An Overview of Current International Cyber Affairs: Processes, Agendas and Instruments

Prepared for the Swiss Ministry of Foreign Affairs

by

Eneken Tikk-Ringas, Senior Advisor, ICT4Peace Foundation

Geneva-Tallinn 2012

Draft 1.0 (24 September 2012)

Contents

Introduction

The objective of this study is to provide an overview of key actors, past and on-going international and regional processes and instruments related to the international governance of cyber security for the purpose of facilitating the engagement by the Swiss Federal Department of Foreign Affairs (FDFA) with other governments and international actors in the field.

The study will first outline the notion of 'cyber security', for the purposes of framing and explaining the scope and logic of the rest of this study. It will then provide a summary of key actors, processes and instruments involved in enhancing global and national cyber security and summarize the status quo of international cyber affairs.

I The notion of "cyber security"

Understanding the notions 'cyber' and 'security' is crucial for setting and weighing priorities and perspectives in current global and regional affairs that, very generally, are related to the uses of information and communication technologies (ICTs). Both words are ambiguous in that they carry a widely acknowledged popular meaning and are additionally established as terms of art in more than one field of expertise. Therefore, while appearing to promise a basis for broad consensus and agenda, both terms may not mean the same thing to different actors and, depending on the context, even have no precise meaning at all.

The following observations are intended to facilitate getting oriented in contemporary multilateral 'cyber security' agendas and processes:

1. **The notion of 'cyber security' combines the concepts of technical security and national security.** In conjunction with (especially the adverse) consequences of uses of ICTs in the society by individual users, industries and governments the term 'cyber' has over the past five to seven years been widely adopted to reflect national interests and national security and international peace and security concerns.

   In technical computer security studies the notion of 'security' is generally translated into the confidentiality, integrity and availability of data (or information or services). National security serves the fundamental and persistent interests of a nation that are expected to rise above the narrow and special interests of parts of the nation and stay below the concern of 'interests of all mankind'. As such, national security is related to the exercise of 'national power' and sovereignty and its remedies often go as alternatives to principles and policies governing the same topic until they fall within the particular scope of interest.

The term 'security' has been used as a term of art in both technical (computer and network security) and international relations and policy (national security, international peace and security) studies. Whereas the term is generally understood as the state of being secure from danger of attack, the scope and methods of achieving such a state are inherently different for the purposes of technical computer security (exercise of technical expertise) and national security (exercise of national authority).

In practice, most of the measures for achieving a condition where ICT-related vulnerabilities and risks to the society and individuals would be minimized and mitigated are those of technical computer and network security. Dunn distinguishes between four perspectives of 'cyber security': cyber security as an IT security issue, an economic issue, a law enforcement issue or a national security issue.[1] Today, 'cyber security' also constitutes (at least potentially) an international peace and security issue.

The term 'cyber security' as used in most international processes is indistinctive of the two disciplines embedded and therefore can appear in different contexts and not have the same meaning for experts and officials depending their area of expertise.

The technical community has historically not used the term 'cyber' as a term of art because of its indistinctiveness. With the rise of national and international 'cyber' security paradigm, however, computer and network security disciplines have been engaged in the process, often without a constructive outcome due to (still) differing understanding of the scope and essence of the issues and, consequently, remedies.

2. The 'issues of cyber security' cover a wide area of activities and functions.

'Cyber security', for the purposes of this paper generally understood as a set of national security and international peace and security relevant uses and implications of ICTs is a comprehensive concept that has evolved over the past few decades.

For years, the primary interests related to the development of an information society were defined by the expectations of economic growth and therefore adjusted to the needs of consumers, e-commerce and Internet Service Providers. With an increase of overall dependence of industries and governance on ICTs accompanied by the incentives and attempts to exploit the vulnerabilities in such systems and processes computer and network security has undergone securitization on a wide national and global scale.

The development of 'cyber security issues' can be understood looking at the phases of development of computers, networking, the www and domain name system, e-commerce, e-governance each of which reveals unique consequences and appliances in the society and related security risks. While not all of those risks are directly relevant to national security and international peace and security, the way we implement and interpret regulations and policies enacted for specific activities and

[1] Dunn 2005 page 20.

functions (such as e-commerce, personal data protection) today needs to be assessed and balanced against national and international security concerns.

Taken from potential adverse effects perspective the uses of ICTS may result in economic consequences, disruption to critical infrastructures or threats to national and international peace and security. Therefore, any regulation or policy decision about 'cyber' involves considerations of more than just the immediate object of regulation or decision.

For these reasons the lists of instruments and overviews of multilateral cyber security arrangements also cover topics like information infrastructure, cyber crime or information society services – all these regulations now need to be interpreted or implemented having regard to national and international security concerns.

3. **The use of the term 'cyber security' often occurs with little criticism and scrutiny.** It is rarely that documents and literature on cyber security follows such a step-by-step, contextual and historical analysis of the issue. It is often that 'cyber' is used in the absence of a deeper understanding of the scope and background of the issue or even to as a deceptive to conceal the absence of expertise. Therefore, careful scrutiny is required when assessing the relevance and impact of different international organizations' agendas, processes and instruments.

4. **'Cyber security' falls into the area of attention and mandate of several organizations and areas of expertise**. As the term comprises a variety of functions and measures, it justifies and calls for attention of different international actors under various mandates (telecommunication infrastructure, economic growth, human rights, crime, international peace and security). It therefore falls into the area of regulatory and political attention of most international and regional organizations.

   Dimensions of uses of ICT invoke the applicability of different 'regimes', regulations and venues, which makes it crucial to identify and match the 'cyber issue' and the appropriate venue, regime and instruments to deal with it.

   Considering the ways ICTs are used to support and develop societies the studies and discussion of 'cyber' are increasingly interdisciplinary, involving technical, policy and diplomatic, legal, social, and economic dimensions. Emphasis on priorities, remedies and goals can be differently placed depending on the dominating background system.

   'Cyber security' constitutes a constantly emerging issue as there is not enough experience implementing peace-time regulations with national security concerns in mind.

5. **National interests and priorities in the field are unequally aligned.** Due to varying stages of information society development, access to global communications and other geopolitical and socio-economic factors the main national concerns related to uses of ICTs vary to a large extent. A polarization of interests has occurred between

liberal democracies headed by the US and the UK on one side and the Shanghai Cooperation Organization countries on the other regarding questions like which model of Internet governance should be adopted on an international level, if international law and in particular the law of armed conflict is (potentially) applicable to uses of ICTs and which uses and implications of ICTs are subject to national sovereignty.

Such deviation of certain interests has led to principal opposition affecting the work of several international organizations (e.g. the UN, Council of Europe) and may lead to delay tactics in several multilateral processes. Dissimilar views on the importance of the issue on the international level and measures to be taken have affected also 'like-minded' processes in NATO and the EU.

Inevitably, cyber security related priorities and capabilities also differ by regions. Therefore, any regional processes in the field are currently likely to get more traction and lead to practicable outcomes.

6. **Implementation of practical security measures is complicated**. Packet-switching technology has the ability to confuse the geographical reality easy to encompass for circuit-switching communications. The protocols of IP-based communication enable anonymity of communications, thus complicating functions such as law-enforcement and state coercion. Yet every 'cyber' asset or function falls under the jurisdiction of a particular nation state even if a link is difficult to establish. Attribution thus constitutes a complex issue embedded in technical reality of how the Internet works, but affecting law enforcement and policy level decision-making about the incidents. With the 'individual' security model focusing on the business models and related risks of self-standing organizations and entities is gradually overtaken by a 'collective' security model where the security of all stakeholders will depend on the risk assessment and capabilities of others, new ways to coordinate security requirements and their implementation need to be put in place.

There are several "hot spots" in international cyber security dialogue that need critical assessment of the notion of 'cyber security' in context, the mandate of international actors involved as well as the potential implications of relevant processes and instruments on an international and national level. An example would be a wide misperception about ITU's mandate in the field of 'cyber security' that many authors consider all-inclusive with a reference to the WSIS (2003)[2] while others reject this argument referring to ITU's mandate as a rather technical and administrative one and not covering politico-military aspects of cyber security. The practical relevance for a country is related to realistic prospects of exercising its interests on an international level as different organizations are likely to offer different remedies and possibly competing solutions to the issues put before them.

II International Organizations: Agendas, Processes and Instruments

1. International and European Organizations

The focus, interests and experience associated with issues of 'cyber security' differ significantly by international organizations just as the emphasis on challenges and acceptable remedies differs by nations. Behind the seeming homogeny and acceptance of a global 'cyber security' agenda the focus is split and often diffused around issues like technical security of computers and networks, development of the information society, availability and maintenance of telecommunication and information infrastructure, e-commerce, human rights, crime, terrorism, uses of force.

