Policy paper

Development of cyber defense strategies on the foundations of strategic culture - small countries perspective

Adriana Dvorsak [1]

Abstract:

The differences in military doctrines occur because of the differences in national developments and strategic cultures. Some major social forces that are shaping the strategic culture are shared beliefs, assumptions, narratives that shape collective identity and relationships to other groups, and ends and means for achieving security objectives. Strategic culture is based on the following determinants: state formation, collective identity, the pattern of turning values into policies, civil society, and acceptance of international norms.

For the small states the asymmetric warfare represents a good part of military and national history. The asymmetric warfare used to be defined as a conflict involving two states with unequal overall military and economic resources; nowadays we should extend the definition to cover unequal resources in general thus covering the asymmetry of information and asymmetry of values.

It is of high importance for small states to underline the national goals of cybersecurity as the national and international level are often not enough distinguished and national strategies may turn out to be a response to the international threats. Upcoming from the Slovenian situation the key success factors of a national cybersecurity strategy are the right partnerships, establishment of effective incident management capabilities. Further success factors are appropriate organization of cybersecurity, appropriate legal framework, formulation of official strategies, expansion of membership of the national Security Council to other stakeholders, and clarified role of the Parliament in the authorization of a possible cyber attack.

Civil society as a determinant of strategic culture is playing its role in promoting values in the field of securitization of cyberspace, the attitude towards technology and in modernization of society. In relationship to regional activities Europeans and Slovenians will have to start thinking about European strategic culture.

---

[1] Adriana Dvoršak, associate of Institute NOVUM, holds Master of Arts degree by College of Europe, Brugge, Belgium. She graduated from International relations, Faculty for Social Sciences, Ljubljana

1. STRATEGIC CULTURE

Recent discussions on the possibility of a cyberwar going on among old adversaries in the Middle East, with Iran, in relation to China, and against authoritarian regimes in North Africa opened the questions on national and international norms in cyberwar, national strategies and national strategic cultures, non-state actors involved in the cyberwar, privacy concerns, and the role of civil society in global internet governance.

National military doctrines build upon the use of cyber capabilities for reconnaissance, information operations, disruption of critical networks and services, for cyberattacks, and as a complement to electronic warfare and information operations. Some countries include specific plans for informational and political operations. Others link cyberwarfare capabilities with the existing electronic warfare planning.[2] The differences in military doctrines occur because of the differences in national developments and strategic cultures.

Prior to laying out the elements of such a cyber strategy of a small country, it is useful to take a step back and look at some major social forces that are shaping the strategic culture. Let us begin with a simple definition that can be applied on the policy level and leaves some space for discussion on the academic level: strategic culture is that set of shared beliefs, assumptions, narratives (both oral and written), that shape collective identity and relationships to other groups, and which determine appropriate ends and means and modes of behavior, derived from common experiences and accepted for achieving security objectives. (Johnson, Larsen)

Strategic culture determinants will formulate strategic behaviors based on political tradition, history, values and beliefs, resources (especially economic and technological in the case of cyber strategy), great stories and classical texts, defense concept, geographical characteristics, experience of a political generation. Besides general determinants we must accept all other specific strategic foundations of individual states that can not be understood as a general strategic determinant. The same is also true for specific strategic cultures of non-state actors. The paper devotes special attention to new actors in cyber warfare however strategic behaviour of strategic personalities and other non-state actors is not examined into details.

Strategic culture is based on the following determinants: state formation, collective identity, the pattern of turning values into policies, civil society, and acceptance of international norms.

---

[2] Lewis, Timlin

In cyber defense state actors are giving way to non state actors which causes some concerns for the militaries. One of them is the nature of the adversary. Security culture is limited to the nation states and in cyberspace we have actors to which we could hardly apply any strategic culture. In this sense the known world with the written rules and strong hierarchical organization is meeting it's opposite. Perhaps western strategic cultures are meeting the actors that are not playing by any set of rules that could be easily grasped as a coherent framework of action. At the moment cybercrime and cyber attacks are carried out by individuals, hacktivists that have their own set of values according to which they play. Justice and feeling of injustice are strong motivation factors for them but we would not go on to pull over the non-state actors in cyberspace any other determinants of strategic culture. If we talk about state-sponsored attacks, the strategic culture can be freely applied.

