Strategy Research Project
International Fellow

Cyber Security:
A Road Map for Turkey

by

Lieutenant Colonel Umit Kurt
Turkish Army

United States Army War College
Class of 2012

DISTRIBUTION STATEMENT: A
Approved for Public Release.
Distribution is Unlimited.

COPYRIGHT STATEMENT:
The author is not an employee of the United States government.
Therefore, this document may be protected by copyright law.

This manuscript is submitted in partial fulfillment of the requirements of the United States Army War College Diploma. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
19-03-2012	Strategy Research Project	

4. TITLE AND SUBTITLE

Cyber security: A Road Map for Turkey

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Lieutenant Colonel Umit Kurt

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Colonel Thomas Galvin
Department of Command, Leadership,
and Management

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution A: Approved for public release Distribution is Unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Cyber warfare is a form of information warfare, sometimes seen as analogous to conventional warfare, among a range of potential actors, including nation states, non-state groups, and a complex hybrid of conflict involving both state and non-state actors. Cyber warfare is a tool of national power, and countries are greatly improving their capabilities to conduct military operations in cyberspace. This is a domain where 'failure is not an option'. An entire nation's ability to operate and fight in the information age is vital toward survival. Nowadays, cyber warfare is mostly focused on economics which may be the shortcut to their victory. This strategic research project addresses the strategic-level issues related to cyber warfare, and describes the need for good national policies and strategies that are adequately resourced. It will focus on the case of the Republic of Turkey and the unique challenges facing that country in planning and implementing such a strategy. This paper will define cyber warfare, cyberspace and provide an analysis on the potential impact this threat could have on both the government and private sector. Finally, it will offer a recommended strategy for Turkey with recommendations for organizational structures and resource requirements.

15. SUBJECT TERMS

Warfare, Strategy

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFED	UNCLASSIFED	UNCLASSIFED	UNLIMITED	30	

USAWC STRATEGY RESEARCH PROJECT

CYBER SECURITY:
A ROAD MAP FOR TURKEY

by

Lieutenant Colonel Umit Kurt
Turkish Army

Colonel Thomas Galvin
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the United States Army War College Diploma. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Lieutenant Colonel Umit Kurt

TITLE: Cyber Security: A Road Map for Turkey

FORMAT: Strategy Research Project

DATE: 19 March 2012 WORD COUNT: 6,146 PAGES: 30

KEY TERMS: Warfare, Strategy

CLASSIFICATION: Unclassified

Cyber warfare is a form of information warfare, sometimes seen as analogous to conventional warfare, among a range of potential actors, including nation states, non-state groups, and a complex hybrid of conflict involving both state and non-state actors. Cyber warfare is a tool of national power, and countries are greatly improving their capabilities to conduct military operations in cyberspace. This is a domain where 'failure is not an option'. An entire nation's ability to operate and fight in the information age is vital toward survival. Nowadays, cyber warfare is mostly focused on economics which may be the shortcut to their victory. This strategic research project addresses the strategic-level issues related to cyber warfare, and describes the need for good national policies and strategies that are adequately resourced. It will focus on the case of the Republic of Turkey and the unique challenges facing that country in planning and implementing such a strategy. This paper will define cyber warfare, cyberspace and provide an analysis on the potential impact this threat could have on both the government and private sector. Finally, it will offer a recommended strategy for Turkey with recommendations for organizational structures and resource requirements.

CYBER SECURITY: A ROAD MAP FOR TURKEY

> When the Internet was designed, security was not a consideration. No one predicted that the new technology would become a global infrastructure that there would be incredible increase in speed, connectivity and the number of users (currently more than 2 billion). Rapid, unexpected growth combined with a too-rosy view of technological progress has led to some very real dangers. The absence of rules to govern international behavior in cyberspace compounds the problem. The effect of the new technologies is not dissolving borders but to shrink distance.
>
> —James Andrew Lewis[1]

The U.S. Department of Defense (DoD) states that "military, intelligence, and business operations all depend upon cyberspace for mission success."[2] This is also true for Turkey. Cyberspace is a new and challenging global domain, and it is imperative all nations keep cyberspace "safe, secure, and available for use."[3] This paper will provide a strategic direction for Turkey to meet this challenge.

