International Law Research; Vol. 2, No. 1; 2013
ISSN 1927-5234 E-ISSN 1927-5242
Published by Canadian Center of Science and Education

Governmental Efforts and Strategies to Reinforce Security in Cyberspace

Gonenc Gurkaynak[1,2], Ilay Yılmaz[1] & Nazli Pinar Taskiran[1]

[1] ELIG Attorneys-at-Law, Istanbul, Turkey

[2] Member of Faculty at Bilkent University School of Law, Ankara, Turkey

Correspondence: Gonenc Gurkaynak, ELIG Attorneys-at-Law, Citlenbik Sok. No: 12, Besiktas, Istanbul, Turkey. Tel: 90-212-327-1724. E-mail: gonenc.gurkaynak@elig.com

Received: September 13, 2013 Accepted: October 21, 2013 Online Published: October 31, 2013

doi:10.5539/ilr.v2n1p185 URL: http://dx.doi.org/10.5539/ilr.v2n1p185

Abstract

The Internet is changing the world by bringing new ways to communicate to people and supporting open society and economic growth. The decrease in connection costs means accessing the Internet will become cheaper and easier, allowing more people around the world to use it. Increasing our dependency on the digital world brings new opportunities but also new threats. The more we open information and support digital mediums, the less guarded we become against the people and groups aiming to attack our digital intimacy. This openness also has certain effects on the soundness of the digital information of governments. Governments also have started to make effective use of digital technology over the last three decades. Hackers, leakers, international intelligence units and illegal groups target strategic digital networks, Internet sites and the infrastructures of governmental organizations as well as individual and private companies. Governments have started to develop strategies against these cyber-attacks, including legislative measures to protect themselves. Events in cyberspace happen at high speed and answering to these attacks and developing protections immediately are crucial points of cyber security. As the nature of the technology requires high speed development, governments need to adopt dynamic strategies against these attacks. Moreover, the cross-border nature of threats makes it essential to improve international cooperation.[1]

Keywords: cyber security, policy, privacy, data protection, cyber-crime, Turkey, European Union, Budapest Convention

1. Introduction

At the international level, there is no harmonized definition for cyber security[2] and the definition of cyber security varies from country to country[3]. Such variation influences different approaches to cyber security strategies among countries[4]. Cyber security strategies provide a strategic framework for a government's approach to cyber security[5]. For the purposes of this article, we define a cyber-security strategy as "long and short term governmental efforts such as policy making, international cooperation and technical support for the actors of cyber space for maintaining to improving security of information infrastructures and services"

Cyber security is an important challenge that requires dynamic and cooperative national and international policies. Such requirements mostly arise from the borderless nature of cyber-attacks. No matter how effective their strategy is, governments cannot on their own provide the security that is so essential for digital networks to fulfill their obligations. As such, the challenges of cyber security require cooperation between governments and this cooperation in return will require new policies and forms of policy making. In recent years, many

[1] Special thanks to Janelle Filson for her contributions to this article.

[2] H. Luiijf, K. Besseling, M. Spoelstra, P. de Graaf, Ten National Cyber Security Strategies: a comparison, CRITIS 2011 – 6th International Conference on Critical information infrastructures Security, September, 2011.

[3] In 1983, OECD defined computer-related crime as any illegal, unethical or unauthorized behavior involving the transmission or automatic processing of data.

[4] Lewis, J., Cyber security: turning national solutions into international cooperation. Vol. 24. Csis, 2003.

[5] European Network and Information Security Agency ("ENISA"), National Cyber Security Strategies, Practical Guide on Development and Execution, December, 2012.

governments, international organizations and foundations have searched for cooperative means to fight against cyber security.

Several governments have constructed their own cyber security strategies and regulations separately. The European Union ("EU") focuses on a solid legal and regulatory framework and promotes the Council of Europe Convention of Cybercrime ("Budapest Convention" or "Convention") as a blueprint for international cooperation and enforcement regarding cyber security which will be explained below in the section addressing multilateral cyber security approaches. The Anglosphere[6] on the other hand emphasizes a leading private sector role, an educated workforce, outreach and diplomacy for maintaining national cyber security. This includes the United States of America (US) which underlines the freedom of information in its cyber security legislation and emphasizes the role of the private sector. Still, due to the sensitivity of governmental information, cyber security is of vital importance and tends to be prioritized over freedom of information. The Baltic States are in tight cooperation with the North Atlantic Treaty Organization ("NATO") in the development of their national cyber security strategies. Meanwhile, the post-Soviet Commonwealth of Independent States bloc, led by Russia and China, focuses on internal threats, abhors extra-territorial judicial action, and promotes a corresponding international framework under the support of the United Nations ("UN")[7].

