A Comparative Analysis of the National Cyber Security Strategies of Leading Nations

Ünal Tatar, Orhan Çalık, Minhac Çelik and Bilge Karabacak
Tubitak Bilgem Cyber Security Institute, Ankara, Turkey
unal.tatar@tubitak.gov.tr
orhan.calik@tubitak.gov.tr
minhac.celik@tubitak.gov.tr
bilge.karabacak@tubitak.gov.tr

Abstract: The rapid pace of technological developments in the area of information and communications technologies caused nations and peoples to be more reliant on cyber infrastructure to survive. Besides opportunities, the widespread use of information technology introduces new threats as well. Risks related to cyber security have started to threaten critical infrastructures, which are defined as assets that are essential for the functioning of a society and its economy. Cyber security has become one of the most serious national security concerns. In 2003 the United States was the first nation to prepare and publish a national cyber security strategy In the last ten years, 35 other nations have subsequently published their national cyber security strategy document. There are several aspects for national cyber security strategies. According to Luiijif and Healey (2012), there are five mandates of national cyber security: 1) Military cyber operations, 2) Counter cybercrime, 3) Intelligence/Counter intelligence, 4) Cyber security crisis management and critical infrastructure protection and 5) Internet governance and cyber diplomacy. In this study, the national cyber security strategies of France, Germany, The Netherlands, United Kingdom, United States and Turkey are examined and compared. Correlations between specific properties of the nation (economic power and political situation etc.) and focus and content of its cyber strategy were examined. The results of the study will provide guidance for nations that plan to prepare or update a national cyber security strategy.

Keywords: cyber strategy, strategic analysis, national security

1. Introduction

The widespread use of IT systems from personal objective to business functions made governments dependent on these systems. Next to the opportunities introduced by cyber infrastructure, risks sourced from this new domain evolved over time. While first cyber threats were based on jokes and fame-driven, in the last decade profit-driven hackers emerged and finally cyber is used by nations as a kind of military power. In order to cope with the challenges and risks of cyber domain and exploit its opportunities, nations consider cyber security as an inseparable part of national security and economic development. In this new era, nations prepare national cyber security strategies incorporated into national security strategies to protect themselves from risks and to exploit the opportunities of this new domain.

In the last decade, three important events occurred that triggered and accelerated national cyber security strategy preparation processes. Firstly, in 2007 cyber-attacks to Estonia's Internet infrastructure changed the paradigm about the impacts of a cyber-attack. During attacks on Estonia, the availability of systems run over Internet were interrupted for a period of time, mush of the national critical information infrastructures became unavailable. Russian hackers were blamed for the cyber-attacks. Secondly, in 2008, during the war between Russia and Georgia in South Ossetia, a cyber war had begun before the real one started. This is the first instance of use of cyber space during a real war as a force multiplier. Thirdly the last important event occurred in 2010, the use of the Stuxnet worm. Stuxnet was the first recognized cyber weapon that targets SCADA systems of critical information infrastructures directly. The Stuxnet worm infected systems in Iran's uranium enrichment facility at Natanz. Because of its technical complexity, experts believe that there is at least one nation state behind this worm. Iran blamed the United States and Israel. After the Stuxnet incident, in cyber space, not only hackers or non-state groups but also states become active offensive actors. When we examined the number of published national cyber security strategies, there is a notable increase after 2008 and 2010 (Figure 1).

In order to provide guidance for nations that plan to prepare or update a national cyber security strategy aguide inmto the leading nations compared five aspects: 1) Military cyber operations, 2) Counter cybercrime, 3) Intelligence/Counter intelligence, 4) Cyber security crisis management and critical infrastructure protection and 5) Internet governance and cyber diplomacy.