Cyber warfare is a tool of national power, sometimes seen as analogous to conventional warfare, where the threats involve ranges of potential actors, including nation states, non-state groups, and complex hybrids of both state and non-state actors working together. "Over 120 nations are engaged in developing cyber warfare capability,"[4] demonstrating the degree to which nations recognize cyber warfare as one of the most vital national security challenges for today and in the future.

Yet not all nations have prioritized their cyber warfare efforts as they should, and risk being caught unprepared. For example, although Turkey approved cyber terrorism and other cyber threats in a formal list of threats to national security, it still has not created a national cyber security umbrella or incorporated this strategy as part of its anti-terror warfare policy.

This strategic research project addresses the strategic-level issues related to cyber warfare and describes the need for good national policies and strategies that are adequately resourced. It will focus on the case of the Republic of Turkey and the unique challenges facing that country in planning and implementing such a strategy. This paper will define cyber warfare, cyberspace and provide an analysis on the potential impact this threat could have on both the government and private sector. Finally, it will offer a recommended strategy for Turkey with recommendations for organizational structures and resource requirements.

What is What? Battlefield, Actors, Incidents

In cyberspace, the Internet 'battlefield,' actors, threats, and defensive and offensive strategies are similar among many countries. Yet, certain governments are more vulnerable to the threats in cyberspace. For example, why does it seem the U.S is more vulnerable than Turkey? The answer lies in the vulnerabilities in each nation and their level of dependence on cyber networks. To properly frame the issue, it is necessary to understand this elaborate threat environment, actors, their incidents-attacks and current strategies of the U.S. and Turkey.

A Man-made Global Domain. When former Deputy Secretary of Defense William J. Lynn declared cyberspace a "new domain" of warfare, on par with sea, air, land, and space, he knew that this new battlefield was totally different from the battlefields known at the time. Secretary Lynn defined cyberspace as,

> A man-made global domain within the information environment whose distinctive characteristic is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information using interdependent and interconnected information technology infrastructures including the Internet, telecommunications networks, computers systems, and embedded processor and controllers.[5]

Cyberspace has unique characteristics that make it different from the other domains. First, access to cyberspace is very cheap when compared with the other traditional domains. A network connection, a device compatible with this network, and a human are all that are required. All the actors can operate in the domain "with cheap technology and minimum investment."[6] Second, cyberspace is "a domain of technological commerce and communication, not a geographical chessboard."[7] There is no tangible theater of operations. Cyberspace presents a safe haven allowing actors to hide their identity and location "which makes it extremely difficult to attribute any hostile actions to a particular user or nation state."[8] Third, all actors in the global domain both individually and in groups can coordinate and execute cyber operations almost instantaneously. Fourth, this new domain is rapidly expanding and changing in comparison with the traditional ones. To achieve and most importantly sustain success in this battlefield, maintaining tactical and organizational agility and adaptation are a must. Finally, "cyberspace is now a battle space"[9] and it is not possible for any single player to control it completely. The real definition of success in this man-made global domain should be described as "effective use of domain rather than physical control of it."[10] The concept of cyber warfare within the cyberspace is a war against a faceless enemy.

Defining Cyber Warfare. The U.S. DoD defines information warfare as "actions taken to achieve information superiority by affecting an adversary`s information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems,

and computer-based networks."[11] This is the definition that will be used for the purpose of this paper.