Historic experiences of small countries are strongly embedded in asymmetric war however some states changed the sides in the asymmetry formally when they became full members of NATO alliance.[3] Popular sympathies for righteous small fighter groups will probably continue to exist under any particular communication programme, let it be from national or international political elites in EU or NATO. When we look at the strategic culture of our own and try to make assumptions of important items for cyberspace strategy, we can assume that the behaviour of actors in cyberspace e.g. criminals, hacktivists and nation states will play a big role in the response side. So strategic behaviour of adversaries have also certain reverse effect on the national cyber strategy.[4] At one point there will be also a question if the strategic cultures of Europe or European Union exist and how they differ from NATO strategic culture. The author assumes that the cyber defense path which had been approved in US can not and must not be copied in small European countries. In addition, Wamala in ITU framework gives the impression that the guide is too schematic to be adopted by small states and odd enough it skips all together the determinants of strategic culture.

Strategic culture shapes who decides on a national level, how they decide or what is the decision making process, how the decision makers acquire the necessary information, what are the acceptable compromises and acceptable policy options, and what is the learning process or feedback loop between the decision and the action. The decision making processes involved in cyber defense is important because of the formulation of a problem and a threat perception among elites, it affects the formulation of a policy including the initiation of cyber security strategies, development of respective national legislation as well as decisions to adhere to, or to ignore international norms.

[3] Črnčec
[4] Widely reported case of Estonia.

Cyber warfare brought forward new actors which are not to be found in the classical armed conflicts where one military confronts another. Individuals became important for the cyber security (for example hacktivists, patriot hackers, online activists, organized cyber crime, terrorist organizations, and other autonomous actors), which are not subject to international law. In addition these individuals are not familiar with military ethics, laws of neutrality, might not have clear intent, do not follow the rules of hierarchical organization in short, the international law has little or no effect on them. Le us consider only one somehow technical motive for cyber attacks, namely to gain the access to the systems or information important for the national economic or strategic objectives. The motive to gain the access precedes intentional attacks against the confidentiality, the integrity and the availability (CIA) of information communications technology (ICT) of a certain country.

The variety of new actors suggests that they are hardly susceptible to the international law; they seem to be more susceptible to international criminal law which needs a corresponding norm in the national criminal code to be effective. E.g. cyber crime must be criminalised by national criminal codes. Non-specific international norms, which consequently lead to criminalization of widely acceptable behaviour of non-state actors through national criminal codes, increase the feelings of injustice, wrongdoings, and significantly alter the relations among national decision makers and political organisations.

The nature of cybercrime and the legal issues are global and we can expect the states to collaborate in the development of international cyber crime norms. Cyber crime affects their economies and we can be sure that the efforts will be taken to ensure the harmonization of legislation in the individual countries through the international organizations, such as International Telecommunications Union (ITU), INTERPOL, United Nations Office on Drugs and Crime, G 8 Group of States, North Atlantic Treaty organization (NATO), Council of Europe (COE), Organization for Economic Cooperation and Development, Organization for Security and Cooperation in Europe (OSCE), The Commonwealth, European Union, etc. UN and NATO focus on activities related to cyberwar and cyberwarfare whereas any global agreement must be reached within UN.

2. EVOLVING INTERNATIONAL NORMS

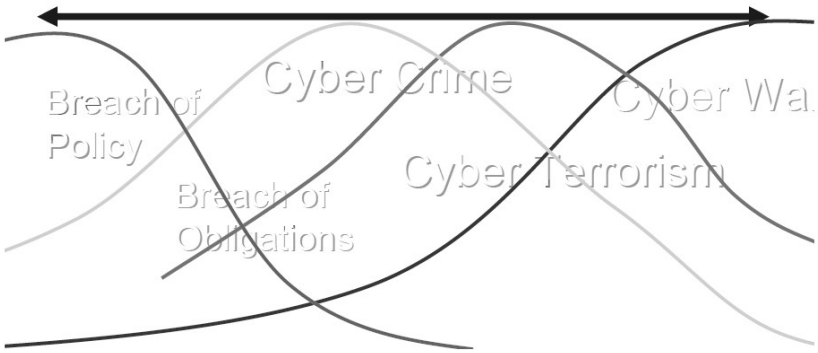
General thesis is that the states had been confronted with the zero sovereignty in cyberspace [5] which affected their views on the structure of power in the international relations. They try to overcome the state of zero sovereignty by