2. Background of Unilateral, Bilateral and Multilateral Approaches on Cyber Security

2.1 Background of Unilateral Cyber Security Approaches

The first national cyber security strategies began to be published during the first years of the previous decade. One of the first countries to recognize that cyber security implicated national security issues was the US. In 2003, the US published the National Strategy to Secure Cyberspace[8] which was a part of the broader National Strategy for Homeland Security that arose after the 9/11 terrorist attacks. Since then, the US considers national cyber security as a fundamental part of national security. The national cyber security strategies of the US split the burden between private and public organizations while also relying on the participation of the public sector to maintain national cyber security.

For similar national security reasons, and due to increasing numbers of attempted cyber-attacks, Europe soon followed suit in developing plans and strategies to address cyber security, although the plans initially were limited in focus. In 2005, Germany adopted the "National Plan for Information Infrastructure Protection". The following year, Sweden developed a "Strategy to improve Internet security in Sweden". Estonia was the first EU Member State to publish a broad national cyber security strategy in 2008, following a severe cyber-attack in 2007. In addition to the French government's "White Book of Defence" which includes a specific emphasis on cyber-attacks, the Prime Minister's Secretary General for Defence and National Security also published France's cyber security strategy, called the "Defence and Security of Information Systems".[9] France marks cyber-attacks against national infrastructure as a major threat that a country may face and generally refers to cyber security as "cyber defence" within their strategy. In 2009, France established a governmental body to maintain cyber security, the National Agency for the Security of Information Systems, which is affiliated with Secretary General of Defense. As discussed in more detail below, when compared to the US, EU member states appear to rely less on voluntary cooperation from the private sector in considering their cyber security action plans and strategies and create a bigger role for the state.

Turkey, as a candidate member state to the EU, has also published its own strategy in 2012, known as the Council of Ministers Decision Regarding Conducting Managing and Coordinating National Cyber Security Activities. The EU acquis of Turkey is categorized under 35 chapters and one of these chapters is "Information Society and Media Chapter" which requires the security of information systems.

Finally, as we search through the unilateral national cyber security approaches of the governments, some themes emerge. The main goals of the unilateral approaches appear to be as follows:

(i) Government security, which includes a focus on information and system security and protection against

[6] The Anglosphere is the term used to describe the group of countries in which English is the native language of the majority. The United Kingdom, Australia, New Zealand, the United States and Canada are considered part of the Anglosphere.

[7] Levin, Securing Cyberspace: A Comparative Review of Strategies Worldwide, 2012. http://www.ryerson.ca/tedrogersschool/privacy/documents/Ryerson_cyber_crime_final_report.pdf

[8] The National Strategy to Secure Cyberspace. (February 2003). http://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

[9] "Défense et sécurité des systèmes d'information. Stratégie de la France". www.ssi.gouv.fr/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf

attacks from foreign states and other groups. The goal is to safeguard a country's sovereignty and security by ensuring the confidentiality of its communications.

(ii) Protection of critical infrastructures, such as the buildings of intelligence units keeping massive volumes of personal data of the citizens, critical telecommunication infrastructures, etc.

(iii) Combatting cybercrime with the help of law enforcement authorities and by reinforcing legal frameworks regarding cyber security.

To successfully accomplish these aims, however, even a unilateral cyber security strategy will require cooperation with other countries and jurisdictions. The type of cooperation depends on the objective – government security, protection of critical infrastructures, or combatting crime – being pursued. For example, bilateral treaties often help with law enforcement while multilateral directives can be issued to protect critical infrastructures. The goal to protect government security and sovereignty is the most difficult around which to build international cooperation, given the sensitive national security and foreign policy issues at play.

2.2 Background of Bilateral Cyber Security Approaches

As stated before, cyber security needs the international cooperation of governments instead of singular efforts. Therefore, it is necessary to agree on mutual legal understanding between governments for cooperating against cyber-attacks at some point. This becomes particularly relevant with respect to combatting cyber-crime. Investigations into cybercrimes will often implicate multiple jurisdictions, necessitating information sharing between countries, or a domestic investigation may find that relevant online evidence is stored and hosted in a different jurisdiction. Formal bilateral arrangements for information sharing are generally formed in Mutual Legal Assistance in Criminal Matters Treaties ("MLATs"). However, MLATs do not exist between all of the countries that might need legal cooperation on cyber-crime investigations.