Miller, Kuehl, and Lachov argue the targets of cyber warfare are civilian infrastructures as well as national security apparatus, as disrupting the adversary's civil society and inhibiting its military actions are both means of achieving the conflict's ultimate political objectives.[12] In his book *The Law of Cyber-Space,* Ahmad Kamal focuses on the financial aspects and claims that cyber warfare can occur between governments and non-state actors, but nevertheless be financed by states.[13] In *The Fog of Cyberwar: What are the Rules of Engagement?,* Larry Greenemeier describes the range of cyber warfare from a "fight against shadowy terrorist networks such as al-Qaeda to conflicts between uniformed national military forces."[14]

In addition to these, cyber warfare is relatively "cheap"[15], and like maneuver warfare, speed and agility matter most.[16] Cyber warfare as a form of information warfare is no longer an esoteric topic of interest to special groups of people with unique technical skills.[17] [18] Despite numerous cyber incidents, threats and actors are still in hidden in its grey void of state-financed warfare.

Threats and Actors of Cyberspace. In his recent article *Cyber weapons*, Ross M. Rustici states that over the last two decades "cyber threats have evolved from solitary hackers motivated by monetary gain and prestige to organized crime and state actors."[19]

Cyber security threats represent one of the most serious national security, public safety, and economic challenges nations face as victims. Threats are very changeable in time and depend upon the abilities of attackers and network capabilities. The threats

of cyberspace can be define in broad categories: cyber theft, cyber espionage, denial of service or distributed denial of service, collapse-sabotage, counterintelligence, hacking, worms, viruses and spam.[20] [21] It is clear that becoming more dependent upon networks makes nations vulnerable targets to a diverse number of "state and non-state actors who have greater access and operational maneuverability to conduct malicious activities"[22] across cyberspace.

The most desirous targets are critical networks, such as financial systems, power and other infrastructure, and government systems. These networks are politically vulnerable that "if interrupted for a while or perform erratically or intermittently would disrupt daily life."[23] These networks are also economically vulnerable in that they have integration with other networks in a redundant chain and this make loses bigger. P.W. Singer and Noah Shachtman argue that "the combination of online crime and espionage that`s gradually undermining the U.S. finances, know-how and entrepreneurial edge is the greatest national security danger."[24] In one instance, the 2009 Annual Threat Assessment of the Intelligence Community estimated cyber-related business losses to be 42 billion dollars for the United States, 140 billion dollars globally, and possibly 1 trillion dollars in intellectual property worldwide[25]. Attacks against them carry political and economic consequences and can be targets for politically motivated hacktivists or economically motivated hackers at the same time.

One of the most common targets for cyber actors is personal data, which a vital importance in every aspect. Cyber warriors and criminals alike can use stolen or hacked personal information to steal identities, seize bank accounts, or conduct fraud. From the perspective of global businesses, it is clear that this has a severe effect on national and

global economies. These are significant concerns for governments, businesses, and individuals in the ability to trust the economy and the safeguarding of their personal information.

Actors in cyberspace include both states and non-states, and they range from unsophisticated amateurs to highly trained professional cyber warriors. All actors in this domain have the ability to execute their attacks from anywhere, such as an office in New York City or a small house room in a village in Turkey. All that is required is a computer and a network connection. This is the capability which makes them unusual and dangerous enemies.

As James Andrew Lewis, a senior fellow and the Director of the Technology and Public Policy Program at the Center for Strategic and International Studies in Washington DC, pointed out that the central role in this domain is played by foreign actors and foreign governments. These "advanced state-sponsored actors have the skill and resources to overcome most defenses."[26] State and state-sponsored actors include national government agencies, state-sponsored white-hatted lawful hackers (Estonia-Cyber National Guard), hacktivists (hackers motivated by patriotism or ideology), patriotic hackers-constructors (the latter day pirates used so often by states like Chinese and Russia), "nation states` military and intelligence cyber-warfare units."[27] Hackers (thrill-seeking teenagers), criminal gangs, insiders-authorized users, spammers (financial backer of spam-spewing servers, bogus e-retailers, phishing schemes) are non-state actors.