[5] Mueller

making proposals and negotiation on the international norms governing the cyberspace (ITU, OSCE, COE, European Union, and NATO). Simultaneously national doctrines emerge which are cutting out the national rules based on national values and beliefs. Lewis and Timlin reviewed policies and organizations of 133 states and roughly divided them into three groups of states. The first one comprises of 33 state that include cyberwarfare in their military planning and organization, second group of 26 states where there is no public discussion of a military role in cyberspace, and 12 states that plan to create specific military commands dedicated to cyberwarfare.[6]

The development of the international norms depends on the national cyber doctrines of the big states[7] which are also the forerunners in formulating the national doctrines, as well as at initiating the cyber warfare issues at the international institutions. The big actors' behaviour is central to the development of the international norms however attention has to be devoted to the small actors' behaviour as well. Cyber attacks and cyber warfare significantly increase the military options of the small states that have to be governed appropriately through multilateral mechanisms. Motives for cooperation highly depend on the assumption of what are the gains from the unilateral action, estimation of resources at hand, including knowledge available to the actor.

Communications law	International criminal law	Law of Armed Conflict
Communications society	Criminal law	Law of Armed Conflict



[6] JLewis, Timlin

[7] For the purpose of the paper the big states in Europe are France, Germany, and United Kingdom. Worldwide United States, China, Russia, Japan belong to the same group of big states.

Figure 1. Regulation of international and national cyber space, adopted from Marc-Arno Hartwig and Radomir Jansky, DG Home Affairs, SEDE meeting on 15 June 2011 - cyber attacks

Up to now international community did not reach an equivocal interpretation of the existing rules and principles of the international law to the cyberwarfare. However it is possible to single out few areas of the international law that are particularly important for the development of the international norms in cyberspace: jus *ad bellum, jus in bello* and the law of neutrality.[8] Legal discourse within the international arena is not the search for some legal truth out there, waiting to be discovered. It is a practice that operates on the basis of common understandings and shared beliefs about the relationship governed by the rules in question. Thus interpretation of the international law is the search for an intersubjective understanding of the norm at hand.[9]

In regard to the development of the international norms we must touch upon types of conflict, having in mind the attribution problem. Still, there is a basic state vs. state situation, non-state actor vs. non-state actor, and state vs. non-state actor. Note that non-state actors are in fact new actors about whom we do not know much, who might not be armed in the classical sense, who are mercenaries or who are taking a part in a cyber conflict unwillingly. Because of the variety and unpredictability of new actors it is worth following the life span and other characteristics of the non-state actors that are involved in the most severe cyber attacks. Smith, Long, and Johnson also analysed the strategic culture of violent non-state actors who are prone to combine terrorist acts with cyber warfare and/or cybercrime.

3. ZERO SOVEREIGNTY IN CYBER SPACE AND ASYMMETRIC WARFARE

For the small states the asymmetric warfare represents a good part of military and national history. Some of the states have realized only recently that their position in the asymmetry changed.[10] They changed sides in asymmetric warfare by joining the alliance and at the same time acquired access to additional resources which taken altogether altered their point of view on global relations. Small states position in the asymmetry is further transposed by growing transnational security threats such as cyberterorism and cybercrime, whereas we have to note that many

[8] Dvoršak

[9] Ian Johnstone, Security Council Deliberations: The Power of the Better Argument, 14 EUROPEAN JOURNAL OF INTERNATIONAL LAW 437, 440–43 (2003).

[10] Damir Črnčec, Obveščevalna dejavnost v informacijski dobi, Defensor, Ljubljana, 2011

analysts consider cyber attack in Euro-Atlantic area as a very realistic security threat in 2012. Two types of asymmetry significantly affect strategic relations: one is the asymmetry of information and another one is the asymmetry of values. The institutional structures of the actors involved in the cyber conflicts as well as the type of public response further reflects the asymmetric nature of cyber conflicts.

The asymmetric warfare used to be defined as a conflict involving two states with unequal overall military and economic resources;[11] nowadays we should extend the definition to cover unequal resources in general thus covering the asymmetry of information and asymmetry of values. In the asymmetric warfare we can expect non-state actors to enjoy certain advantages because of the asymmetric nature of conflicts in cyberspace due to information and value asymmetry. Cyber attack can be launched from almost any place while disguising the location, the identity or the sponsor behind the attack. Applying the principles of military necessity, proportionality and distinction against terrorist cyber attacks will be especially challenging since the terrorists may be even more heavily embedded in the civilian population than usual when launching attacks.[12]

International consensus on the importance of cyber security for the global governance has not been reached yet. There are also significant regional differences in public perception of the importance of cyber attacks for the national economies, importance of privacy issues, and on export regulation of surveillance technologies to non-democratic regimes. Consensus on the importance of cyber security and cyber defense will be formulated earlier in the professional community than consensus within the international community.