In such a flabellum of topics the division of and boundaries between the disciplines and areas of expertise and mandate are not always clear. Several organizations have extended their attention to 'cyber security issues' as the nature of the conflict has shifted over the past few years from (organized) cyber crime to national security relevant incidents with political motivation and undertone and, occasionally, touching upon the concerns of international peace and security.

It is therefore very difficult to assess the impact of particular 'cyber security' processes and agendas on a global and even on a regional and national scale because the codename 'cyber security' conceals different focal points and areas of emphasis.

While some organizations, such as NATO, are relatively new to strategic cyber security dialogue, several organizations, notably ITU, OECD, EU and the UN have entered the 'cyber security' arena each with unique experience and a history of involvement in particular aspects of development and uses of ICTs and have gradually extended their area of attention and involvement.

An uneven landscape like this is explained by several interconnected factors – the historical area of attention of any given organization, its goals and mandate and its constituency, the indistinctiveness of the combining term, but also by now a number of *ad hoc* situations where issues have been brought to the attention of different international organizations by their member states.

The following is intended to provide an outline of main recent and ongoing multilateral cyber security related processes and agendas and an overview of the instruments adopted by major international and regional organizations in the field.

The assessment of relevance and impact of such agendas and processes is solely that of the author, based on her experience and observations from international working groups and to a lesser extent on interviews with colleagues involved in relevant processes. The reader needs to be wary of the deeper interest for and involvement by the author in politico-military rather

than socio-economic aspects of ‘cyber security’.

The United Nations

Main areas of focus and impact: crime, international peace and security
Secondary areas of focus and impact: human rights

The Disarmament and International Security Committee (the **First Committee**) has looked into the developments and uses of technology since late 1990s. The use of information and communication technologies[3] became its focal point from politico-military perspective in conjunction with the Russian draft Resolution from 1998 on the Developments in the Field of Information and Telecommunication in the Context of International Security[4].

Since then the Resolution has been passed yearly[5] with Russia and the Shanghai Cooperation Organization (covered later in this study) countries as the main sponsors. Three groups of governmental experts have been called to consider existing and potential threats in the sphere of information security, possible cooperative measures, and to conduct a study of international information security issues. Yearly national contributions address concerns and proposals on global information security.[6]

The Russian initiative has been counterbalanced by the US with the goal to focus the discussions of 'cyber security' more on combating the criminal misuse of information technologies and law enforcement in the **Third Committee**[7] and 'a global *culture of cybersecurity*'[8] in the **Second Committee**. The concepts of the Second Committee are further pursued in the framework of IGF (covered later in this study).

Cyber crime has been in the focus of the UN since 1990 when the first resolution on computer crime legislation was adopted at the Congress on the Prevention of Crime and Treatment of Offenders.

At the **UNODC** Expert Group on Cybercrime[9] session in Vienna in January 2011 Russia initiated a discussion on a new convention on cybercrime at UNODC, referring to the

[3] The term „use of ICTs" has been adopted to scope key concerns and remedies of international information security.
[4] The original resolution can be found in Annex 1 to this study.
[5] The latest draft resolution can be found as Annex 2 to this study.
[6] See in more detail Tikk-Ringas (2012).
[7] See A/RES/55/63, A/RES/56/121.
[8] UN General Assembly resolution 57/239 (2002) outlined elements for creating a global culture of cybersecurity, inviting member states and all relevant international organizations to take account of them in their preparations for the WSIS. UN resolution 58/199 (2003) further emphasized the promotion of a global culture of cybersecurity and the protection of critical information infrastructures.
[9] The mandate of this group is to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing and to propose new national and

Budapest Convention as unable to provide systematic response to the new trends of cybercrime and 'cyber terrorism'. Russian argumentation on the absence of codified notions of cybercrime and cyber terrorism and the lack of conceptual criminalization at the international level has been supported by China, Brazil and selected African countries. Following the Russian proposal an International Expert Group was tasked to conduct a thorough study on cyber security. Additionally, the Secretariat of the UNODC has drafted and circulated a preliminary questionnaire to seek feedback on the matter from member states.

The United Nations Congress on Crime Prevention and Criminal Justice has addressed the growing threat of cybercrime and its transnational and organized nature, concluding that legislation of different countries is dissimilar and that existing instruments have limited reach. The Congress has also criticized the Budapest Convention for its closed model of implementation and discussion of amendments. Calls have been made for the development of an international instrument on cybercrime. The Congress has emphasized the need for institutionalized capacity building and long-term sustainability, closing gaps in existing legislation and promoting consistency, coherence and compatibility of laws.

The scope and emphasis of developing a new international instrument is still open as the initiative on a new treaty is pending the conclusions to be reached *by the intergovernmental expert group*[10] *to conduct a comprehensive study of the problem of cybercrime* under the Salvador Declaration[11]. The likelihood of such an instrument to be drafted is high as there is more and more of a push for some kind of treaty at UN level from an increasing number of nations and the area of cyber crime is less sensitive area of norm development than that of international peace and security.

It has been noted that a comprehensive response to cybercrime might have to include a range of elements, including criminal law, the possibility of developing a universal international convention on cybercrime, technical assistance and other measures that would link cybercrime to a broader context of development and the use of information and communications technologies in general.[12]

The coalition of countries demanding clarity of norms applicable to cyber security is spear-headed by Russia and China. On September 12th 2011 four countries: China, the Russian Federation, Tajikistan and Uzbekistan submitted a letter to the Secretary General of the United Nations[13]. Annexed to this letter was a draft code of conduct for information security. This document has been promoted as their entry position at the UN GGE discussions. One of the key points enshrined in the Code is the reference to the sovereignty of states.

The purpose of the Code is to identify the rights and responsibilities of states in the information space. The scope is more-or-less similar to the document proposed by the CoE -

---

international legal or other responses to cybercrime (ECOSOC in its resolution 2010/18 and by the Genral Assembly in its resolution 65/230).

[10] Established under General Assembly Resolution 65/230.

[11] Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice systems and Their Development in a Changing World.

[12] United Nations Commission on Crime Prevention and Criminal Justice Report on the twentieth session (3 December 2010 and 11-15 April 2011). E/2011/30* E/CN.15/2011/21*

[13] United Nations General Assembly A/66/359.

Internet Governance Principles. Both are meant to be non-binding instruments and open to all the states. The proposal has faced stiff political rejection by the coalition of the like-minded liberal democracies involving, among others, the US and UK, France, Germany, Australia, Japan and Estonia.

UNIDIR has engaged in event co-hosting and reporting with the German and the U.S. governments and has been proposed by Russia as a venue for conducting a study on the applicability of international law to uses of ICTs for the purposes of the First Committee process.

While the Security Council has so far abstained from discussing cyber security issues, a task force has addressed aspects of cyber terrorism. The Counter-Terrorism Implementation Task Force (**CTITF**) was established by the Secretary-General in 2005 and endorsed by the General Assembly through the United Nations Global Counter-Terrorism Strategy in 2006. In 2011 the Task Force published a compendium on Countering the Use of the Internet for Terrorist Purposes — Legal and Technical Aspects[14], predated by a report on the same topic in 2009.

In accordance with its mandate, the UN has discussed a variety of cyber security topics and issues, but largely without groundbreaking outcome or influence. National input to the First Committee process indicates significant differences in understanding and emphasis on the issue. Although some countries have indicated the UN as best potential guarantor of global cyber security, such proposals have remained below considerable publicity and global consensus threshold.

The main current processes in the UN include the Group of Governmental Experts convening under the auspices of the First Committee to address threats to international information security as the outcome of the work of this group reflects consensus among the Permanent Five about what is regarded as a potential threat to international peace and security and what are the measures expected from member states to build confidence in peaceful uses of ICTs and, in case of a conflict, prevent escalation.[15]

Also, a still pending proposal on a new international treaty on cyber crime deserves attention and perspective assessment from strategic level 'cyber security' communities as this reflects the potential of criminal cooperation on a global level.

National views on international information security are requested yearly under the information security initiative in the First Committee.

Additional readings:
Maurer (2011)

[14] http://www.un.org/en/terrorism/ctitf/pdfs/WG_Compendium-Legal_and_Technical_Aspects_2011.pdf.
[15] The first GGE met 2004-2005 and the second GGE 2009-2010. The meetings of the third GGE are scheduled to August 6-10, 2012 (New York), January 14-18, 2013 (Geneva) and June 3-7, 2013 (New York).