MLATs[10] are usually bilateral, addressing cooperation between law enforcement authorities of two countries, or multilateral, addressing cooperation among a group of countries. There are also hybrid models of MLATs; such as the EU-US MLAT that applies to the relationship of each EU Member State with the US, and the UN Model Treaty[11] for Mutual Assistance in Criminal Matters ("UN Model Treaty"), which is a multilateral model for bilateral MLATs.[12]

The scope of the UN Model Treaty is the mutual assistance between the states regarding criminal investigations. Such mutual assistance includes taking evidence or statements from individuals, making detained people available to give evidence or assist in investigations, effecting service of judicial documents, executing searches and seizures, conducting inspections, and providing evidence and records, including bank, financial, corporate or business records.

MLATs usually define the territories, the types of criminal activity, and the types of judicial proceedings that fall within their scope. It can be particularly critical to apply MLATs to terrorism activities and other crimes that transcend borders but, as discussed below, there are many challenges as well. MLATs specify the types of requested assistance that must be provided and that may be refused; its interaction with other treaties; and whether the treaty or national law will prevail in the event of conflict.

However, if there is no MLAT between two countries, a formal request for criminal assistance known as rogatory letters may also be used for bilateral cooperation. Under some circumstances and as an exception (e.g. child abuse), by the internet actors' own initiative, even MLATs are not needed for cyber-crime investigations as the internet actors may co-operate without following the MLAT procedure.

[10] Below please find some examples of MLATs:

EU-US Agreement on Mutual Legal Assistance Between the European Union and the United States Of America (2003), http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:181:0034:0042:EN:PDF

Canada-US, Treaty on Mutual Legal Assistance in Criminal Matters (1985), http://www.treatyaccord.gc.ca/text-texte.aspx?id=101638

UK-US, Treaty on Mutual Legal Assistance in Criminal Matters (1994), http://www.fco.gov.uk/resources/en/pdf/treaties/TS1/1997/14

US-China, Agreement on Mutual Legal Assistance in Criminal Matters (2000), http://www.state.gov/documents/organization/126977.pdf

US-Turkey, Extradition and Mutual Assistance in Criminal Matters (1979), http://photos.state.gov/libraries/turkey/461177/pdf/32t3111.pdf

[11] Article 15 of the UN Model Treaty on Mutual Assistance in Criminal Matters ("UN Model MLAT"), http://www.un.org/documents/ga/res/45/a45r117.htm

[12] The main MLAT providing a right to direct interception across borders is the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (2000) Art. 20; (Interception of Telecommunications without the technical assistance of Another Member State). http://www.official-documents.gov.uk/document/cm70/7054/7054.pdf.

Nonetheless, due to the rapid and unpredictable nature of cyber-attacks, bilateral cyber security approaches such as MLATs and rogatory letters are not always sufficient, especially for a law enforcement authority fighting against a borderless cyber-attack or other cyber security threats that do not resemble a traditional criminal investigation. It may be difficult to determine in advance whether the investigation will implicate foreign policy and intelligence issues rather than crime-fighting. Moreover, obtaining information through MLATs may prolong the investigation process if the treaty does not contain clear timeframes. The terms of the MLAT may not be up-to-date with the latest technology or types of cyber-crime. Finally, if MLATs lack sufficient safeguards, they may threaten individual privacy rights, particularly if they allow an investigatory authority to access evidence abroad and circumvent domestic judiciary processes.

2.3 Background of Multilateral Cyber Security Approaches

Virtually all countries support the establishment of international cooperation on cyber-crimes, as they are awakened to its importance and as the sophistication and scale of cyber-attacks grows.

Before the beginning of the last decade, many countries already were determined to establish international cooperation on a multilateral level. However, this intention was limited to sharing best practices with each other. As the borderless nature of cyber-crimes became more pronounced and attacks increased in the following years, a common understanding of a cyber-crime and legal framework became more critical. The main international organizations such as the UN and OECD started to actively work on international cooperation on cyber security and key legal instruments started to be published in this respect. Cyber security has thus been on the agenda of the UN for a number of years. The UN General Assembly has expressed itself on cyber security matters in its major resolutions.

The first resolution,[13] issued on December 4, 2000, focuses on combating the criminal misuse of information technologies. It draws on the United Nations Millennium Declaration and asks states to ensure that the benefits of the new technologies are available to all. It recognizes that the free flow of information can promote economic and social development, education and democratic governance. The resolution warns that unless addressed, the increasing criminal misuse of information technologies may have grave impacts on all states. In particular, the resolution includes the following statements:

"*States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies*."