Hackers and other individuals who "operate under the auspices and possibly the support of nation-state actors"[28] are the ones primarily responsible for these attacks. It

becomes clear that the most dangerous threat in this domain, as Daniel Gallington stated, are humans and insiders have an unique importance among this group, because they are the most lethal cyber security threats.[29] “Whether intentionally or unintentionally, authorized users often are guilty of spreading of viruses, exposing personal data and compromising private accounts.” said Sternstein Aliya, in his recent article *Dangerous Liaisons*. “In contrast, malevolent employees with legitimate access rights smuggle out sensitive data on removable USB drives to commit identify theft or espionage.”[30] Against this major threat, `reliable people` seem the only solution to build a reliable and effective cyber security system.

Incidents of Cyber Warfare-Is There Anyone Out There? Just as recent instances of stolen intellectual property such as the successful hacking of Google (Operation Aurora) and the WikiLeaks classified document disclosures of 2010 have shown, cyber threats both external and internal are “nearly impossible to prevent.”[31] Getting the details about cyber incidents is difficult. But, there are a lot of reports on a variety of cyber incidents against the vulnerabilities of governments, militaries, or individuals in the cyber domain. Several examples follow:

An excellent case of economically motivated cyber theft was the case of South Korean company SK Communications. In July 2011, SK announced “it had been the subject of a hack which resulted in the theft of the personal details of up to 35 million of its users.”[32]

In early 2011, U.S.-based computer security company McAfee, Inc. announced that someone, probably a Chinese hacker operating with external assistance, exfiltrated sensitive financial data related to oil and gas field exploration and operational details on

data acquisition systems from five undisclosed Western multinational companies. The operation, known as Night Dragon,[33] put these Western companies in positions of disadvantage against their Chinese competitors. This underlined how economically and politically motivated hackers can target not only the defense industrial base, government, and military computers, but global corporate and commercial targets. McAfee still has no direct evidence to name the originators of that attack so far.

Cyber incidents significantly increased the profile of cyber warfare.[34] Stuxnet has a unique status in all these cyber incidents that occurred so far. It is one of two large-scale successful sabotage efforts against infrastructure. Iran was attacked by the Stuxnet worm, thought to specifically target its Natanz nuclear enrichment facility *i*n September 2010. The worm was the most advanced piece of malware ever discovered. This intentionally designed malware directed against a nation-state resulted in the physical destruction of state-owned equipment. Gary D. Brown, in his article *Why Iran Didn`t Admit Stuxnet was an Attack* describes physical damage of the attack as "The centrifuges were destroyed as effectively as if someone had taken a hammer to them, and these were not just random bits of equipment."[35]

On November 9, 2011, the terrorist Kurdistan Workers' Party (PKK) attacked and brought down the Turkish Finance Ministry (www.maliye.gov.tr) website. They replaced the website with propaganda material. Ultimately, no taxpayer information was affected. It was a denial of service incident executed by a terrorist organization.

In January 2012, the Information and Communications Authority (ICTA), governmental institution responsible from coordination of cyber security efforts in

Turkey, was hacked itself. It was also a denial of service incident that executers not known.

Cyber Security: Challenges

Janczewski Lech and Colaric Andrew, in their book *Cyber Warfare and Cyber Terrorism,* describe cyber security as "the newest and most unique national security issue of the twenty-first century."[36] Cyber security, without international or public boundaries, has no easy "regulatory, behavioral or technological fix" as well. [37]

Cyber security is the sum of the attempts to secure our vulnerabilities against attacks/incidents of cyber attackers within cyberspace. In other words, cyber security is the sum of the attempts to secure our vulnerabilities against the faceless enemy. Do we know who they are or where they are? Which abilities and capabilities do they have? Their unpredictable techniques and tactics make them increasingly more and more sophisticated due to their nature within a man-made, boundless global battlefield.

There are too many unknowns. In such a foggy circumstance, the government or private sector has to deal with this huge challenge through several tactics—"new legislation, a push for international standards, public awareness campaigns and heightened surveillance."[38] To make this picture clear, nations need to pursue "a multi-layered cyber security approach"[39] to deter, prevent, detect, defend against and quickly recover from cyber threats coming from attackers not bound by normal legal and cultural restraints.

Cyber security is still mostly undefined territory and its doctrine far from mature. While trying to achieve multi-layered cyber security, nations must overcome some basic challenges. These are global and directly affect national cyber security policies.