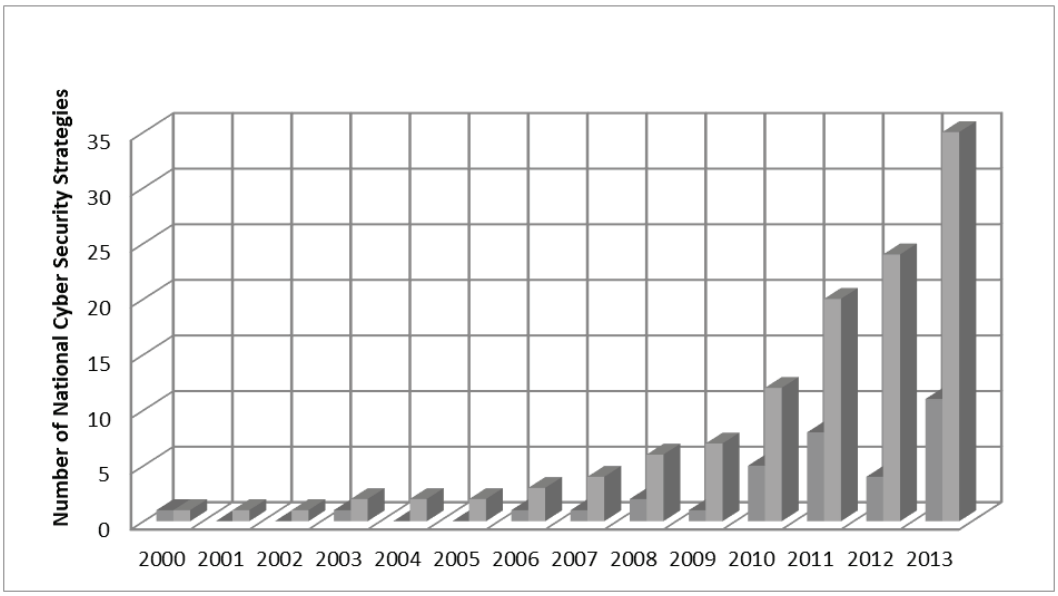

Figure 1: Number of national cyber security strategies (by year and cumulative)

In this study, cyber security strategies of 6 nations are chosen because of their specific features. The United States and the Netherlands are two nations which prepared two separate strategies for cyber security (for civilian aspects) and cyber defense (for military aspects). The United States and The United Kingdom are two states that prepared and updated their cyber security strategies. Along with others such as France and Germany are chosen since they have high rankings in GDP and ICT usage. Since Turkey is the last nation published its cyber security strategy, it is in the scope of this research.

2. Military perspectives towards cyber space

The security perception of militaries has undergone a fundamental change with the emergence of cyber threats in the last decades. As the dependency on internet technologies has been on rise, the vulnerability of networks and possibility of attacks targeting critical infrastructure have increased. This change pushed governments to re-adjust their threat perceptions and security mechanisms to confront cyber threats. In the last four years, the tendency of administrations to release cyber security strategies constitute main sources to interpret how the militaries consider cyber space and how they generate their cyber policies.

The weight attached to military perspective of cyber space in the strategy documents analyzed in this research differs widely in each country. In some countries, the main concern stemming from cyber space is dominated by military point of view, whereas in some focus is on other dimensions of cyber space for instance, fight against cyber crime.

It may be safely argued that military perspective took over the US cyber space strategy as the Washington administration have increasingly considered cyber threats among national security concerns. In the National Security Strategy, published by White House in 2010 'large scale cyber attacks' are counted as one of the threats US faces in addition to terrorism, natural disasters and pandemics with a special reference to their asymmetric character. Another point demonstrating US policy-makers' perception of cyber threats is the inclusion of digital infrastructure as a strategic asset that must be secured.

> *"Our digital infrastructure, therefore, is a strategic national asset, and protecting it—while safeguarding privacy and civil liberties—is a national security priority." (US National Security Strategy p.27, 2010)*

Large scale cyber attacks are not the only dimension of cyber threats. The opportunities offered by the Internet have been widely enjoyed by transnational terrorist groups that use cyber space not simply for propaganda, recruitment or basic hacking activities but also for stealing money to finance terrorist attacks and acquiring sensitive information about security. Defined as 'crime-terror' nexus, US National Security Strategy draws attention to terrorists' use of cyber space with its influence to undermine global confidence in the international financial system. (US National Security Strategy, 2010, p.49)

For more inquiry on US military perspective on cyber space, it would be useful to have a closer look at the Department of Defense (DoD) Cyber Security Strategy, partially publicized in 2011. At the very beginning of this document, it is stated that DoD treats cyber space as a operational domain 'to organize, train and equipped' (DoD. 2011) It may be interpreted from the document that the main reasoning lying behind the US military perspective of cyber space to view cyber threats as national security threats is the nation's critical infrastructure dependency on networks. Describing US critical infrastructure, DoD pointed at five services whose providers hold strategic importance for national security: Energy, banking and finance, transportation, communication and defense industrial base. (DoD 2011) It is significant to recognize critical infrastructures defined by DoD are mostly controlled by private sector. Since it is another discussion how to ensure security of networks owned by private sector, it is apparent a new structural organization between state and private sector ought to be built to remain delicate balance of security and privacy by respecting liberal values.