"*Legal systems should protect the confidentiality, integrity, and availability of data and computer systems from unauthorized impairment and ensure that criminal abuse is penalized*."

The second resolution was issued on December 19, 2001 and covers similar ground to the first resolution. It calls on states to coordinate and cooperate against criminal misuse of information and communication technologies. The resolution calls for national law, policy and practice to combat computer crime[14].

The resolution of December 20, 2002[15], the third resolution, focuses on the creation of a global culture of cyber security. It notes the growing dependence of governments, businesses, other organizations and individual users on information technologies. The resolution notes that cyber security requirements increase as countries increase their participation in the information society. The resolution makes it clear that government and law enforcement cannot address cyber security alone without the support of all stakeholders.

The fourth resolution[16] also deals with the creation of a global culture of cyber security and the protection of critical information infrastructures. Issued on December 23, 2003, it states the growing reliance on information infrastructures by critical national services in areas such as energy generation, transmission and distribution, air and maritime transport, banking and financial services, water supply, food distribution and public health. The resolution invites all UN Member States to develop strategies for reducing risks to critical information infrastructures, in accordance with national laws and regulations.

The Disarmament and International Security Committee of the UN ("First Committee"), as one of the main committees of the UN that deals with international peace and security matters, also has jurisdiction over information security issues.[17] However, the First Committee's work faces certain challenges in trying to balance

[13] A/RES/55/63: Combating Criminal Use of Information and Communication Technologies

[14] A/RES/56/121: Combating Criminal Use of Information and Communication Technologies

[15] A/RES/57/239: Culture of Cybersecurity

[16] A/RES/58/199: Critical Infrastructure

[17] Eneken Tikk-Ringas, Developments in the Field of Information and Telecommunication in the Context of International Security: Work of

the different legal and political cultures of UN members. There are wide differences in the views of the states in terms of cyber security definitions, the scope of national security, perceived threats, and the appropriate role of the UN regarding international information security issues. For example, Russia's definition of international information security underlines the elimination of threats to both communication infrastructure and the information itself. On the other hand liberal democracies argue on freedom of expression grounds that concepts of security should not include the information itself, and that cyber security issues should be focused on the security of infrastructure and networks only.

The International Telecommunication Union ("ITU") is the UN's specialized international organization for information and communication technologies and it takes the lead in coordinating international efforts for cyber security, including by providing assistance and services to the UN's Member States. ITU also includes the private sector in its efforts. The governing legal texts of the ITU are adopted by the ITU Plenipotentiary Conference. In 2010, a Plenipotentiary Resolution[18] strengthened the authority of ITU on cyber security[19] and cyber-crime[20].

In 2007, ITU published the Global Cybersecurity Agenda ("GCA"). The GCA is a global framework for international cooperation[21] designed to increase public confidence and security in the use of information and communication technologies. It includes not only principles on legislation and international cooperation on cyber security but also technical and procedural measures, initiatives aimed at improving organizational structures to create warning systems and incident responses, and capacity building. These efforts are grounded in principle of international cooperation, including governments, industry and non-governmental organizations.

The executing arm of the ITU on cyber security issues is the International Multilateral Partnership against Cyber Threats ("IMPACT"). Through its Global Response Centre, based in Malaysia, IMPACT provides governments with access to facilities, industry experts and academics and other resources to improve their capabilities in dealing with cyber threats. It also provides emergency responses to identify cyber threats and share resources to assist Member States of the UN.

The Organization of Economic Co-operation and Development ("OECD") also focuses on the development of effective policies to maintain cyber security. The OECD publishes recommendations addressing governments and other stakeholders on policy making with respect to cyber security.[22] The Directorate for Science, Technology and Industry of OECD is mainly responsible for the matters regarding cyber security. The OECD Working Party on Information Security and Privacy mainly assists governments for developing national cyber security strategies.

3. The European Policy of Cyber Security

Below are the main strategic documents of the EU with respect to cyber security:

- The Strategy for a Secure Information Society[23]
- The Council Resolution of December 2009[24]
- The Electronic Communications Regulatory Framework[25]

the UN First Committee 1998-2012, ICT4Peace Publishing, Geneva, 2012.

[18] Gender mainstreaming in ITU and promotion of gender equality and the empowerment of women through information and communication technologies, Retrieved October 24, 2013, from http://www.itu.int/ITU-D/sis/Gender/Documents/Resolution_70_2010.pdf

[19] ITU defines cyber security as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: Availability; Integrity, which may include authenticity and non-repudiation; Confidentiality."