Tikk-Ringas (2012)

Instruments:

- United Nations. Economic and Social Council. Resolution 2010/18 – Twelfth United Nations Congress on Crime Prevention and Criminal Justice. E/2010/18. New York: United Nations, 22 July 2010.
- United Nations. Economic and Social Council. Resolution 2009/22 – International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity related-crime. E/2010/18. New York: United Nations, 30 July 2009.
- United Nations. Economic and Social Council. Resolution 2004/26 – International cooperation in the prevention, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes. E/2004/26. New York: United Nations, 21 July 2004.
- United Nations. General Assembly. Resolution 64/211 Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures (2010)
- United Nations. General Assembly. Resolution 65/232 - Strengthening the United Nations crime prevention and criminal justice programme, in particular its technical cooperation capacity. A/RES/65/232. New York: United Nations, 23 March 2011.
- United Nations. General Assembly. Resolution 65/230 - Twelfth United Nations Congress on Crime Prevention and Criminal Justice. A/RES/65/230. New York: United Nations, 1 April 2011.
- United Nations. General Assembly. Resolution 64/211 - Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures. A/RES/64/211. New York: United Nations, 17 March 2011.
- United Nations. General Assembly. Resolution 63/193 – Preparations for the Twelfth United Nations Congress on Crime Prevention and Criminal Justice. A/RES/63/193. New York: United Nations, 24 February 2009.
- United Nations. General Assembly. Resolution 60/288 – The United Nations Global Counter-Terrorism Strategy. A/RES/60/288. New York: United Nations, 20 September 2006.
- United Nations. General Assembly. Resolution 57/239 - Creation of a global culture of cybersecurity. A/RES/57/239. New York: United Nations, 31 January 2003.
- United Nations. General Assembly. Resolution 56/121 - Combating the criminal misuse of information technologies. A/RES/56/121. New York: United Nations, 23 January 2002.
- United Nations. General Assembly. Resolution 55/63 - Combating the criminal misuse of information technologies. A/RES/55/63. New York: United Nations, 22 January 2001.
- United Nations. General Assembly. Resolution 53/70 - Developments in the field of information and telecommunications in the context of international security. A/RES/53/70. New York: United Nations, 4 January 1999.

IGF

Main areas of focus and impact: Internet governance, information society development
Secondary areas of focus and impact: human rights

The Internet Governance Forum (IGF) is an open forum which has no members. The second phase of the World Summit on the Information Society (WSIS), held in Tunis, on 16–17 November 2005, requested the Secretary-General of the United Nations to convene "a new forum for a multi-stakeholder dialogue" – the IGF.[16] The mandate of the IGF, set out in Paragraph 72 of the Tunis Agenda for the Information Society[17], is to discuss the main public policy issues related to Internet governance in order to foster the Internet's sustainability, robustness, security, stability and development. The key questions IGF was intended to resolve where whether Internet governance should be transnational and private-sector led, or instead be put under the authority of territorial nation-states and intergovernmental organizations; and 2) whether the U.S. would continue to hold a privileged position in the overall system of global Internet governance through its control of IP addressing and domain names – and if not, what was the alternative?[18] The Secretariat is hosted by the United Nations Office at Geneva.

Since then, it temporarily became the leading global multi-stakeholder forum on public policy issues related to Internet governance.[19]

The first meeting of the IGF took place in Athens, Greece in 2006. The following meetings took place in Rio de Janeiro, Brazil in 2007, Hyderabad, India in 2008, Sharm El Sheikh, Egypt in 2009, Vilnius, Lithuania in 2010 and Nairobi, Kenya in 2011. The next meeting will take place in Baku, Azerbaijan in 2012. Initially the mandate was given by the UN General Assembly for only five years. During the meeting in 2010 several participants and states expressed their opinion to support the continuation of the IGF. The United Nations General Assembly agreed in December 2010 to extend the IGF's mandate for another five years.

Recently, the margin of usefulness of the IGF has received different assessments from governments. While the forum is perceived as useful for information society related discussions and coordination as it brings together initiatives and experience from various international organizations and governments. At the same time it has been referred to as largely ignorant to emerging security concerns. With the national security interests surrounding Internet governance issues the role of the IGF has gradually decreased and it is unlikely to produce practicable answers to the two key questions it was called to elaborate on.

Despite its marginal role in strategic level decision-making and concept development about national and international security concerns IGF still offers a useful networking and representation base for addressing economic and social aspects of Internet governance. However, IGF has not been used by the

[16] http://www.un.org/News/Press/docs/2006/sga1006.doc.htm.
[17] The Tunis Agenda for the Information Society, available at:http://www.itu.int/wsis
[18] http://www.internetgovernance.org/2012/07/30/is-there-any-hope-for-the-internet-governance-forum.
[19] http://www.intgovforum.org/cms/aboutigf.

leading governmental powers to propose new initiatives or discuss strategic issues.

G8

Main areas of focus and impact: technical security, CII, cyber crime

The Group of Eight first addressed information security in the communiqué of the Meeting of Justice and Interior Ministers (December 9-10, 1997). A program of specific actions was adopted to enhance national abilities to investigate and prosecute high-tech crimes and strengthen international legal regimes for extradition and mutual legal assistance.

The G8 countries have recently also turned their attention to the threat of the convergence of cybercrime and terrorist activity.

The involvement of the G8 in the global cyber security debate in the past few years has been modest. In Deauville 2011 the governments reaffirmed the need for coordination of the security of networks and services on the Internet.[20]

G8 has been used as a restart platform for emphasizing the need to deal with cyber security from a strategic and constructive perspective. However, its role in shaping multilateral discussions is rather declarative given the principal differences between the U.S., Russia and China on the next steps needed to stabilize international cyber security affairs.

Instruments:

- Principles and Action Plan to Combat High-Tech Crime (Annex to the 1997 Communiqué)
- Principles on Trans-Border Access to Stored Computer Data (1999)
- Principles on the Availability of Public Data Essential to Protecting Public Safety (2002)
- Recommendations for Tracing Networked Communications across National Borders in Terrorist and Criminal Investigations (2002)
- Principles for Protecting Critical Information Infrastructure (2003)
- Best Practices for Network Security, Incident Response and Reporting to Law Enforcement (2004)
- Best Practices for Law Enforcement Interaction with Victim-Companies During a Cyber-Crime Investigation (2005)
- Declaration on Renewed Commitment for Freedom and Democracy (2011)

[20] G8 DECLARATION: RENEWED COMMITMENT FOR FREEDOM AND DEMOCRACY (G8 Summit of Deauville - May 26-27, 2011)

Council of Europe (COE)

Main areas of focus and impact: human rights, cyber crime
Secondary areas of focus and impact: Internet governance, cyber terrorism

Although the Council of Europe is best known in the area of cyber security for its Convention of Cybercrime (also known as the Budapest Convention), it was the first international organization to address the issue of **automated data processing and privacy** in 1981[21]. It therefore has an important role of guaranteeing the independence of national data protection authorities. COE has also looked into the issue of cyber terrorism.

The **Budapest Convention**, adopted in 2001, is often in the core of cyber security and law discussions and questions about the sufficiency and adequacy of international law are often raised with reference to the Convention as the so far sole document addressing "cyber". Such an approach is legally ill-grounded as the Convention addresses only international criminal cooperation in the field of computer and network security. Under Article 27 t is not applicable in case of national security interests involved.

As recently several states in the world have suggested that the Convention needs update and does not adequately respond to all the new threats and challenges, several studies on the subject have been conducted.[22,23,24]

Overall, the Council of Europe is moving towards amending the Convention. The main challenges include cross-border forensics, jurisdiction and illegal access to data stored in the cloud, a set of issues possibly to be resolved by an additional protocol. The US has been against any changes in the Convention as it currently reflects the US legal landscape. The US has also noted that the ratification procedure is cumbersome and is concerned changing the Convention might send the wrong message to other countries.

Seen from the U.S. perspective the motivation behind rejecting the Convention by Russia and the like-minded countries is primarily political. Russian diplomats have confirmed that since

---

[21] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.I.1981.
[22] Cybercrime and Internet jurisdiction. Discussion paper prepared by Prof. Dr. Henrik Kaspersen http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079repInternetJurisdictionrik1a%20_Mar09.pdf.
[23] Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from "Cloud Computing Providers. Prepared by Joseph J. Schwerha IV http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_reps_IF10_reps_joeschwerha1a.pdf.
[24] Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal? Prepared by Jan Spoenle. http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/internationalcooperation/2079_Cloud_Computing_power_disposal_31Aug10a.pdf.

the Convention was not negotiated on a representative enough basis they do not see it as an acceptable platform for international cooperation in this field.