What is a Cyber Attack, and How is it Distinguished from Exploitation? Security is the sum of measures taken against defined threats. Most conventional threats are well-defined in national or international law. But unfortunately in cyberspace, there isn't consensus on the definition of a cyber attack. For example, what is the difference between a cyber exploit and a cyber attack? Many believe the difference between an exploit and an attack is about whether a malicious incident in this domain is equivalent to the use of force, to an attack using conventional weapons.

But, “There is no international agreement on what constitutes an act of cyber war.” said Jeffrey Carr stated in his book *Inside the Cyber Warfare.*[40] The United States sees that this is a problem and has been leading the effort to gain common definitions. But they have not been alone. The Council of Europe declared a convention on cyber crime in 2001. The Council of Europe’s Convention on Cybercrime (ETS No.185, 2001)[41] has just “addressed the procedural laws in the signatory countries for investigating cybercrime.”[42] Today it may be considered as a cornerstone or a good starting point for international law of cyber. However, there are two hurdles to overcome. First, this Convention does not “go beyond the basic necessities for solving identity theft or protecting intellectual property.”[43] Second, it only has support of 32 signatory countries. There are 15 additional countries, including Turkey, which have signed the convention but thus far have not implemented its provisions.

The situation in Estonia in 2007 was a good example of this challenge. In April 2007, Estonia was attacked by Russian-financed hacktivists in retaliation for the relocation of the Bronze Soldier of Tallinn.[44] There were a series of coordinated denial of service attacks against vulnerable targets, including major government institutions,

media organizations, and financial websites. Estonia contacted the North Atlantic Treaty Organization (NATO) to ask for support by operation of NATO's Article 5, but was rebuffed.[45] For NATO, an attack would trigger a potential self-defense response by the Alliance and this cyber incident did not meet their threshold of an attack of war.[46] Although some tend to call incidents such as these attacks, NATO's rebuff showed that no matter how malicious an action was, if there was "no damage, death or destruction"[47] it would not be considered as an armed attack.

Only three cyber incidents could meet this standard of an equivalent to armed attack. First was the Stuxnet virus, which destroyed equipment in an Iranian nuclear facility. Second was the reported blackout in Brazil. Third was Israel`s alleged disruption of Syrian air defenses in 2007 during a raid on a suspected nuclear facility.[48] At this point, everything else can be qualified as crime or espionage.

Accountability: who is outside? Accountability is the second major challenge in cyber security. The structural anonymity of cyberspace allows "masking both perpetrator and motive."[49] It's not easy to detect what or who is responsible for incidents or attacks, because it is practically very difficult to track the point of attack as various IPs are being used as cover.

In addition to this, sometimes victims may not even know when they were attacked. For example, in the Stuxnet case, the Iranians were unaware that they were under attack, and several months later still have not determined the source of the worm.[50] In the Night Dragon case, McAfee has no direct evidence to name the originators of these attacks but said they had "strong evidence suggesting that the attackers were based in China."[51] That was all they could determine.

On the other hand there is a second dilemma that if there is no definite evidence about a government that is the attacker, then should one still hold this government to account for the hackers from in their midst who attack another country?

Security vs, Freedom Dilemma: Cannot Hit the Kill Switch. Exercising cyber security must be done in a way that respects legitimate use of the Internet, which sometimes can be a significant constraint. Free and easy flow of information was the underlying idea behind the Internet. The security of this information was not such a big deal at the beginning. Today, every effort to secure the information complicates information sharing. The balance between the connecting people and protecting people is of vital importance. The Council of Europe's Convention on Cybercrime, a positive effort to create a voluntary-based international strategy for cyber security, serves this purpose and "promotes free flow of information while simultaneously preventing free dissemination of intellectual property through norms of responsible behavior"[52] by blocking unauthorized access to networks. It is not so easy to balance these two imperatives. Maybe really "there is only one way to block all authorized access" Aliya Sternstein said "is to do the very thing that freedom-loving people fear the most-hit the kill switch."[53]

Strategies for Cyber Security

All the above challenges should be taken into consideration while nations develop their cyber security strategies and design their cyber security infrastructures. These are not easy to develop because this type of security strategy is so new.