Although there is no mention about the institutional framework of cyber security policies in US strategy documents, it is worth noting the formation of US Cyber Command in 2010, a special unit in US Army's Strategic Command specializing on cyber threats. The formation of cyber command has launched another critical discussion on US cyber strategy: Does US adopt an offensive or defensive attitude in cyber space?

In land, air and naval forces, there may be much clearer divisions between offensive and defensive forces. However, drawing a clear-cut separation line between these two areas in cyber space is less likely. Although US cyber strategy documents have their core a defensive mission, there are some certain practices proving US have an 'active defense' understanding. Those who are of the opinion to base cyber strategy on a more offensive approach argue the higher costs of building resilience is one of the first factors that should motivate governments to choose offensive tools.

In Healey's (2012) words:

> *"Cyber defense is enormously expensive; it involves massive investment of financial and human resources to adapt organizations, technology and processes (and even basic human behavior traits) to comply with proper information security procedures."*

Underlining the cyber defense's obligatory character to contain offensive measures, Healey also imply simple defensive steps are not sufficient to ensure network security:

> *"In the late 1990's the US DoD made defense the clear priority, judging that their traditional military power could coerce any likely adversaries without the use of offensive capabilities. But if the DoD's own cyber systems were disrupted, all of those traditional military forces could be left deaf and blind." (Healey 2012.)*

In the US strategic documents, there have been no direct reference to offensive cyber capabilities but, in practice a number of evidences suggest Washington views cyber military instruments as an effective coercive asset to reach foreign policy goals. Although its diplomatic effectiveness is open to question, The Stuxnet incident has exhibited that cyber weapons could be used to attack strategic facilities. It should be also born in mind that American military strategy's transformation following the 9/11 has led American leaders to opt pre-emptive strikes which is highly possible in cyber war where attribution is difficult.

Doubtlessly, the US is not the only power seeking to utilize cyber capabilities to defend its networks in an offensive manner. The United Kingdom appears to become another superpower to favor offensive steps. While the 'UK Cyber Security Strategy' (The UK Cabinet Office. 2011.) prioritizes struggle against cyber crime to make the country the safest place for business, an economically-driven approach; British Ministry of Defense has tended to be equipped with offensive cyber tools.

As reports suggest, one major step toward active cyber defense for the UK is to cooperate with individual hackers, even if they were convicted. It is declared that Britain plans to recruit convicted computer hackers to a recently set up cyber defense unit, the Joint Cyber Reserve Unit (JCRU) which was announced by the UK government in September 2012. The Ministry of Defense has a 500-million pound initiative to recruit hundreds of reservists as computer experts to contribute country's defense alongside regular armed forces. The JCRU aims to reinforce national security by safeguarding computer networks and vital data, and it will also launch strikes in the case of cyberspace (The Guardian.2013).

3. Struggling against cyber crime

Cyber crime is a kind of criminal activity carried out by means of computers or the Internet (Oxford 2013). As in many areas of cyber space, there is not a satisfactory definition about the details. Therefore, cyber crimes may be categorized into two basic groups. The ones aiming to acquire private personal information mainly for stealing money through exploits and security breaches constitute the widespread cyber crime. In this group major part of cyber criminals concentrate on identity is theft and phishing. They can get passwords with the help of a malware that copy all key strokes and intervene financial interactions which really disturbs not only individual customers but also large corporations.

The second area in which more serious crimes have been conducted regards cyber attacks having specific institutional targets in order to suspend public services the institutions provide. DDoS and DoS attacks against governmental networks, can occur against institutions which are critical for people's daily life such as transportation, energy, and banking.