Cyber crime related questions have been discussed within the Cybercrime Convention Committee (T-CY) as well. The T-CY started to work with the subject in 2009, focusing on issues like jurisdiction and trans-border access to data and data flows.[25]

CODEXTER, established in 2003 to strengthen legal action against terrorism and safeguard fundamental values and address the causes of terrorism, has discussed the issue of cyber terrorism and concluded that:

"*The existing international conventions and other instruments that promote the harmonization of national substantive and procedural law and international cooperation are applicable to these misuses of the Internet for terrorist purposes: The computer-specific provisions of the Council of Europe's Cybercrime Convention that address national substantive law, national procedural law, and international cooperation can be used in cases of terrorism.*

Furthermore, the substantive and procedural rules as well as the rules on international cooperation found in international instruments on terrorism, on money laundering and financing of terrorism, and on general mutual assistance and extradition are also applicable in the cyber terrorism context.[26]

In 2006 the COE launched its Global Project on Cybercrime focused on global capacity building in the field. It also organizes an annual Octopus conference on fight against cybercrime. The **Octopus Interface** is a format for discussing the implementation and trends related to the Budapest Convention. Yearly events since 2007 elaborate on cybercrime threats and trends, implementation of the Budapest Convention as well as national policies and initiatives on cybercrime.

The Council of Europe has also looked into the issue of Internet Governance to create a non-criminal law framework on freedoms and liberties, obligations and responsibilities on the Internet as a European reflection to the IGF meetings. Such activities reflect the ideas of the European Convention of Human Rights. At a 2011 conference a package if Internet Governance Principles[27] was introduced accompanied by a set of principles on the protection and promotion of the universality, integrity and openness of the Internet[28].

---

[25] Ad hoc sub-group of the T-CY on jurisdiction and trans-border access to data and data flows. Draft Terms of Reference. T-CY (2011) 5 E http://www.coe.int/t/dghl/standardsetting/t-cy/tcy2011/TCY_2011_5E_BU_draft_tor_crossborder_v3.pdf.

[26] See CODEXTER (2007) cyberterrorism and other use of the internet for terrorist purposes – Threat Analysis and Evaluation of International Conventions.

[27] Declaration by the Committee of Ministers on Internet governance principles was adopted by the Committee of Ministers on 21 September 2011. https://wcd.coe.int/ViewDoc.jsp?id=1835773&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383.

[28] Recommendation CM/Rec(2011)8 of the Committee of Ministers to member states on the protection and promotion of the universality, integrity and openness of the Internet. Adopted by the Committee of Ministers on 21 September 2011

The activities of the Council of Europe are most valuable from the perspective of updating national criminal law and following the trends in investigating and prosecuting cyber incidents. The impact of the Budapest Convention is increased by a platform the Council of Europe has developed with the European Union. However, given the principal resistance to the Convention by a group of countries to include Russia, Brazil, South Africa, the impact of the European Union has decreased in this niche.

Instruments:

- Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (1981)
- Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data Regarding Supervisory Authorities and Trans-border Data Flows (2001Convention on Information and Legal Co-operation Concerning "Information Society Services" (2001)
- Convention on Cybercrime (2001)
- Additional Protocol to the Convention on Cybercrime Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed through Computer Systems (2002)
- Recommendation on Promoting the Public Service Value of the Internet[29] (2007)
- Resolution on Internet Governance and Critical Internet Resources[30] (2009)

The European Union

Main areas of focus and impact: technical security, information infrastructure, information society, e-commerce, cyber crime
Secondary areas of focus and impact: national security

The priority objectives for the European Union (EU) in the field of cyber security have long been the common market and related information society aspects as well as cybercrime. The European Network and Information Security Agency (ENISA) serves as relevant capability agency for the European Union, the EU Member States and the business community.

The EU has approached the issue of cyber security from rather different angles (see scheme 2), often in a defragmented and even competing manner. EU's main contribution to its

https://wcd.coe.int/ViewDoc.jsp?id=1835707&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383.

[29] Recommendation CM/Rec (2007) 16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet https://wcd.coe.int/ViewDoc.jsp?id=1207291&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75

[30] Reykjavik Resolution. http://www.coe.int/t/dghl/standardsetting/media-dataprotection/conf-internet-freedom/REYKJAVIK_RESOLUTION_INTERNET_GOVERNANCE.pdf

member states cyber security has been a harmonized level of preparedness to defend against cyber attacks as its numerous directives and decisions address security measures, required levels of security and practices for securing and maintaining information systems and services.

On the politico-military side, the EU has contributed to the mostly regional dialogue on critical infrastructure protection and cyber terrorism. In the past five years the European discussion on cyber security has comprised cyber defence from a military perspective. In 2009, a Concept of Computer Network Operations was adopted by the EU Military Committee.

In 2011, an EU Presidency organized conference to look into cyber security and defence as a comprehensive security policy challenge, analyzing present problems and solutions as well as future trends, with special regard to opportunities for co-operation with other international organizations. Since then, cooperation has been tightened with NATO, OSCE and the Council of Europe.

The fight against cybercrime has been a priority for European Union for a long time with dozens of directives have been adopted on various aspects of uses of ICTs and development of information society. Its most recent policy documents include:

1) Stockholm Programme which inter alia sets future priorities for the fight against cybercrime.
2) Digital Agenda for Europe.[31] The overall aim of the Digital Agenda is to maximize the social and economic potential of ICTs.
3) EU Internal Security Strategy[32], including as one of its five priorities the security in cyberspace and requiring the member states to pool their efforts at EU level.

On 30 September 2010 the European Commission published a new draft directive on attacks against information systems and repealing Council Framework Decision 2005/222/JHA[33] to update the cybercrime legislation of the EU and replace older Framework Decision. On the EU Directive proposal on attacks against information systems, Künnapu mentions that EU is struggling to draw a clear line between a crime and administrative offence which is directly connected to the question of whether to initiate or not a criminal procedure. Opinions on that matter differ in Member States.

The European External Action Service (EEAS), created under the Lisbon Treaty in 2009 is a diplomatic corps supporting the post of a new foreign affairs chief (Catherine Ashton from the U.K.) heading the European Union's international diplomacy. The role of the European External Action Service– is to support the High Representative in fulfilling their mandate to conduct the EU's Common Foreign and Security Policy. One of the tasks undertaken by the

[31] COM(2010) 245 final/2 A Digital Agenda for Europe http://eur-lex.europa.eu/Result.do?T1=V5&T2=2010&T3=245&RechType=RECH_naturel&Submit=Search

[32] COM(2010) 673 final The EU Internal Security Strategy in Action: Five steps towards a more secure Europe http://eur-lex.europa.eu/Result.do?T1=V5&T2=2010&T3=673&RechType=RECH_naturel&Submit=Search

[33] COM(2010) 517 final http://eur-lex.europa.eu/Result.do?T1=V5&T2=2010&T3=517&RechType=RECH_naturel&Submit=Search

EEAS is preparing the Communication on European Strategy for Cyber Security. This initiative is in progress and is expected to address cyber risks and threats and their potential dramatic impact on the European economy and society as well as propose measures to mitigate them.

The strategic objectives of this initiative are to overcome national fragmentation and support Member States in their efforts to ensure safe and resilient digital environment for all EU citizens, businesses and public administrations and to effectively prevent cybercrime, in respect of human rights and European values and to ensure concerted EU international activities in order to safeguard the EU's interests in the field of cyber security. The wording of the draft from May 2012 indicates key issues for the EU – consolidation of the approaches of the former pillars and creating a concerted response of many naturally competing or practically non-aligned entities.

The impact of the European Union in the field of international cyber security is defined by a harmonized level of cyber security in Member States (and the EEA) deriving from the numerous information society related instruments. The upgrade of relevant criminal law represents a valuable addition to any country's cyber crime arsenal. The work of ENISA has recently intensified and the agency has issued valuable guidance on CERT cooperation and cyber incident handling, also of strategic national relevance.

The maturing of the EU Joint Communication on a European Strategy on Cyber Security will indicate the shared views and values of the like-minded and the balance of interests between the EU countries. It is difficult to assess the practical impact of the document at this point.

Additional readings:

Klimburg and Tiirmaa-Klaar (2011), pages 29-36.

Instruments[34]:

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such data
- Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures
- Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions – Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime /*COM/2000/0890 final */
- Council Resolution of 3 October 2000 on the organization and management of the Internet (2000/C293/02)

[34] See Annex i for a more detailed list of EU instruments in the field of cyber crime and the fight against terrorism.

- Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')
- Communication from the Commission to the Council, the European parliament, the Economic and Social Committee and the Committee of the Regions COM(2000) 890 final – Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime
- Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data
- Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society
- Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Network and Information Security: Proposal for A European Policy Approach /* COM/2001/0298 final */
- Council Resolution of 28 January 2002 on a common approach and specific actions in the area of network and information security
- Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive)
- Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorization of electronic communications networks and services (Authorization Directive)
- Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive)
- Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive)
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
- Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the reuse of public sector information
- Decision No 1151/2003/EC of the European Parliament and of the Council of 16 June 2003 amending Decision No 276/1999/EC adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks
- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on unsolicited commercial communications or 'spam' (Text with EEA relevance) /* COM/2004/0028 final */

- Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems
- Decision No 854/2005/EC of the European Parliament and of the Council of 11 May 2005 establishing a multiannual Community Programme on promoting safer use of the Internet and new online technologies (Text with EEA relevance)
- Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC
- Communication from the Commission to the Council, the European Parliament, the European Economic and Social committee and the Committee of the Regions - A strategy for a Secure Information Society – "Dialogue, partnership and empowerment" {SEC(2006) 656} /* COM/2006/0251 final */
- Communication from the Commission to the European Parliament, the Council the European Economic and Social Committee and the Committee of the Regions - Communication on the implementation of the multiannual Community Programme on promoting safer use of the Internet and new online technologies (Safer Internet plus) /* COM/2006/0661 final */
- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on fighting spam, spyware and malicious software /* COM/2006/0688 final */
- Communication from the Commission on a European Programme for Critical Infrastructure Protection /* COM/2006/0786 final */
- Communication from the Commission to the European Parliament, the Council and the Committee of the Regions - Towards a general policy on the fight against cyber crime /* COM/2007/0267 final */
- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection - "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" /* COM/2009/0149 final */
- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Final evaluation of the implementation of the multiannual Community Programme on promoting safer use of the Internet and new online technologies /* COM/2009/0064 final */
- Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorization of electronic communications networks and services (Text with EEA relevance).

OECD

Main areas of focus and impact: human rights, e-commerce
Secondary areas of focus and impact: crime, CII

OECD has been engaged in privacy and computer-related crime from early on and was probably one of the first organizations to examine computer re-lated crime. With shared values on pluralistic democracy, respect for human rights and market oriented economies OECD's main focus is on economic and societal aspects of cyber security. The impact of OECD on the strategic threads of cyber security has been modest, but is increasing in the light of controversies around the topic of Internet Governance.

OECD Guidelines on Privacy in the form of a recommendation by the Council of the OECD was adopted and became effective in September 1980 and have been used in the development of laws and policies in a number of OECD countries, including Japan and Australia. As noted by the chairman of the Committee in charge of drafting the guidelines, as compared to the Council of Europe Convention the guidelines aimed at being less 'European' in orientation.
OECD's Intergovernmental Working Party on Information Security and Privacy (WPISP) develops policy recommendations and reports in the field of information society and resilience building. OECD's regular reports analyzing the impact of technology on information security and privacy as well as the OECD report on critical information infrastructure protection practices among its Member States are well-established sources of best practices, organizational structures and the regulations.

In 2011 OECD invited a study on Future Global Shocks including a sub-study on Reducing Systemic Cybersecurity Risk.[35]

As observed by Klimburg and Tiirmaa-Klaar[36], cybersecurity in the OECD context has predominantly been a sub-category of economic and technology policy and for that reason the rise of cybersecurity as a subject for national security has somewhat reduced its importance for the OECD's agenda.

Additional readings:

Klimburg and Tiirmaa-Klaar (2011), pages 23-24.

[35] http://www.oecd.org/sti/futures/globalprospects/46889922.pdf.
[36] http://www.oiip.ac.at/fileadmin/Unterlagen/Dateien/Publikationen/EP_Study_FINAL.pdf.

Instruments:

- Recommendation of the Council on the Protection of Critical Information Infrastructures [C(2008)35] 396
- Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy (2007)
- Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data (1980)
- Annex to the Recommendation of the Council of 23rd September 1980 Guidelines governing the protection of privacy and Trans-border flows of personal data
- Guidelines for the Security of Information Systems and Networks (1992, 1997, 2002)
- Recommendation on Cross-Border Co-operation in the Enforcement of Laws against Spam (2006)
- BIAC and MAAWG Best Practices for Internet Service Providers and Network Operators
- Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders (2003)

OSCE

Main areas of focus and impact: crime, terrorism, international peace and security
Secondary areas of focus and impact: CII

OSCE started discussions on strategic cyber security in 2008, with support from the Estonian Chairmanship of the Political and Security Committee. Previously, it had focused on combating cyber crime and terrorism. In June 2010 the U.S. proposed a discussion on norms for state behavior in cyberspace in 2010.[37] After a short deliberation of options, the strategic cyber security agenda now focuses on confidence building measures in cyberspace.

On the Ministerial Council level the Internet and cybersecurity are reflected in the OSCE Charter on preventing and combating terrorism.[38] The Parliamentary Assembly has adopted resolutions and declarations related to cybercrime and cybersecurity at different meetings. In Astana 2008 a Resolution on Cyber Security and Cyber Crime[39] expresses the regret that the international community has not been able to agree on specific countermeasures against cyber threats so far and urges the parliamentarians of the OSCE participating States to intensify their efforts in convincing the parliaments and governments in their countries that threats originating from cyber space are one of the most serious security challenges of present time

[37] See Schneider, Deborah, 'Cyber Security Keynote Address for the U.S. Department of State', United States Mission to the
OSCE, 9 June 2010, http://www.osce.org/fsc/68524.
[38] http://www.osce.org/mc/42536
[39] http://www.oscepa.org/publications/declarations/doc_download/256-astana-declaration-english

The Resolution on Cyber Crime[40] adopted in Oslo (2010) encourages the continuation of discussions in international forums on how to respond effectively to the abuse of cyber space for criminal and in particular terrorist purposes. The Belgrad (2011) Resolution on the overall approach of the OSCE to promoting cybersecurity[41] calls on the participating States to implement the Astana Commemorative Declaration – Towards a Security Community, particularly by increasing the efficiency of the OSCE in promoting a safer cyberspace to contribute to the fight against transnational threats as well as to the security and stability of the OSCE area

The Belgrade Declaration[42] reaffirms the Astana Declaration of 2008 and the Oslo Declaration of 2010 and their resolutions on cyber crime and cyber security recalling that cyber attacks are a great challenge to governments and that the results of a cyber attack against vital State infrastructure and commercial infrastructure are equivalent in nature to those of a conventional act of aggression.

Enhancing cyber/ICT security is a cross-dimensional topic and endeavor in the OSCE. For a number of years already the Organization's Action against Terrorism Unit (TNT/ATU) and its Strategic Police Matters Unit (TNT/SPMU) focused on awareness-raising and capacity-building activities in their related fields and promoted a comprehensive approach to cyber security, while the Representative on Freedom of the Media (RFoM) and the Office for Democratic Institutions and Human Rights (ODIHR) have also done relevant work.

In the past OSCE worked on individual projects aimed at combating terrorist use of the Internet and on combating cybercrime. This was followed by efforts to raise awareness and to promote a comprehensive approach to cyber security (as part of the OSCE's comprehensive approach to security). While OSCE remains engaged on specific cybercrime related trainings for law-enforcement professionals, its focus has shifted to developing confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies.[43]

OSCE was one of the first organizations to refer to a 'comprehensive cyber security' agenda distinguishing between (a) the politico-military domain, including critical infrastructures, and (b) cybercrime and terrorist use of the Internet.[44]

Despite a considerable contribution to the cyber security agenda the role of the OSCE has remained somewhat debated due to the reluctance of the liberal democracies headed by the U.S. to elaborate a binding set of norms on State behavior. Instead, the OSCE is currently mandated to elaborate proposals on Confidence Building Measures, possibly working to include a relevant chapter in the Vienna Document[45].

[40] http://www.oscepa.org/publications/declarations/doc_download/267-oslo-declaration-english
[41] http://www.oscepa.org/publications/declarations/doc_download/681-belgrade-resolutions-english
[42] http://www.oscepa.org/publications/declarations/doc_download/675-belgrade-declaration-english
[43] (PC/DEC/1039) [http://www.osce.org/pc/90169].
[44] 9.-10.05.2011 A Comprehensive Approach to Cyber Security: Exploring the Future OSCE Role. http://www.osce.org/event/cyber_sec2011.
[45] The Vienna Document 1999 was adopted by the FSC and endorsed at the Istanbul Summit. It is included in the Istanbul Document 1999.

Nevertheless, OSCE is increasingly regarded by many nations as a forum with high potential for constructive cyber security discussions. It is believed that this is an area where the OSCE brings a lot of unique expertise to the table and where the Organization can fill an existing gap in international efforts related to cyber security. Of course, what countries discuss at the OSCE level should then, ideally, also feed into what they discuss elsewhere, including at the global level, i.e. the UN.[46]

The 2011 OSCE Lithuanian Chairmanship-in-Office initiated the OSCE Conference on a Comprehensive Approach to Cyber Security: Exploring the Future OSCE Role (May 2011). One outcome was that delegations voiced their support to look into the possibility of harnessing OSCE expertise in the area of Confidence Building Measures (CBMs) and to apply it to cyberspace as part of enhancing inter-state transparency, predictability, stability and reducing the risks of misperception, escalation and conflict; and as a means to complement efforts, inter alia, at the UN level.

