | 24 S. Felician, North and South Korea: A Frozen Conflict on the Verge of Unfreezing?

11 | 23 M. Comelli and R. Matarazzo, Rehashed Commission Delegations or Real Embassies? EU Delegations Post-Lisbon

11 | 22 A. Veclani, N. Sartori and R. Rosanelli, The Challenges for European Policy on Access to Space

11 | 21 P. Droz-Vincent, A Return of Armies to the Forefront of Arab Politics?

11 | 20 M. Haubrich Seco, Decoupling Trade from Politics: The EU and Region-Building in the Andes

11 | 19 N. Koenig, The EU and the Libyan Crisis: In Quest of Coherence?

11 | 18 M. Fiore, Israel and Iran's Nuclear Weapon Programme: Roll Back or Containment?

11 | 17 R. Balfour and H. Ojanen, Does the European External Action Service Represent a Model for the Challenges of Global Diplomacy?

11 | 16 K. Oksamytna, The European Union Training Mission in Somalia: Lessons Learnt for EU Security Sector Reform

11 | 15 E. Gross and A. Rotta, The EEAS and the Western Balkans

11 | 14 M. Garavoglia, Democracy in Europe: Politicizing Champions for the European Public Sphere

Istituto Affari Internazionali
Via Angelo Brunetti, 9 00186 Roma
Tel.: +39/06/3224360 Fax: + 39/06/3224363
E-mail: **iai@iai.it** - website: **http://www.iai.it**
Send orders to: **iai_library@iai.it**

The Institute

The Istituto Affari Internazionali (IAI), founded by Altiero Spinelli in 1965, does research in the fields of foreign policy, political economy and international security. A non-profit organisation, the IAI aims to further and disseminate knowledge through research studies, conferences and publications. To that end, it cooperates with other research institutes, universities and foundations in Italy and abroad and is a member of various international networks. More specifically, the main research sectors are: European institutions and policies; Italian foreign policy; trends in the global economy and internationalisation processes in Italy; the Mediterranean and the Middle East; defence economy and policy; and transatlantic relations.
The IAI publishes an English-language quarterly (The International Spectator), an online webzine (AffarInternazionali), two series of research papers (IAI Quaderni and IAI Research Papers) and an Italian foreign policy yearbook (La politica estera dell'Italia).