Fighting against cyber crimes is a multi-dimensional task. A wide range of networks, from military to universities, are the targets of cyber crimes. Each and every institution has its own concerns when it comes to cyber security. Due to the lack of a comprehensive approach in many countries and because of transnational character of cyber crimes, institutions have taken their own security measures to confront cyber crime. With the increase of cyber crime which pose a national threat, governments started to involve in fight against cyber crime. One of the first fields where private public cooperation is a deep requirement is struggle against cyber crime. Thus, governments' active support to private companies for ensuring cyber security is strategically important (Klimburg and Healey 2012). The first international treaty is the Budapest Convention by Council of Europe (or Convention on Cyber Crime) which seeks to harmonize national laws, upgrading investigative techniques and develop more cooperation for a more international and effective struggle against cyber crime (Council of Europe 2001).

The United Kingdom may be fairly defined as the country which puts considerably more effort to confront cyber crimes. The first and foremost purpose of British Cyber Security Strategy is to ensure business security. The first objective of economically driven-strategy is "Tackling cyber crime and making the UK one of the most secure places in the world to do business." In order to reach this goal, the document foresees some legal amendments, development of cyber capabilities and increase the law enforcement agency potential (The UK Cabinet Office 2011). The UK strategy contains three concrete steps for improving cyber security capabilities:

- Create a new national cyber crime capability as part of the new National Crime Agency by 2013
- Pursue the agenda defined at the recent London Conference on Cyberspace to establish internationally-agreed ‘rules of the road’ on the use of cyberspace
- By the end of 2011, build a single reporting system for citizens and small businesses to report cyber crime so that action can be taken and law enforcement agencies can establish the extent of cyber crime (including how it acts individuals and the economy).

For the aim of securing the cyber business environment, the British government allocated 28 million £ in 2011-2013 (Morse 2013).

Unlike the UK, the US has focused more on international cooperation in cyber crime mainly for its transnational character. Apart from immense efforts to create an international framework to prevent cyber crime, Washington administration has also worked to adjust its legal system with the rapidly evolving specialties and specifications of cyber crime. It is claimed that the total damage of cyber crime to American economy is an annual of 8,993 million$ (Ponemon Institute. 2013). The US has announced (The White House. 2011) its determination to wage an international war against cyber crime in its Cyber Security Strategy.

In German Cyber Security Strategy, it may be observed that cyber crime is not viewed as the most crucial topic. The struggle against cyber crime is one of the ten objectives listed at the end of the strategy document. Germany has held a more national perspective by aiming to hiring skilful staff to law enforcement units and creating platforms where Federal Office for Information Security work with private sector representatives. Despite, all these efforts it should be noted that struggle against cyber crimes does not stand at the focal point of German cyber strategy. They are simultaneously working for setting against cyber espionage and

intelligence exploitation. German government also expressed her willingness to work closely with international bodies including Council of Europe and United Nations particularly in information sharing (Bundesministerium des Innern, 2011). Germany ranks the second after the US in having highest cost caused by cyber crime with 5,950 million $ (Ponemon Institute 2012).

In one of the well-prepared national strategies examined in this study, the Netherlands seems to have a tendency to tackle the issue from a legal point of view. Regarding cyber crimes, the Dutch strategy has a special focus on generating compatible laws, advancing investigation techniques and some additional work to assist these steps. Upgrading law enforcement units' cyber capabilities to confront crimes in this is also among the measures the strategy document anticipates (The Dutch Ministry of Security and Justice 2011).

Attaching lesser importance to cyber crime, France considers the only step against cyber crime is to tighten legal measures. French cyber strategy outlook also includes international cooperation against cyber crime (French Network and Information Security Agency 2011).

Apart from broader precautions outlined in previous cyber security strategies, Turkey has some specific actions in order to stimulate an effective effort to prevent cyber crimes. For this purpose, setting essential standards on how to gather evidences in cyber crime incidents and getting the most advanced technological infrastructure are two prominent responsibilities of Interior Ministry and Ministry of Transportation, Maritime Affairs and Communication respectively. The Turkish government constructs its strategy on fight against cyber crime on keeping up to date records on incident. It may be maintained Turkish approach would create progress in outlining general characteristics of cyber criminals and be helpful to predict their next move (Turkish Ministry of Transport, Maritime Affairs and Communication, 2013).