Concretely, in PC/DEC/1039 the OSCE participating States decided to develop CBMs to reduce the risks of conflict stemming from the use of information and communication technologies. The aim is to have a first set of such CBMs ready for adoption at the 2012 OSCE Ministerial Council in Dublin. Although the failed attempt to sign the US-Russian bilateral CBM package has resulted in tension between the two players it is anticipated that the OSCE CBMs discussion will be extended beyond 2013 and will be a constructive and productive effort.

OSCE process on CBMs in cyberspace will indicate valuable consensus platform between largely European countries and the balance of interests between the US and Russia. The work of IWG established under PC Decision 1039 is likely to be extended and the outcome considered relevant to the UN First Committee work in the field.

Instruments:

- OSCE Strategy to Address Threats to Security and Stability in the Twenty-First Century[47]
- Decision No. 7/06 on Countering the Use of Internet for Terrorist Purposes
- Decision No. 3/04 on Combating the Use of the Internet for Terrorist Purposes (MC.DEC/3/04)
- Decision No. 7/06 on Countering the Use of Internet for Terrorist Purposes (MC.DEC/7/06) (supported the Council of Europe's efforts in combating cyber crime)
- Ministerial Statement on Supporting the United Nations Global Counter-Terrorism Strategy (MC.DOC/3/07) in support of the UN strategy and the work done by the UN.

[46] From an interview with an OSCE official.
[47] http://www.osce.org/mc/17504

ITU

Main areas of focus and impact: crime, technical security, information infrastructure
Secondary areas of focus and impact: CII, international peace and security

ITU is the United Nations specialized agency for information and communication technologies – ICTs. In addition to our 193 Member States, ITU membership includes ICT regulators, leading academic institutions and some 700 private companies. Therefore, ITU has been referred to as a true multi-stakeholder organization best suitable for Internet Governance.

ITU's role in cyber security has been advocates as a strategic one by the SCO countries and a rather administrative one on the liberal democracies side. One of the main differences between the two wings is the model of Internet governance that currently is split between several organizations, notably ITU and ICANN, the latter being mandated to supervise and develop the IP addressing and domain name system. With the ITU being responsible for development and maintenance of the telecommunication infrastructure the authority of both organizations is unclear at least in theory.

The ITU, under its Constitution, is established maintain and extend international cooperation among all its Member States for the improvement and rational use of telecommunications of all kinds. The issue related to the scope of such mandate arises primarily from the context rather than the wording of relevant provisions in the ITU instruments. The Constitution includes provisions on stoppage and suspension of telecommunication services, legal bases valuable for state-on state action in case of a conflict.

The International telecommunication Regulations adopted in 1989 and currently being revised (subject to discussion of the next ITU Plenipotentiary in Dubai, December 2012) have been referred to as empowering the ITU with the supervision over the security of the Internet. While the topic of privatization of telecommunication services was discussed and considered in 1989, the legal status of ITRs is hardly strategic. However, ITU's mandate has been *de facto* extended by the WSIS process and the IGF.

The launch in 2007 by ITU Secretary-General, Dr. Hamadoun I. Touré, of the ITU Global Cybersecurity Agenda (GCA) came as a surprise to those countries who had regarded ITU as primarily a technical and standardization agency. ITU has promoted GCA as a framework for international cooperation aimed at enhancing confidence and security in the information society. The GCA is designed for cooperation and efficiency, encouraging collaboration with and between all relevant partners and building on existing initiatives to avoid duplicating efforts.

In 2001, the ITU Council decided to hold the World Summit on the Information Society (WSIS) and in Resolution 56/183, the United Nations' General Assembly endorsed the

framework for the Summit adopted by the ITU Council.[48] The first phase of the Summit was held in Geneva in December 2003 and the second phase in Tunis in November 2005.

The WSIS Declaration of Principles[49] call for a global culture of cybersecurity to strengthen information security and network security, authentication, privacy and consumer protection, and for building confidence among users of ICTs.

The WSIS[50] and the 2006 ITU Plenipotentiary Conference have mandated the ITU with coordinating international efforts in the field of cybersecurity as the sole Facilitator of Action Line C5, "Building confidence and security in the use of ICTs".

The Tunis Agenda[51] describes the establishment of a mechanism for implementation and follow-up to WSIS and requests ITU to play a facilitator/moderator role for WSIS Action Line C5. In order to stress the importance of the multi-stakeholder implementation of related work programmes, ITU has named this the Global Cybersecurity Agenda[52] initiative.[53]

In 2011 the ITU concluded a strategic alliance with the International Multilateral Partnership Against Cyber Threaths (IMPACT) an international public-private initiative of controversial reputation. IMPACT is projected to host the ITU GCA.

Since 2011 IMPACT officially holds the status of executing arm of ITU in the field of cyber security. According to the agreement, IMPACT provides ITU's 193 Member States access to expertise, facilities and resources to effectively address cyber threats, as well as assists United Nations bodies in protecting their Information and Communication Technologies (ICT) infrastructures.[54] The IMPACT/GCA initiative of the ITU has received wide acceptance from the international community[55] but has been rejected by the U.S. and the like-minded as an attempt to acquire excess authority over strategic decision-making in the field.

The processes to follow are the upcoming plenipotentiary in Dubai that is expected to clarify the balance of interests between economically less developed countries and leading information societies on the model of Internet governance and is also expected to specify ITU's role in this respect.

Instruments:

- ITU Constitution
- International telecommunication regulations (1989)
- Resolution 50 – Cybersecurity (2008)[56]
- Resolution 52 - Countering and combating spam (2009) [57]

[48] http://www.itu.int/osg/spu/cybersecurity/docs/UN_resolution_56_183.pdf
[49] http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1161|1160
[50] http://www.itu.int/wsis/
[51] http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2267|0
[52] http://www.itu.int/osg/csd/cybersecurity/gca/index.html
[53] http://www.itu.int/osg/csd/cybersecurity/WSIS/background2nd.html
[54] http://www.itu.int/ITU-D/cyb/cybersecurity/impact.html
[55] http://www.itu.int/ITU-D/cyb/cybersecurity/docs/IMPACT_AnnualBook.pdf
[56] http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.50-2008-PDF-E.pdf

- Resolution 58 - Encourage the creation of national Computer Incident Response Teams, particularly for developing countries
- Resolution 60 - Responding to the challenges of the evolution of the numbering system and its convergence with IP-based systems / networks
- Resolution 64 - IP address allocation and encouraging the deployment of IPv6
- The World Telecommunication Development Conference Resolution 45 (Hyderabad, 2010)
- *Resolution 130 (Rev. Guadalajara, 2010) on Strengthening the role of ITU in building confidence and security in the use of information and communication technologies user awareness of risks in cyberspace*
- *Resolution 174 (Guadalajara, 2010) on ITU's role with regard to international public policy issues relating to the risk of illicit use of information and communication technologies*[58]
- *Resolution 181 (Guadalajara, 2010) on Definitions and terminology relating to building confidence and security in the use of information and communication technologies*[59]
- *International Telecommunication Union. –Overview of cybersecurity – Recommendation*
- *ITU-T X.1205‖. Series X: Data Networks, Open System Communications and Security" – Telecommunication security. Geneva: United Nations, April 2008*
- Resolution on Non-Discriminatory Access and Use of Internet Resources (2008)
- Sample Legislative Language for Cyber Crime (2008)
- WSIS Declaration of Principles (2003)
- WSIS Plan of Action (2003)

ICANN

This section is pending additional input from the ICANN Point of Contact. Contribution expected Oct 15, 2012.

Main areas of focus and impact: technical security, administrative aspects

ICANN represents a much-disputed format of an international organization as it is established under the US jurisdiction and therefore does not represent a true inter-governmental organization model. Many nations have accused the United States in retaining the control package over the Internet by subjecting ICANN to its national jurisdiction as the organization is in effective control over developing and maintaining the DNS system and managing the IP addressing system.

ICANN has been reluctant to get involved in national security and international peace and security concerns related to or potentially solvable by the security of DNS. Secure DNS, IPv6.

Additional readings:

[57] http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.52-2008-PDF-E.pdf
[58] http://www.itu.int/osg/csd/cybersecurity/WSIS/RESOLUTION_174.pdf
[59] http://www.itu.int/osg/csd/cybersecurity/WSIS/RESOLUTION_181.pdf

Klimburg, Tiirmaa-Klaar (2011), pages 21-22.

NATO

Main areas of focus and impact: national security, international peace and security
Secondary areas of focus and impact: CII

NATO's deeper engagement in 'cyber defence' issues started with the decision in 2003 to subscribe a cyber defence expertise from the CCD COE finally established in Tallinn, Estonia in 2008.

Due to politically motivated cyber attacks against Estonia in 2007 and following the initiative of Estonia, France, the U.K. and the U.S., the North Atlantic Council and the Military Committee ordered development of NATO Cyber Defence Policy[60] and NATO Cyber Defence Concept[61].