Variety of security threats grew exponentially alongside the probability of cyber attacks. Number of institutions that are entrusted with cyber security is particularly dense in Europe even if they are somehow over-involved with the strong principles of bureaucratic organizations. Structure of modern power is atomized giving disproportional power into the hands of individuals or small groups that can threaten much bigger actors especially if the institutional structures can not overcome the bureaucratic nature of the organization.

4. RECOMMENDATIONS FOCUSING ON THE NEEDS OF SMALL COUNTRIES

International norms and codes of conduct will be developed for the state behaviour and should primarily aim at preventing conflicts between the states in cyberspace.

[11] Thaza
[12] Murphy

The COE definition in the Convention on Cybercrime is sufficiently flexible to address the technology that goes beyond traditional computer systems. It includes mobile telephones that have the capability to produce, process and transmit data, such as accessing Internet, sending e-mail, and transmitting attachments.

At the moment cyber defense activities seem to be more acceptable by wider audiences than cyber crime activities criminalizing different online and offline behaviour of the individuals. Massive surveillance infringes human rights and privacy rights of citizens. In addition we have seen that penalising intellectual property rights (IPR) infringement on massive scale does not enjoy the popular support and it has already altered the political scenery in Europe.

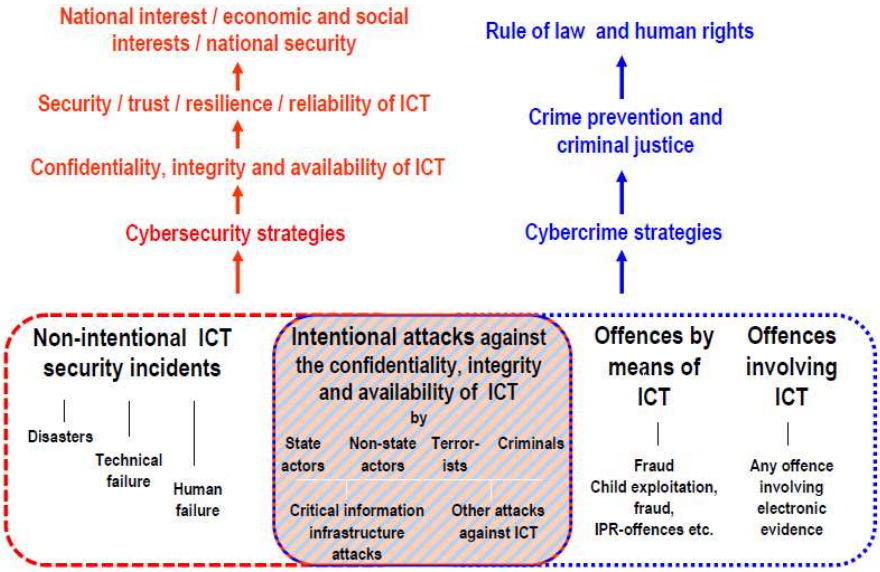


Figure 1. Cybercrime and cybersecurity strategies, Alexander Seger, Octopus conference 2011, COE

Cyber security stands for protection from intentional attacks against and by means of computers, any crime involving electronic evidence on a computer system. As a principle it is a subject of national criminal laws together with international criminal law and international norms in the field of communications technology. Punishment comes after the crime has been committed. In opposition to cyber security cyber defense stands for protection of critical infrastructure.

We can draw a conclusion that specific cyber security strategies might be separated

from cybercrime strategies, however synergies and complementarities exist. The governments are responsible for drafting cyber defense strategies; militaries are responsible to define the objectives and appropriate measures to achieve them. The governments are also hold responsible for success of private-public partnership and cooperation of the stakeholders.

There is a need to reconsider cybersecurity concepts and to bring together cyberdefense and cybercrime strategies in small states. To be more precise, human resources must be carefully considered before the government decides to establish CERT, CERT for public administration networks and CERT for critical infrastructure located in MoD. Basically MoD CERT in a small state like Slovenia should take over the role of incident management and become responsible for computer networks defense, coordination of cyber warfare resources and cooperation with national and foreign partners. The author also recommends the embedded expertise approach as human resources are insufficient in the small states to form effective cyber troops that would receive appropriate training for military purposes only. This author recommends authorizing the policy making body Council for information security to collaborate with partners on the national level independently in order to overcome bureaucratic hurdles.