The U.S is a pioneer on this issue, so their approaches and lessons learned are important. As President Obama stressed in his speech on national cyber security May 29, 2009;

> Hardening digital infrastructure to be more resistant to penetration and disruption; improving nation`s ability to defend against sophisticated and agile cyber threats; and recovering quickly from cyber incidents are the essentials to improve resilience to cyber incidents while seeking to reduce threats by working with allies on international norms of acceptable behavior in cyberspace, strengthening law enforcement capabilities against cybercrime, and deterring potential adversaries from taking advantage of our remaining vulnerabilities reducing are essentials to reduce the threat.[54]

For these purposes, the U.S. government released two national strategies for operating in cyber space.

The U.S. released its International Strategy for Cyberspace (ISC) in May 2011. The goal of the U.S. describe in this policy document as “to promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation."[55] The document states that “first of all nations has inherent right to self-defense, DoD's strategy is actually defensive in nature, but reserve the right to use all necessary means - diplomatic, informational, military, and economic -, the U.S. military power will be used if necessary.”[56] As laid out in specific policies in pages 18-23 in the ISC, the U.S. seeks to strengthen national infrastructure against cyber attacks, achieve agreements on international norms of acceptable behavior in cyberspace, and strengthen law enforcement capabilities against cybercrime. The goal of the U.S. cyber security strategy is a reliable, resilient, trustworthy digital infrastructure to operate effectively in cyberspace, defend national interests, and achieve national security objectives.[57] The necessary measures have to be taken to ensure to this end state are to improve resilience to cyber incidents and reduce cyber threats.

In its July 2011 Defense Strategy for Operating in Cyberspace (DSOC), the DoD designed five strategic initiatives to provide a roadmap for implementation of the national strategy: [58]

- Taking cyberspace as an operational domain; creating and use new defense operating concepts to protect DoD networks and systems,[59]
- Being partner with other U.S. government departments and agencies and the private sector to enable a whole-of-government cyber security strategy,[60]
- Building strong relationships with U.S. allies and international partners to strengthen collective cyber security[61], and
- Leveraging the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation.[62]

Both 2011 strategies address the inherent challenge of cyberspace. However, they did not clearly define cyber attacks. Nor do they specify how the U.S. will respond to such attacks. Even so, the U.S. has taken a leading role in international cyber security issues, as it did in the Council of Europe's 2001 Convention on Cybercrime in Budapest.[63] But the disparities among national laws and regulations are inhibiting a unified, collective approach to creating a safe, secure, and strong cyberspace. So for now, nations must cope with the domain's challenges and create and implement cyber security strategies alone.

As of March 2012, Turkey has neither officially established a national cyber security strategy nor founded an institution responsible to implement it or coordinate all cyber security efforts in public and private sectors the way the U.S. has. It is now

imperative that Turkey does so, and the nation must immediately start with identifying responsible institutions and updating its laws.

Perhaps before formulating her cyber security strategy, Turkey needs an accurate and objective self assessment, to know where to start and what to do first, and identify what and where Turkey's cyber vulnerabilities are. [64]

Turkey can only properly secure her digital environment by working with international partners. Turkey should strengthen its international partnership on a range of issues "such as laws concerning the investigation and prosecution of cybercrime; data preservation, protection, and privacy; and approaches for network defense and response to cyber attacks on cyber domain"[65] and act together with her allies on a host of issues, especially use of force and sovereign responsibility. The government should work with national-public and private- and international partners to promote responsible behavior and deny those who would try to harm digital infrastructure, dissuade and deter malicious actors, and be ready to defend these vital national assets.

Turkey is too small a nation to have an offensive cyber policy, and she has no reason to attack anyone. It is much more feasible for Turkey to develop a defensive policy to counter cyber attacks than to focus on offensive cyber attack and exploitation strategies. At least for now, Turkey's priority should be update and develop a defensive cyber security strategy against the real threats today.