The NATO Cyber Defence Management Authority (CDMA) Board has the main responsibility for coordination and strategic decision-making on cyber defence within the Alliance. The newly established Emerging Security Challenges Division coordinates political and strategic oversight for NATO cyber defence efforts. The NATO Computer Incidence Response Capability Technical Centre serves as a central technical authority on operational cyber defence issues.[62]

In order to promote consultations among Member States, NATO has initiated a framework of Memoranda of Understandings with Allies. The cyber defence MOU-s between the NATO CDMA and national cyber defence authorities facilitate regular consultation, information - sharing, and describe how the NATO Rapid Reaction Teams can support individual Allies in case of cyber crises. The MOU frameworks are open for PfP nations, in particular to the "NATO+10" group comprising Finland, Sweden, Ireland, Austria, Switzerland, Israel, South Korea, Japan, Australia and New Zealand as like-minded and technologically advanced partners.

The Lisbon Summit commits NATO and the Allies to address the new security challenges and, among other objectives, draws a very ambitious roadmap for the cyber-agenda of the Alliance. It includes bringing all NATO military and civilian bodies under central protection, introducing the cyber component to the defence planning process and accelerating information sharing and early warning capabilities.[63]

[60] A restricted document.
[61] A restricted document.
[62] http://www.oiip.ac.at/fileadmin/Unterlagen/Dateien/Publikationen/EP_Study_FINAL.pdf
[63] NATO, Developing NATO's cyber defence policy, 25 January 2011, http://www.nato.int/cps/en/natolive/news_70049.htm.

In 2010 NATO started a revision of its Cyber Defence Policy and the new Policy was adopted in June 2011.[64]

NATO's main concerns for 2012 have been achieving the full operational capability of NCIRC (expected October 2013), a CERT-like entity providing NATO agencies with information systems and network security services. NATO has also reorganized its information security agencies and created an umbrella organization in charge or both internal and cross-alliance information and communications systems.

The Policy Review process indicated considerable differences of mind among the Allies as to how to focus NATO's cyber defence activities. Politically, NATO has abstained from engaging in discussions of offensive capabilities and instead reiterated the need for cooperation and mutual assistance in case of a crisis or an attack both in Article 4 and Article 5 frameworks. The Policy itself is a rather vague and inconsistent document, accompanied by an action plan. The action plan divides tasks between NATO's reorganized agencies (in 2012 NATO Communications and Information Agency was established to bring NATO's information systems under a more centralized protection) and calls for a series of actions to explore and plan further cooperation among Allies in the field of strategic cyber security.

Recent updates indicate some lack of strategic vision in the field of cyber security and cyber defence. Potential action items include PfP arrangements and initiative on cyber security matters as well as recommendations on NATO's focus and strategic goals for the next Summit.

Instruments*[65]:

- NATO Cyber Defence Concept (2008)
- NATO Cyber Defence Policy (2011)

[64] A restricted document.
[65] NATO documents in the field are restricted.

2. Non-European Regional Organizations

OAS[66]

The Organization of American States has been supported in its cyber security related activities by the US Department of Justice. The work in the region comprises yearly cyber security conferences focusing mainly on law enforcement issues and CERT cooperation. OAS is planning a separate initiative for the Caribbean members. Training of judges and prosecutors is one of urgent needs. Brazil has been supporting the RU/CH narrative in the UN and on a bilateral basis.

AG/RES. 2004 (XXXIV-O/04): Adoption of a comprehensive Inter-American strategy to combat threats to Cybersecurity: A multidimensional and multidisciplinary approach to creating a culture of Cybersecurity.

AU[67]

The African Union has elaborated a draft convention on cybersecurity with assistance from ITU.[68] The Draft Convention seeks to harmonize African cyber legislations on electronic commerce organization, personal data protection, cyber security promotion and cyber crime control. It defines the security rules essential to establishing a credible digital space in response to the major security related obstacles to the development of digital transactions in Africa. The Republic of South Africa has been supporting the RU/CH narrative in the UN and on a bilateral basis.

ASEAN[69]

In ASEAN cyber security has been addressed by ASEAN Political-Security Community and ASEAN Economic Community.

The ASEAN Economic Community (AEC) Blueprint[70] was adopted in 2007 and it sets the goals and actions that should be implemented by 2015. Under section B (Competitive

[66] The OAS brings together all 35 independent states of the Americas and constitutes the main political, juridical, and social governmental forum in the Hemisphere.
[67] The African Union consists of 54 African states. The only all-African state not part of the AU is Morocco.
[68] Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/events/2011/WDOcs/CA_5/Draft%20Convention%20on%20Cyberlegislation%20in%20Africa%20Draft0.pdf.
[69] The Association of Southeast Asian Nations (ASEAN) was established in 1967 and currently it consists of ten Southeast Asian countries.
[70] http://www.aseansec.org/5187-10.pdf.

Economic Region) subsection B4 (Infrastructure Development) of the Blueprint points 51 and 52 refer to cybercrime and cybersecurity.

The ASEAN Political-Security Community (APSC) Blueprint[71] was adopted in 2009. Under Section B (A Cohesive, Peaceful and Resilient Region with Shared Responsibility for Comprehensive Security) Subsection B.4.1 (Strengthen cooperation in addressing non-traditional security issues, particularly in combating transnational crimes and other trans-boundary challenges) ASEAN should strengthen cooperation and assistance in combating and suppressing cyber crimes including cooperation among law enforcement agencies, taking into account the need of each country to develop laws to address cyber crimes.

ASEAN Vientiane Action Programme (VAP) 2004-2010[72] was adopted in 2004. Annex B of the VAP contains areas and measures for the AEC development of national Computer Emergency Response Teams (CERTs) and its capacity building, developing and implementing national cyber-laws and relevant telecommunications and IT policies and regulations that are consistent with international standards and norms, and ASEAN regional policy and regulatory frameworks and guidelines.

ASEAN Regional Forum in 2012 met a special workshop on confidence building measures (CBMs) in cyberspace. See as an important regional factor in shaping the UN discussion of CBMs ASEAN is currently setting up an initiative to develop a regional package of such measures.

SCO[73]

SCO has over the past years produced a package of information security related declarations and instruments. The Bishkek Declaration[74] on international information security emphasized the concern over the threat of using it for purposes inconsistent with the tasks of protecting international stability and security; the Dushanbe Declaration[75] (2008) referred to the importance of the UN General Assembly of Resolution 62/17 “Developments in the field of information and telecommunications in the context of international security”; The Yekaterinburg Declaration[76] (2009) highlighted the significance of ensuring international information security as one of the key elements of the common system of international security; the Tashkent Declaration (2010) noted that information security is closely linked to ensuring the state sovereignty, national security, social and economic stability and interests of citizens.

The Astana Declaration[77] (2011) emphasizes that the emerging real threats to information security are causing grave concern.

---

[71] http://www.aseansec.org/5187-18.pdf
[72] http://www.aseansec.org/VAP-10th%20ASEAN%20Summit.pdf
[73] The Shanghai Cooperation Organisation (SCO) is a permanent intergovernmental international organisation which was established in 2001 by the Republic of Kazakhstan, the People's Republic of China, the Kyrgyz Republic, the Russian Federation, the Republic of Tajikistan and the Republic of Uzbekistan.
[74] http://www.sectsco.org/EN/show.asp?id=92
[75] http://www.sectsco.org/EN/show.asp?id=90
[76] http://www.sectsco.org/EN/show.asp?id=87
[77] http://www.sectsco.org/EN/show.asp?id=294

An Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security was signed in Yekaterinburg on 15 June 2009. This instrument represents the SCO league approach to norms development and supports the Russian and Chinese initiatives to draft a new treaty for cyber security.

ECOWAS[78]

ECOWAS has adopted the Directive on Fighting Cybercrime in ECOWAS (2009) that provides a legal framework for the member states, which includes substantive criminal law as well as procedural law. The Directive deals with offences specifically related to ICT, incorporating traditional offences into ICT offences and sanctions for such offences.

APEC[79]

APEC's Cybersecurity Strategy[80] was approved at the APEC Telecommunications and Information Working Group meeting in 2002. In 2005 the Lima Declaration[81] was adopted recognizing the importance of ensuring the security and integrity of the APEC region's communications infrastructure, in particular the Internet, in order to bolster the trust and confidence of users and enable the continued advancement of this infrastructure. The Lim Declaration's Program of Action for the APEC Telecommunications and Information Working Group was also accompanied by the Key Principles for Broadband Development in the APEC Region; the Compliance and Enforcement Principles; the Guiding Principles for PKI-based Approaches to Electronic Authentication and the Principles and Implementation Guidelines for Action Against Spam.

Also in 2005 APEC Economic Leaders adopted the APEC Strategy to Ensure Trusted, Secure and Sustainable Online Environment[82].

APEC TEL Strategic Action Plan: 2010 – 2015 is the main policy instrument in terms of cybersecurity and cybercrime.