[20] The latest version of the Cybersecurity Guide for Developing Countries is available at http://www.itu.int/ITU-D/cyb/publications/index.html

[21] Nagpal, R., Cyber Terrorism in the Context of Globalisation, II World Congress on Informatics and Law, Madrid, 2002.

[22] Recommendation of the Council on Principles for Internet Policy Making, Retrieved October 24, 2013, from http://acts.oecd.org/Instruments/ShowInstrumentView.aspx?InstrumentID=270&InstrumentPID=275&Lang=en&Book=False

[23] Communıcatıon from the Commıssıon to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, Retrieved October 24, 2013, from http://ec.europa.eu/information_society/doc/com2006251.pdf

[24] Council Resolution of 18 December 2009 on a collaborative European approach to Network and Information Security, Retrieved October 24, 2013, from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:321:0001:0004:en:PDF

- The CIIP Action Plan[26]
- The Commission Communication on Critical Information Infrastructure Protection 'Achievements and next steps: towards global cyber security' adopted on 31 March 2011[27]
- Review of the Data Protection Legal Framework[28]
- European Strategy for Cyber Security[29]

In addition, the Cybercrime Convention[30] was adopted by the Committee of Ministers on November 8, 2001[31]. The Convention was the first international treaty addressing several categories of crimes committed via the Internet and other computer networks. The Convention aims to establish a "common criminal policy" through harmonizing national legislation, enhancing law enforcement and judicial capabilities, and improving international cooperation.

The Convention identifies cyber-crimes that should be prosecuted and gives directions for the investigation of such crimes. The problem of international cooperation is also addressed. The Convention mainly draws guidelines for signatory countries in their national legal frameworks for fighting cyber-crime. Chapter I of the Convention contains a brief definition of terms. Chapter II defines measures that are appropriate to the national level. Chapter II, Section 1 deals with substantive criminal law; Section 2 deals with procedural law; and Section 3 deals with jurisdiction.

In July 2013, the EU proposed a new Cybersecurity Directive that would require private companies to maintain a minimum level of infrastructure security or else face significant fines of up to two percent of global turnover.[32] Among many other initiatives, the directive will also require Member States to create national competent authorities (NCAs) responsible for network security risks and incidents and who would be notified in the event of any serious cyber security breach. Member States will also be required to establish a Computer Emergency Response Team (CERT) to deal with hacking and malware issues.

However, even if a common legal framework such as the Cybercrime Convention is significant to facilitate international cooperation for law enforcement bodies and the new EU directive will make serious strides toward European information security, a common understanding for defining and maintaining cyber security is still missing at the European level. Governments continue to have separate approaches in their domestic strategies, with different views on the role of the private sector, the balance between privacy and security, and the degree to which cyber security is considered part of national defense.[33] Governments' efforts to keep the borders of their local legislation and policies in place and to retain some control over their own national security measures and sovereignty, while struggling to reach international cooperation, contributes to this lack of cohesion. Moreover, the relatively slow pace at which standards must be introduced and negotiated between Member States makes it difficult for any cross-border harmonization initiatives to keep up with the rapid pace of technological change.

The EU's Cybersecurity Strategy is also criticized not only for providing vague and open-ended strategies but

[25] 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), Retrieved October 24, 2013, from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0021:EN:NOT

[26] The CIIP Action Plan, Retrieved October 24, 2013, from http://sta.jrc.ec.europa.eu/pdf/scni/ExperimentalPlatforms/1-CIIP_INFSO_WS%2020090619.pdf

[27] 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, Retrieved October 24, 2013, from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:EN:PDF

[28] Review of the data protection legal framework, Retrieved October 24, 2013, from http://ec.europa.eu/justice/newsroom/data-protection/opinion/090501_en.htm

[29] European Strategy for Cyber Security, Retrieved October 24, 2013, from http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/conference/cyber-exercise-conference/presentations/2.%20Conf%20Paris%20-June%202012-%20-%20A.%20RONNLUND%20-EC.pdf

[30] Convention on Cybercrime, Retrieved October 24, 2013, from http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

[31] Keyser, Mike. "Council of Europe Convention on Cybercrime", 2002

[32] EU Cybersecurity plan to protect open internet and online freedom and opportunity – Cyber Security strategy and Proposal for a Directive (July 2, 2013), Retrieved October 24, 2013, from http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

[33] Silva K, Europe's fragmented approach towards cyber security (October 10, 2003). http://policyreview.info/articles/analysis/europe%E2%80%99s-fragmented-approach-towards-cyber-security.

also for not properly protecting personal data.[34] European Data Protection Supervisor ("EDPS") Peter Hustinx published an official opinion on Security Policy on a Cyber Security Strategy of the EU. The opinion was highlighting the measures to procure a high level of network and information security across the EU. EDPS mainly found EU Cyber Security Strategy "regrettable" and that EU cyber security strategy does not emphasize privacy as a key part of any planned dealing with personal data.