In this defensive cyber security strategy, the Turkish government's Ministry of Transportation (MOT) should take the leading role, co working with key public and private players and military, and design an effective umbrella mechanism to achieve "a true common operating picture that integrates information from the government and the

private sector and serves as the basis for informed and prioritized vulnerability mitigation efforts and incident response decisions."[66]

Institutions for Cyber Security

With the overall lead agency for cyber security identified in Turkey, the next step is to determine the support role that the Turkish military might play. Again, the U.S. provides a useful example on how to do it. As will be evident, the military will require its own institution to protect defense-related networks and coordinate national efforts with MOT.

The United States divides principal responsibility for cyber security between the DoD and Department of Homeland Security (DHS). Upon an important security failure of DoD networks in November 2008, on June 23, 2009, former U.S. Secretary of Defense Robert M. Gates directed the Commander of U.S. Strategic Command (USSTRATCOM) to establish U.S. Cyber Command (USCYBERCOM) to integrate its cyber defense operations across the military.[67] [68] It inaugurated USCYBERCOM in May 2010.[69]

CYBERCOM's active defenses only fully protect networks in the government's *dot mil* domain. Protection of digital infrastructure at non-military departments falls under the aegis of DHS, primarily at the National Cyber Security and Communications Integration Center. The center also houses the U.S. Computer Emergency Readiness Team. This group defends against cyber attacks within the *dot gov* domain and is responsible for security collaborations with government and private industry. Included in these relationships are public-private partnerships with the owner/operators of strategic national assets.

When one reviews Turkey from this institutional perspective, one can see the need for coordinated individual cyber security efforts. At the institutional base, Information and Communication Technologies Authority (ICTA), Turkish General Staff, ASELSAN (Turkey`s top defense company), HAVELSAN (a Turkish defense software company), and TUBITAK (Turkey's government`s scientific research institute) are dealing with cyber and cyber security issues separately. There is an ongoing effort to join all these individual efforts under a governmental umbrella since late of 2008.

Today, ICTA, akin to The National Institute of Standards and Technology (NIST), is working in cooperation with related national and international partners to increase the cyber security capacity and capability of Turkey since 2004. As a member of International Multilateral Partnership Against Cyber-Threats (IMPACT) Organization, ICTA gives training on Cyber Security Studies to the authority of the countries including Azerbaijan, Albania, Bosnia and Herzegovina, Georgia, Kazakhstani, Kyrgyzstan, Kosovo, Egypt, Mongolia, Sudan, Tajikistan, Turkmenistan.

The government agencies, military institutions and private sector in Turkey use individual solutions against cyber attacks. For example, today most government agencies rely on foreign solutions, while the Turkish General Staff (TGS) and National Intelligence Agency (MIT) use local cyber security solutions developed by HAVELSAN.[70] Furthermore, TUBITAK presents local "crypto solutions"[71] to all government agencies, military institutions and private sectors.

Although especially strategic government agencies increase their current level of security against cyber attacks, it is clear that these individual solutions do not provide sufficient solution for the takers. These individual efforts must be supported to invest

better cyber defense solutions. Therefore Turkey needs “a national coordination body”[72] to coordinate all these individual cyber security efforts under a national office that may include different governmental institutions including a CYBERCOM also.

Turkey is set to coordinate its various individual efforts in order to build a national cyber security umbrella as part of its anti-terror warfare, including efforts to set up a national office to boost security at strategic government agencies, nationalize some of the firewalls used in others and provide national solutions in general.[73]

The cyber security organizational structure of Turkey should comprise four core institutions. They can have different command and control and institutional relations in accordance with the chosen organizational structure. These four institutions should be:

The first is the Cyber Defense Foundation (CDF) should be established under the aegis of overall lead agency as a coordination office to bring and coordinate all individual efforts under a national cyber security umbrella.