---

[78] The Economic Community Of West African States (ECOWAS) is a regional group of fifteen countries, founded in 1975. Its mission is to promote economic integration.

[79] Asia-Pacific Economic Cooperation (APEC) is a forum for facilitating economic growth, cooperation, trade and investment in the Asia-Pacific region.

[80] http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan012298.pdf

[81] http://www.apec.org/Meeting-Papers/Ministerial-Statements/Telecommunications-and-Information/2005_tel.aspx

[82] http://www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/~/media/Files/Groups/TEL/05_TEL_APECStrategy.ashx

III Brief Summary of Points of Emphasis

The focal point in cyber security discussions has shifted from information society development, e-commerce and primarily economic and social agendas to national security and international peace and security aspects of state and non-state behavior. The key processes to participate in and follow are the UN Disarmament and International Security Committee Resolution on International Information Security[83] and respective regional action at OSCE and ASEAN. The discussions of the Group of Governmental Experts under the auspices of the First Committee are likely to indicate short- to mid-term trends in international cyber security.

While the UN, split between polarizing priorities and views of the U.S. and other liberal democracies on one side and China, Russia and several other countries on the other, is yet undecided about its exact role in promoting confidence building measures in cyberspace, namely if it should have a more proactive and directing role or rather an endorsing and consolidating responsibility, high expectations are put on regional efforts, namely those of OSCE and ASEAN, to coordinate and frame regional views on confidence building and stability in cyberspace. While NATO's role is currently moderate due to a general standby policy promoted by the U.S., there is potential in NATO for capability development activities for its smaller members. PfP nations' engagement is encouraged and helping to facilitate the next political agenda and possibly a strategic defence agenda would likely be welcomed.

The heightened attention to cyber security has, however, also resulted in a wider recognition that cybercrime is a problem feeding into strategic security challenges and thus needs to be mitigated in parallel to national and international security concerns. The dialogue on cyber security has reintroduced the incentives of economic growth, human rights and freedoms and Internet governance. These topics now start undergoing a "securitization review" to be balanced against national and international peace and security concerns. The latter trend however, is just dawning and subject to resistance by historically established communities of Internet freedom, human rights and others.

Processes to get engaged and/or observe in the field of cyber crime are the cyber crime treaty initiative at the UN, amendments to the Council of Europe Cyber Crime Convention as well as development of the EU legal frameworks on cyber crime.

The discussions on international level are often confused by still inconsistent and often misleading use of key terms that diffuses crime, rights, peace and security and other issues into one large 'cyber security' agenda. While for many participating actors such a diffusion of terms and agendas does not constitute major obstacles in developing their positions, strategically less prepared and politically less sensitive communities have considerable difficulties with following relevant international developments. Still, many countries have not

[83] See para ... for details.

yet developed priorities and leads for strategic cyber security and are targeted by competing soft power injections by both leading strategic coalitions.

Constructivism from the side of international organizations is affected by political polarization on cyber security. Strategic differences introduce political obstacles to implementation of otherwise well-established international instruments, including the Budapest Convention and, theoretically, the Law of Armed Conflict.

The situation is further complicated by the fact that from a strategic perspective, 'cyber security' involves different areas of expertise and levels of authority and thereby constitutes a bundle of challenges difficult to grasp and address by any one expert or body. Adequate collective mechanisms of addressing this emerging global challenge have not formed yet. With many events occurring yearly to address cyber security, very few have found a constructive and specialized, yet insightful and contributing niche. Government level issues often deviate considerably from academic emphasis areas and a constructive dialogue is cumbersome, not least because of relative opacity of international strategic dialogue.

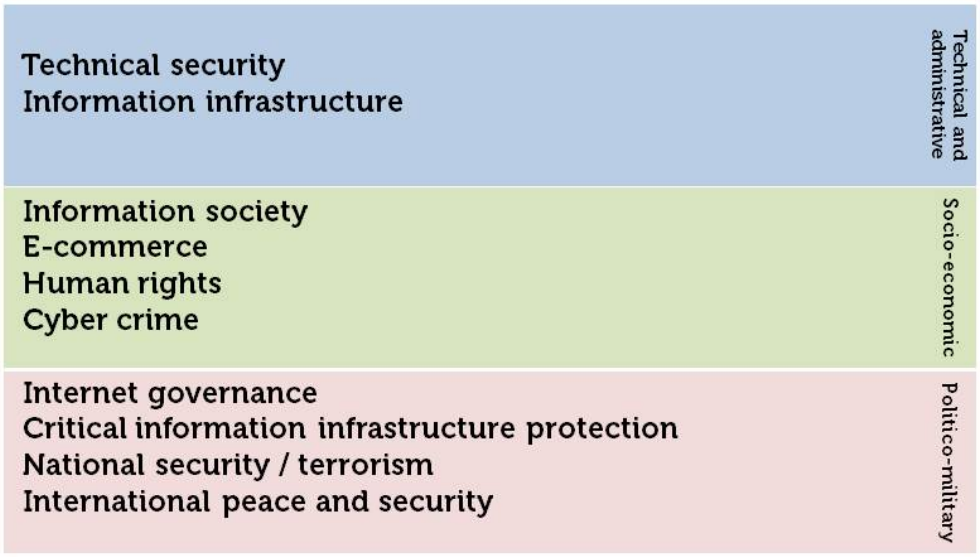
While a lot of political support is invested into the CBMs agenda, further important topics in the international dialogue comprise the fight against cyber crime, prevention of acts of aggression by state actors against each other as well as organized and politically motivated acts by non-state actors. The issue of international law and how it is applied to uses of ICTs by state and non-state actors is re-emerging and threatening to corner the CBMs discussion unless attended timely with satisfactory depth of argument.

The discussions on international cyber security are dominated by less than two dozens of states. Both political coalitions are engaging in extending their sphere of influence among non-aligned countries, thereby placing a lot of effort into developing narratives that such countries are likely to side with. The rise of soft and smart power approaches has been led by the US, Russia, China and to a somewhat lesser extent by the UK, leaving the niche for smaller state incentives and measures wide open.

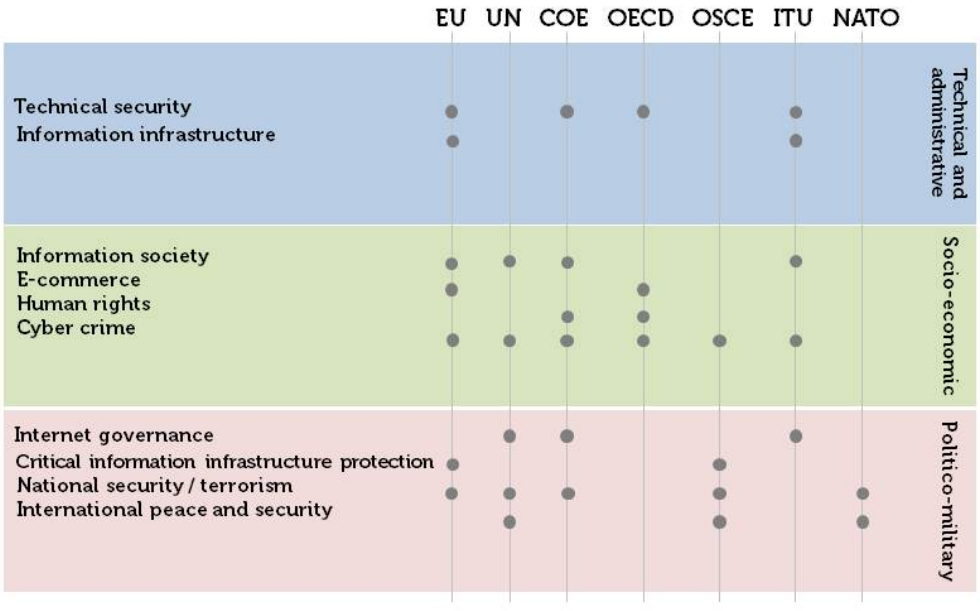
Events organized by regional organizations indicate a wide commitment and initiative in the field of cyber security, with often less emphasis on global political issues than, e.g. the UN or OECD processes. This does not mean that regional attempts to mitigate cyber security are less strategic. Rather, regional organizations get better traction in cooperation and coordination due to shared interests and pre-established contact and collaboration networks.

Additional Sources:

Michael Portnoy and Seymour Goodman (2008)
Klimburg, Tiirmaa-Klaar (2011)
Sieber COMCRIME Study (1998)
Dunn (2005)
CIIP Handbook
Peter Sommer, Ian Brown (2011) Reducing systemic Cybersecurity Risk
Melzer (2011)



Scheme 1: Division of main 'cyber security' topics into technical, socio-economic and politico-military issues



Scheme 2: Involvement and attention areas of international and European regional organizations