ITU National Cybersecurity Self-Assessment Tool lines up the activities leading to the formulation of a cybersecurity strategy.[13] The following sequence of tasks adjusted from the ITU self-assessment tool represents the backbone of a national strategy on cybersecurity.

A Case for National Action:

- Identify a national policy on cybersecurity.

Participants in the National Response:

- Identify key government ministries and agencies with leadership responsibilities in cybersecurity and describe their roles.
- Identify key other participants with responsibilities in cybersecurity and describe their role(s).

Organizing for Cybersecurity:

- Identify organizational structures to be used for the development of cybersecuritypolicy and describe the workings of these structures and the involvement of other participants.
- Identify organizational structures to be used for ongoing cybersecurity operations and describe the workings of these structures and the involvement of other participants.

[13] Scope of Wamala's ITU national cybersecurity strategy guide is even wider and therefore difficult to follow by small states. The author of this paper holds true that small defense must integrate more functions within one institution to achieve the optimal cybersecurity ends than the big states.

Government-Private Sector Collaboration:

- Identify objectives and structures for government/private sector collaboration.
- Identify objectives and structures for trusted government/private sector collaboration.

Incident Management Capabilities:

- Identify location within government of the incident management capability function.
- Identify and prioritize objectives of the incident management capability function.

Legal framework:

- Identify objectives for updating the legal framework related to cybercrime.

Culture of Cybersecurity:

- Identify and prioritize objectives for building a national culture of cybersecurity.

Additional Requirements:

- Identify how the national strategy will be finalized and promulgated.
- Review funding requirements and sources for each element of the national strategy.
- Identify implementation timeframes.
- Identify metrics and reassessment objectives.

We should not neglect the ways in which the private sector is being pressured, compelled, and even encouraged to policing the internet by governments. By bringing this up we have touched upon the question of values in the field of securitisation of cyberspace, modernisation and the attitude of the society towards technology. The idea of security is most closely associated with the tradition of real politik, and the national security apparatus. Civil society is most often associated with respect for rights, democracy, diversity and openness. Securitisation of cyberspace builds momentum to either concede to the terms of the security debate and to the national security community, or to resist it altogether. Slovenian tradition in standing up for civil liberties is reach and inspirational hence civil society is not in favour of securitization of internet as it is the case in many European states.

In relationship to regional activites we should bring forward the European activities in the field of communications society, cooperation of police (EUROPOL), and cooperation of CERTs (ENISA) and start to think about European strategic culture. Besides national strategic cultures and strategic cultures

of violent non-state actors, we will have do develop the understanding of strategic behaviour of entity *sui generis* – what is the collective identity of European Union and what kind of values are turned into policies. We could move toward one more definition of strategic culture that will include technology, geography, history, organisational culture, European Union identity based on values such as soft power approach, secularization, rule of law, parliamentary democracy, institutional character of EU, normativisation, demilitarization in comparison to US etc. [14] "In fact, Europe is in need of updated assessments of the phenomena of migrations and their consequences, terrorism, cyber security, the security of trade routes, energy security or the rivalry for natural resources."[15]

To conclude, development in international and regional organizations put pressure on national decision makers and legislative to formulate cyber security system which will enable states to participate in international activities. National elites are responsible to bring national cyber capabilities, to be precise national incident management capabilities to required level for cooperation.

References

Črnčec Damir. Obveščevalna dejavnost v informacijski dobi, Defensor, Ljubljana, 2011.

Čaleta Denis, Rolih Gorazd Cyber security in the operation of critical infrastructure – an analysis of the situation in the field of Slovenian defence ISSN 2232-2825 November 2011 – 13/št. 3 Znanstveno-strokovna publikacija Slovenske vojske Contemporary Military Challenges Sodobni vojaški izzivi Deibert

Hartwig Marc-Arno, Jansky Radomir. CYBER ATTACKS – A new threat to EU´s security. DG Home Affairs European Parliament Security and Defence Subcommittee Meeting. 15 June 2011.

Koot Matthijs R. aka @mrkoot. Dutch Council on Int'l Affairs' Advise On Digital Warfare. Internet: http://blog.cyberwar.nl/2012/01/dutch-council-on-intl-affairs-advise-on.html, Jan. 22, 2012 [February 8, 2012].