4. Critical infrastructure protection and national crisis management

Among the five domains of cyber security, protection of critical infrastructure and national crisis management is the one which is likely to increase cyber security's strategic significance for national security. The topic of ensuring safety for critical infrastructure is actually a matter of national security with or without cyber. But, the networks operating in running critical infrastructures are not immune from growing dependencies of internet technologies. Therefore, one may advocate cyber security has been combined with the national security mostly with the critical infrastructure. Although the question of what are critical infrastructures varies for every states, the general definition suggested to be the providers of essential services of a country within a national security framework.

Furthermore, one of the tricky challenges of cyber security lies behind the fact that a remarkable part of critical infrastructures (CI) in liberal market economies are run by the private sector, not by state despite that they are deemed an integral part of national security. To enable private sector to offer more secure and sustainable services is tied to governmental assistance to these service providers (Klimburg and Healey 2012).

United States' decision makers in cyber security created a new institutional mechanism to protract information sharing between private and public stakeholders by establishing a new National CERT. This should be also implied on a global basis, for United States cyber strategy (The White House 2011). On national crisis management, another challenge emerges in cyber space regarding who has the authority of responding a cyber attack. In American case, it is the president who would decide to use a cyber weapon. However, the unprecedented rapidity of cyber attacks put pressure on decision making mechanisms. In the national strategies analyzed in this paper, none of them presents a proposal to overcome this imbroglio.

French Operational Center of the Security of Information Systems (COSSI) , France's main body for coordinating cyber security initiatives, has the main responsibility for national crisis management as well as preparing and implementing cyber crisis action plan. Underlining the crucial importance of critical infrastructure, French national strategy underscores the security measures regarding these facilities (French Network and Information Security Agency. 2011).

Following to struggle against cyber crime, the UK puts protection of CI's as the second important objective of cyber security strategy. It is aimed to boost public private partnership (PPP) and encourage both sides for further collaboration. To present the need of cooperation it is stated:

> *"Much of the infrastructure we need to protect is owned and operated by the private sector. The expertise and innovation required to keep pace with the threat will be business-driven" (The UK Cabinet Office 2011).*

As an indicator demonstrating the Dutch government's intention to have a comprehensive approach which contains all actors in the field of cyber security, in the Netherlands' cyber strategy document forming appropriate cooperation all national stakeholders and international actors is put among the essential principles (The Dutch Ministry of Security and Justice 2011). At this point, it is crucial to note the Dutch strategy incorporates international actors, either states or non-state ones, to a national security issue which is supposed to remain within national frameworks. Not going into details, this part of strategy seems to embark a constructive example in terms of building confidence building measures which are decisive for international cyber alliances.

The German strategy gives considerable more weight to protection of CI's in comparison with the other domains of cyber space. Berlin government has another detailed cyber security strategy which is readied specifically for CI protection. Three of ten steps in German cyber action plan is regarding directly CI's by pointing at the PPP as an obligation to reach these goals (Bundesministerium des Innern. 2011). In order to create an efficient crisis management in case of national cyber incidents, German National Cyber Security Council was established to coordinate between law enforcement units, Constitutional Court, intelligence agencies, Federal News Agency and some ministries.

As it was mentioned earlier, the definition and determination of CI differs on country's prosperities. Relatedly, Turkish government has chosen to determine the facilities providing critical services (Turkish Ministry of Transport, Maritime Affairs and Communication 2013). According to Turkey's cyber action plan conducting sectoral risk analysis of CI's, the public organizations responsible for regulating and auditing the critical sectors and generating sectoral emergency action and business continuity plans are given priority for CI protection. Turkey has also experienced significant progress in institutionalization in cyber security, as the country managed to form a national CERT (USOM) and expected to establish CERT's to specific sectors.

One critical point on Turkey's strategic approach about CI protection may stem from the exclusion of reactive sanctions while producing CI's cyber strategy. Whereas essential components of defensive cyber actions such as protect, detect, respond and recover can be found in CI protection strategy, instruments to deter any attack to these strategically important services should be implemented into legal framework.