4. National Cyber Security Strategy of the United States

As mentioned above, the United States was one of the first countries to recognize cyber security as a national strategic matter. In 2003, the US published the National Strategy to Secure Cyberspace[35] which was a part of the National Strategy for Homeland Security developed after 9/11.

The National Strategy to Secure Cyberspace emphasized the changes that technological developments have brought to business environments and the need to protect the cyber space[36] created as a result of these developments. The National Strategy to Secure Cyberspace provided a framework for protecting critical infrastructures which are stated to be crucial for American economy and security. Under the relevant document, critical infrastructures of public and private institutions are in the sectors of agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping.

The main goals of the strategy of 2003 were stated as:

- Preventing cyber-attacks against critical infrastructures
- Reducing national vulnerability to cyber attacks
- Minimizing damage and recovery time from cyber-attacks that do occur

The National Strategy to Secure Cyberspace of 2003 determines five priorities listed below:

- National Cyberspace Security Response System
- National Cyberspace Security Threat and Vulnerability Reduction Program
- National Cyberspace Security Awareness and Training Program
- Securing Governments' Cyberspace
- National Security and International Cyberspace Security Cooperation

The Cyberspace Policy Review is published[37] on May 29, 2009 following the issuance of the Comprehensive National Cybersecurity Initiative. The main goal of the Cyberspace Policy Review was generally assessing the policies of the US regarding cyber security matters. In 2011, US published Blueprint for a Secure Cyber Future[38] mainly focusing on protecting the critical information infrastructures and building a stronger cyber ecosystem.

Finally, in 2013, the National Institute of Standards and Technology, part of the US Department of Commerce, proposed draft voluntary standards for companies to improve the security of their information and networks.[39] The guidelines were requested by President Barack Obama after Congress failed to make progress on legislation to accomplish similar aims.

The US approach has some notable differences with the EU and several of its Member States. As a liberal state that emphasizes the role of private actors, national cyber security efforts of the US, first of all, underline the voluntary responsibilities of the private sector for maintaining cyber security. The voluntary nature of the guidelines issued in the US stands in stark contrast with the EU Directive that will issue requirements backed by

[34] Opinion of the European Data Protection Supervisor, Retrieved October 24, 2013, from https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2013/13-06-14_Cyber_security_EN.pdf

[35] The National Strategy to Cyberspace, Retrieved October 24, 2013, from http://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

[36] Under National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23) cyberspace is defined as the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.

[37] Cyberspace Policy Review, Retrieved October 24, 2013, from http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

[38] Blueprint for a Secure Cyber Future, Retrieved October 24, 2013, from http://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf

[39] Selyukj A, *U.S. proposes minimal corporate cyber security standards* (October 22, 2013) Retrieved October 24, 2013, from http://www.reuters.com/article/2013/10/22/net-us-usa-cybersecurity-standards-idUSBRE99L1LR20131022

heavy fines. The US's approach might lead to better relationships with data providers and corporations, whose cooperation they need to successfully combat cyber-crime. On the other hand, it may lack the teeth necessary to create sufficient security. The approach of EU is on the other hand more limited with the private sector which may lead to weaker cooperation but stronger safeguards.

The US cyber security strategy has also been roiled by recent disclosures and leaks. One of the most significant cases in the US regarding national cyber security is the WikiLeaks case, as it is commonly known. In 2010, WikiLeaks (www.wikileaks.org) published a video of US military personnel celebrating after a Baghdad airstrike of July 2007. After the video was published, the US military charged a soldier in connection with the leak of a classified video along with thousands of other documents that had been provided by him to WikiLeaks.[40] Army Specialist Bradley Manning was sentenced on August 21, 2013 to 35 years of imprisonment for the WikiLeaks disclosures.[41]