Lewis James A., Timlin Katrina. "Cyber security and Cyberwarfare**,** Preliminary Assessment of National Doctrine and Organization " Center for Strategic and International Studies. [On-line]. http://www.unidir.org/pdf/ouvrages/pdf-1-92-9045-011-J-en.pdf [February 8, 2012].

Libicki Martin C. Cyberdeterrence and cyberwar, Project Air Force (U.S.), Rand Corporation, 2009

Mitropoulou Angeliki. Does the European Union have a strategic culture? March 29, 2011 [On-line]. [February 8, 2012]. http://www.e-ir.info/2011/03/29/does-the-european-union-have-a-strategic-culture-2/

Melzer Nils. Cyberwarfare and International Law. [On-line]. http://www.unidir.ch/pdf/ouvrages/pdf-1-92-9045-011-L-en.pdf. [February 8, 2012].

Mueller Milton. Politicization of digital tools. [On-line]. Dr. Milton Mueller, professor at the School of Information Studies (Syracuse University), analyzes the politicization of digital tools, at an Ifri seminar on "The Internet in China and Russia", IFRI, http://www.ifri.org/?page=contribution-detail&id=6744&id_provenance=79&lang=uk. [February 8, 2012].

[14] The five fundamental threats for Europe included in the December 2003 European Security Strategy were terrorism, the proliferation of weapons of mass destruction, regional conflicts, state failure and consequent regional instability and, last but not least, organised crime. Strategy defines also three strategic objectives.

[15] Jankowski,

Murphy John F. Mission impossible? International law and the Changing Character of War. In Pedrozo Raul A. "Pete", Wollschlaeger Daria P. International Law Studies. Volume 87. International Law and the Changing Character of War. Naval War College Newport, Rhode Island. 2011.
Papanastasiou, Afroditi, Application of International Law in Cyber Warfare Operations (September 8, 2010). [On-line]. Available at SSRN: http://ssrn.com/abstract=1673785. [February 8, 2012].
Seger Alexander. Cybercrime and cyber security strategies. [On-line]. Octopus conference 2011, Discussion paper: Cybercrime Strategies Prepared by Global Project on Cybercrime, Octopus Conference on Cooperation against Cybercrime, (Strasbourg, 21-23 November 2011). COE www.coe.int/octopus. [February 8, 2012].
Jankowski Dominik. Does the EU Really Need a New Security Strategy ?February 21st, 2012 http://foreignpolicyblogs.com/2012/02/21/eu-security-strategy/?utm_source=rss&utm_medium=rss&utm_campaign=eu-security-strategy
James M. Smith, Jerry Mark Long, Thomas H. Johnson. Strategic Culture and Violent NonState Actors: Weapons of Mass Destruction and Asymmetrical Operations Concepts and Cases INSS Occasional Paper 64 February 2008 USAF Institute for National Security Studies USAF Academy, Colorado
Johnson L. Jennie, Larsen A. Jeffrey. Comparative Strategic Cultures Syllabus. Defense Threat Reduction Agency. 20 November 2006 1
Svete Uroš. EUROPEAN E-READINESS? CYBER DIMENSION OF NATIONAL SECURITY POLICIES, Journal of Comparative Politics (ISSN 1338-1385) Pan European University, Bratislava University of Ljubljana, Faculty of social sciences, Volume 5, Number 1, 2012 http://www.jofcp.org/assets/jcp/JCP-January-2012.pdf
Thaza V. Paul, Asymmetric Conflicts: War Initiation By Weaker Powers 20, 1994.
Council of Europe. Convention on cybercrime. [On-line]. http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm. [February 8, 2012].
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. Conclusions on Critical Information Infrastructure Protection, Achievements And Next Steps: Towards Global Cyber-Security, Brussels, 2011.
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, 2009.
International Strategy For Cyberspace. Prosperity, Security, and Openness in a Networked World, May 2011. [On-line]. http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf. [February 8, 2012].
Wamala Frederick. International Telecommunication Union National Cyber security Strategy Guide. [On-line]. http://www.itu.int/ITU-D/cyb/cyber security/docs/ITUNationalCyber securityStrategyGuide.pdf [February 8, 2012].
International Telecommunication Union http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-self-assessment-toolkit.pdf [On-line]. [February 8, 2012].
Kuehl Dan. From Cyberspace to Cyberpower: Defining the Problem. Information Resources Management College/National Defense University [On-line]. http://www.carlisle.army.mil/dime/getDoc.cfm?fileID=181 [February 8, 2012].