5. Intelligence and counter-intelligence

The division between cyber-crime / cyber-theft and cyber espionage has not been clearly drawn yet. The controversy has also maintained in distinguishing military cyber activities, cyber crime and cyber espionage. What would happen, if a group of hackers with certain assistance of state A conducted cyber theft operation against networks of state B specifically aiming to acquire confidential information about state A's military secrets. Is this a cyber crime which leads to conviction of hackers, a military cyber activity or cyber espionage?

Let alone undefined grey areas, cyber espionage is the most threatening part of cyber security impinging on both private and public sectors. The large amount of stolen intellectual property has created problems for universities which pushed them to take additional security measures (The New York Times. 2013). Along with universities cyber espionage dominates the security agenda of states as well. The stolen information is not only a huge loss in terms of research and development but also a factor that strongly shake the credibility of the institution.

The US cyber strategy has not specifically mentioned cyber espionage. However, property rights, industrial espionage and whether protection of confidential data belong to business and the state are the issues found in strategy documents (The White House 2011). Furthermore, the cyber strategy of Department of Defense associates counter-espionage activities with the efforts of finding the identities of attackers, hackers. The difficulties of attribution in a cyber attack is assigned to specific cyber intelligence units (DoD. 2011).

British Defense Ministry along with the Security and Intelligence Agencies and Government Communications Headquarters (GCHQ) have a central role in exposing cyber threats and mitigate their risk. In a review of cyber

strategy exhibits the budget allocated to the agencies. The same report suggests 157 million £ is planned to spend on detection of threats (Morse. 2013).

Strengthening cyber espionage vulnerabilities is one of the first measures taken by the Dutch government. Developing technical capabilities will progress hand in hand with adjusting legal procedures in terms of cyber counter-espionage. The strategy document also call governmental institutions to work closely with each other in order to stand against cyber espionage activities, the ones resulted from abroad in particular (The Dutch Ministry of Security and Justice. 2011).

In German cyber security strategy, cyber espionage has a similar weight with the other strategies. A special part is given to this issue in the document (Bundesministerium des Innern. 2011).

Turkey's National Intelligence Agency (MIT) involves broadly in gathering evidence to resolve cyber incidents. However, there is no certain reference on how to counter espionage activities in cyber space in Turkey's strategy.

6. Cyber diplomacy and internet governance

Cyber Diplomacy also known as *public diplomacy 2.0,* is mainly about adopting technological innovations in communication and information technology to diplomacy (Melissen. 2007). It generally involves with public relations and has brought about a new dimension to traditional diplomacy by integrating new equipments which enable states to interact not only with their counterparts but also with the ordinary people in different countries. Probably due to cyber diplomacy's weak and loose connection with security issues, many strategy documents do not contain special part for cyber diplomacy.

States tend to recognize cyber diplomacy as a framework in which state-to-state communication and international cooperation on cyber issues are shaped. The Dutch cyber strategy underlines the need for inter-state cooperation and promises the Netherlands would actively participate in UN Forum of Internet Governance. Similarly, Germany underscores international cooperation and pledges to provide active assistance to organizations like, UN, NATO AND G-8.

In the global internet society, a set of mechanisms dealing with internet governance consists of civilian bodies including representatives from industry. The state's intervention to this structure is severely limited. Internet Architecture Board (IAB) and Internet Engineering Task Force (IETF) are two of the most influential institutions in terms of internet governance.

International Cyber Policy Unit is the UK's internet governance instrument which was formed under Foreign Secretary (Klimburg and Healey 2012). The British cyber strategy chiefly focuses on international cooperation to create a framework for international cyber law as well as on developing bilateral relations with powerful actor in cyber. London thinks the stepping of EU in cyber discussion more widely would spark more policy production in this issue. Instead of an international understanding like the UK, France insists of adjusting national legal framework with the latest cyber developments (French Network and Information Security Agency 2011).

The wording of the US cyber strategy "International Strategy for Cyber Space" itself indicates Washington views the cyber space as a domain which should be tackled internationally. Thus, cyber diplomacy is attached great importance for American cyber policy. As a clear demonstration of strategic change, the strategy document published in 2003 called "National Strategy to Secure Cyber Space." The US has assigned a decisive role in boosting cooperative ties among nations. It also highlights the preservation of freedom of speech, legal sanctions regarding internet governance in a liberal manner (The White House 2012).