Both international organizations[42] and the press[43] criticized the decision and the conduct of US government with respect to WikiLeaks case for favoring an extreme national security understanding over freedom of information. More recently, the US has sought to extradite and charge Edward Snowden for leaking details of the US's e-mail monitoring programs run by the National Security Agency. Again, the difficulty in balancing freedom of information against national security interests is at the forefront of the debate, along with concern about the cooperation between the government and internet service providers with access to enormous amounts of private data. The NSA disclosures have been blamed for halting the progress of cyber security legislation in the US Congress and also affected efforts at international cooperation on cyber security by overshadowing talks between China and the US that were meant to improve cooperation.[44]

As demonstrated by the Snowden leaks, the US also requires the robust participation of the private sector with respect to national cyber security, and security agencies like the NSA have sought to use information provided by private companies to assist them. NSA is highly criticized for being too close to main leading Internet companies which are holding massive amount of user data and for reportedly collecting personal data directly from the servers of private companies[45]. The data mining program of the NSA, named PRISM, is reported by the press to tap directly into the servers of the main leading Internet companies. Following the accusations against the NSA, these leading companies have denied that NSA collects personal data directly from their servers.

Even though the US highlights freedom of information as one of the key elements for its cyber security strategies, the US government's reaction to the cyber leaks and its consequences overshadow this highlight and set a difficult example for other countries formulating their own strategies.

5. National Cyber Security Strategy of Turkey

The Information and Communications Technologies Authority ("ICTA") of Turkey is the authority for cyber security, information security and data privacy regulations in Turkey and it was founded in 2000. ICTA is the main regulatory and supervisory authority regarding all information and communications strategies in Turkey and it is the first sectorial regulatory body of Turkey. While policy making is the responsibility of Ministry of Transportation, Maritime Affairs and Communications, regulation power is given to ICTA.

ICTA is a member of IMPACT. Following the IMPACT membership, the timeline of maintaining a cyber-security strategy for Turkey was as follows:

- 25.02.2010 Representation of intention,
- 29.04 - 23.07.2010 Preparatory meetings with 23 participants,
- 01-31.08.2010 Working with focus groups,

[40] Loney, *Soldier charged over leaked video of attack*, Retrieved October 24, 2013, from http://www.reuters.com/article/2010/07/06/us-iraq-usa-journalists-idUSTRE6653FK20100706

[41] Sledge, *Bradley Manning Sentenced To 35 Years In Prison For WikiLeaks Disclosures*, Retrieved October 24, 2013, from http://www.huffingtonpost.com/2013/08/21/bradley-manning-sentenced_n_3787492.html

[42] Cohn, *The Bradley Manning Verdict and the Dangerous "Hacker Madness" Prosecution Strategy*, Retrieved October 24, 2013, from https://www.eff.org/deeplinks/2013/07/manning-verdict-and-hacker-madness-prosecution-strategy

[43] Gillmor, *The Bradley Manning verdict is still bad news for the press*, Retrieved October 24, 2013, from http://www.theguardian.com/commentisfree/2013/jul/30/bradley-manning-verdict-bad-news-for-journalists

[44] Blanchard, *China, U.S. talks on cyber security go well: Xinhua*, Retrieved October 24, 2013, from http://www.reuters.com/article/2013/07/10/us-china-usa-cyber-idUSBRE96904820130710

[45] Ferenstein, *Report: NSA Collects Data Directly From Servers Of Google, Apple, Microsoft, Facebook And More*, Retrieved October 24, 2013, from http://techcrunch.com/2013/06/06/report-nsa-collects-data-directly-from-servers-of-google-apple-microsoft-facebook-and-more/

- 11-13.01.2011 Final meetings with the participants,
- 19.01.2011 Finalization of the injections,
- 22-26.01.2011 Performing real attacks,
- 27-28.01.2011 National Cyberattack Exercise (“NCE”) Sessions.

Objectives of the NCE were raising awareness, increasing human capacity, detecting vulnerabilities, mitigating risks, improving intra and inter organizational cooperation in 2011. Forty-one public and private institutions attended the sessions. The NCE sessions revealed a lack of adequate and internationally harmonized regulations.

International cooperation is one of the ICTA’s aims. Therefore, following the decisions taken in 2011, ICTA started actively cooperating with European Counsel and ENISA on the regional level and with ITU on the international level. ICTA published reports regarding national and international dimensions of cyber security.[46]

As a governmental step for maintaining cyber security in Turkey, a decision regarding conducting, managing and coordinating national cyber security activities came into force on October 20, 2012[47]. On June 20, 2013, another decision on the national cyber security strategy and action plan for the years 2013-2014 came into force.[48] Under the decision of October 20, 2012, a Cyber Security Board was established in Turkey. The Cyber Security Board of Turkey is entitled to determine the governmental precautions regarding cyber security, to approve national cyber security strategies and procedures and principles within this scope and to maintain the national cyber security and coordination.

Following the decision of October 20, 2012, the National Cyber Security Strategy and Action Plan for 2013-2014 was published. The aim of this action plan is to maintain the security of the information and communication technology systems used by state institutions and organizations. Critical infrastructures are also defined under this action plan and it is clearly stated within the action plan that Cyber Security Board is authorized for insuring the security of critical infrastructures of public and private sectors. The Center for Intervention to National Cyber Incidents was established in accordance with the action plan. National Cyber Security Strategy and Action Plan for 2013-2014 is the first action plan of Turkey regarding national cyber security and the targets to be protected under this action plan are the public IT systems and critical IT infrastructures operated by both government and private sector. One of the key actions under the action plan was specified as amending the primary legislation by considering the needs of cyber security in Turkey and the deadline of such action is stated as September, 2013. There have not been significant amendments on primary legislation with respect to cyber security so far.

Building a solid cyber security strategy is also a crucial element for Turkey on the road to EU membership, as “Information Society and Media Chapter” also requires security of information. By entering into the EU information society, Turkey aims to liberalize electronic communication services and networks and to maintain a single market. The main EU acquis in information technologies was the "New Regulatory Framework" accepted by the Turkish government in 2002. The New Regulatory Framework both encourages liberalization of the IT sector and includes provisions with respect to cyber security. Thus provides a balance between these matters.

6. Conclusion

National cyber security strategies aim to protect the societies that became more dependent on cyber space against cyber-attacks. As explained above, international approaches through international organizations and individual solutions of the governments are two main options for policy making process to maintain cyber security. Cyber-crime is borderless and cyber-attacks may target users in any country making both unilateral and multilateral efforts important to a successful outcome.

States like the US that are more devoted to the freedom of information within their overall legal background and more inclined for liberal economy tend to regulate national cyber security by loading the major part of the responsibility on the private sector, so far on largely a voluntary basis. Moreover, they are inclined to regulate

[46] ICTA, Cyber Security Exercises of International Organizations, Ankara, 2009, Retrieved October 24, 2013, from http://www.cybersecurity.gov.tr/publications/uksgf.pdf and ICTA, Maintaining Cyber Security, Current Status of Turkey and the Measures to be Taken, Ankara 2009 http://www.cybersecurity.gov.tr/publications/sg.pdf

ICTA, Protection of Critical Infrastructures, Ankara 2010 http://www.cybersecurity.gov.tr/publications/CIP_Rapor.pdf

[47] Decision of the Council of Ministers Regarding Conducting, Managing and Coordinating National Cyber Security Activities of October 20, 2012, Retrieved October 24, 2013, from http://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18-1.pdf

[48] National Cyber Security Strategy and Action Plan of Turkey 2013-2014, Retrieved October 24, 2013, from http://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1-1.pdf

the security of the infrastructure rather than the information itself. However, the recent Wikileaks and Snowden disclosures have damaged the US's ability to be a leader on this issue, while underscoring the difficulty of balancing national security with freedom of information.

MLATs and other bilateral mechanisms have proven to be useful in several contexts, notably in criminal investigations. However, due to the slow progress of the cyber security investigations carried out by MLATs that lack clear timeframes when compared to the dynamic nature of cyber-attacks, more rapid and effective bilateral tools is necessary for cooperation of the governments, especially outside of traditional criminal investigations. Moreover, MLATs may have difficulty keeping up with the rapid pace of technological change and so may not always be sufficiently flexible.

In some cases the overall cyber security understanding of a state may not match the practice of cyber security at the multinational level, as is seen in the EU as it struggles to reach a common understanding about approaches to cyber security, even as it issues robust directives to boost the protection of information in the private sector. Even if the national cyber security strategies mentioned within this article are substantial steps to maintaining the cyber comfort of the states, (i) a common international understanding, (ii) compliance with the currently effective legislation, and (iii) proposals on substantial grounds are required to maintain the harmony of the cyber security legislation.

International cooperation of law enforcement agencies and international consensus and understanding on cyber security is essential for international cyber-crime investigations, despite the many challenges. It is necessary to harmonize legal instruments in between nations to ensure an international cooperation against cyber security threats. National and international tools which are suitable for the nature of the cyber-attacks should be developed. As stated within the article, cyber security has become one of the main security items of a government. Governments in the end should continue the dialogue and take transparent steps to balance the safety of personal information and freedom of information with national cyber security.

Copyrights