7. Conclusion

In this study, cyber security strategies of 6 nations are chosen because of their specific features such as experience in cyber strategy making, economic power and publication date of strategy document. The results show that nations concentrated on several aspects in accordance with their current situation. Some nations focus on economic impact of cyber incidents and fight with cybercrime, some others concentrate on cyber as a

military force multiplier or preventing cyber-attacks against national critical information infrastructures and key resources to sustain its society.

Absence of widely adopted methodologies for evaluating the effectiveness of cyber strategies suggests that this new era of cyber security policy making is still in its early days (OECD 2012). For nations which will prepare or update a cyber-security strategy, it is recommended that to have a holistic view, define their priorities and focus more on the aspects of cyber security that are coherent with their national priorities. Another important point is considering not only the threats and risks in cyber space but also its opportunities.

References

Bundesministerium des Innern, (2011) "Cyber-Sicherheitsstrategie für Deutschland" [online] http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf?__blob=publicationFile access date: 10,28,2013

Council of Europe, (2001) "Convention on Cyber Crime", [Online] http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm access date: 10,21,2013

French Network and Information Security Agency, (2011) "Information Systems Defense and Security France's Strategy" [online] http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf access date: 10,20,2013

Healey J, (2012) "Lessons From Our Cyber Past: The First Military Cyber Units" [Online Transcript], (Washington DC: Atlantic Council) http://www.acus.org/event/lessons-our-cyber-past -first-military-cyber-units/transcripts access date: 10,17 ,2013

Klimburg, A. and Healey, J. (2012) "Strategic Goals & Stakeholders" in Alexander Klimburg (Ed.), National Cyber Security Framework Manual, NATO CCD COE Publication, Talinn

Luiijif, E. and Healey, J. (2012) "Organizational Structures & Considerations" in Alexander Klimburg (Ed.), National Cyber Security Framework Manual, Talinn, NATO CCD COE Publication,

Melissen, J. (2007) "The New Public Diplomacy: Soft Power in International Relations", New York, Palgrave Macmillan

Morse, A. (2013) "The UK Cyber Security Strategy: Landscape Review", National Audit Office, London Oxford University Press

OECD (2012), "Cybersecurity Policy Making at a Turning Point: Analyzing a New Generation of National Cybersecurity Strategies for the Internet Economy", [online] OECD Digital Economy Papers, No. 211, OECD Publishing http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf access date: 10,22,2013

Oxford Dictionaries, [Online] http://www.oxforddictionaries.com/definition/english/cybercrime?q=cyber+crime access date: 09,29,2013

Ponemon Institute (2012) "Cost of Cyber Crime Study: United States" [online] http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf access date: 10,26,2013.

The Dutch Ministry of Security and Justice (2011) "The National Cyber Security Strategy", The Hague. [online] https://www.enisa.europa.eu/media/news-items/dutch-cyber-security-strategy-2011 access date: 10,24,2013

The Guardian (2013) "Ex-hackers could be recruited to UK cyberdefence force", [online] http://www.theguardian.com/technology/2013/oct/22/uk-cyber-defence-force-ex-hackers-gchq access date: 10,27,2013

The New York Times (2013) "Universities Face a Rising Barrage of Cyber attacks" New York,

The UK Cabinet Office (2011) "The UK Cyber Security Strategy Protecting and promoting the UK in a digital world", [Online] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf access date: 10,29,2013

The White House (May 2010) "National Security Strategy" Washington, http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf access date: 09,23,2013

The White House, (July 2011) "International Strategy for Cyberspace, Prosperity, Security, and Openness in a Networked World" Washington, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf access date: 09,25,2013

Turkish Ministry of Transport (2013), Maritime Affairs and Communication, "National Cyber Security Strategy and Action Plan 2013-2014" Ankara [Online] http://www.ccdcoe.org/strategies/TUR_CyberSecurity.pdf access date: 10,27, 2013

US Department of Defense, Department of Defense Strategy for Operating in Cyberspace, July 2011, Washington http://www.defense.gov/news/d20110714cyber.pdf access date: 10,29,2013