Second is the Cyber National Guard Team, a government funded, white-hatted hacker organization under the aegis of the CDF. This team would include cyber security experts for protection of digital infrastructure at non-military government institutions. The Foundation should defend the Turkish public *.gov.tr* domain against cyber attacks and also be responsible for security collaborations with government and private industry. Included in these relationships are public-private partnerships with the owner/operators of strategic national assets. Turkish universities would launch postgraduate courses and education programs to produce the necessary human resources for future efforts. The National Cyber Security Coordination Foundation (USGKK), the country's first civil cyber

defense agency, is a newly established governmental institution that can carry out this mission.

Third is the Operational Test Teams from within all the government agencies. These would operate under the aegis of overall lead agency and should be established by the cyber security experts from the related governmental institutions such as the Ministries Turkish defense contractors and agencies, and law enforcement to actively probe Turkey`s cyber infrastructure, both public and private, especially *.gov.tr* and internal secure systems, as well as Turkey`s Internet nodes and service providers to identify vulnerabilities and mitigate risks. ICTA can carry out after relevant changes on its current structure in accordance with its new mission.

The fourth institution would be a military command modeled on the U.S. Cyber Command. 'Turkey's CYBERCOM' would probably be a "two- or three-star Cyber Command at the office of the General Staff."[74] The military would require its own institution to protect its own networks in the .mil.tr domain and establishing a single chain of command running up to the Chief of General Staff; and working to share all information and help to coordinate responses with the overall lead agency for cyber security.

CYBERCOM must have representatives from all services including gendarmerie and a direct coordination authority with an overall lead agency for cyber security. Being directly under TGS`s chain of command is not the only option for the Turkish CYBERCOM. The Turkish CYBERCOM can carry out all of its responsibilities under the aegis of MOD as a new and independent service under command of a four star general.

Cyber Security: Organizational Structures

We try to underline the necessities of the organizational structure of cyber security for Turkey. With these four core institutions, Turkey has three courses of actions to make its decision about cyber security structure of own. These courses of actions were established by military perspective.

The first course of action (COA 1) would have the MOT as the overall lead agency with a two or three star led CYBERCOM under direct supervision of the TGS chain of command. CYBERCOM would have direct coordination authority with MOT. CDF, therefore, is the coordination office under the MOT. USGKK would serve as the Cyber National Guard Team. ICTA would serve as an Operational Test Team under the aegis of MOT, and CYBERCOM would have representatives under the aegis of MOT.

COA 2 would be a military-centered construct with the TGS as the overall lead agency with a four star led CYBERCOM serving dual-hatted as both the CDF and in its original role within the TGS chain of command. USGKK would serve under the aegis of CYBERCOM while ICTA be the test team under the TGS.

COA 3 would have the MOT as the overall lead agency with a two or three star led CYBERCOM as a new service under the aegis of the Ministry of Defense and with direct coordination authority with the TGS. Roles of the CDF, USGKK, and ICTA otherwise do not change.

In COA 2, TGS takes the overall responsibility of Turkey`s cyber security alone. In the unity of command perspective maybe it seems a good option but it is not so easy to fulfill Turkey’s overall cyber security necessities by TGS alone. Even if this option can be seen as acceptable and suitable, this new endless domain needs close coordination and well organized and unified efforts against faceless enemies. In that respect, this

option has feasibility problems. On the other hand, giving overall cyber security coordination to CYBERCOM in addition to its inherent cyber security responsibilities has great risk. With the challenges of risk and feasibility problem, this COA is not preferred but still could be done.

COA 3 creates the problem of civilian authority over a military institution in a new capacity. This option has some acceptability difficulties in today`s bureaucracy of Turkey, because TGS is directly under the aegis of Prime Minister and not the MOD. While this resembles current U.S practices, it requires additional changes in military bureaucracy in Turkey to be implemented.

COA 1 seems the best COA in terms of feasibility, acceptability, suitability and risk. It meets the necessities of cyber space and spreads the responsibility between institutions. It is also suitable for today`s bureaucracy of Turkey.

Conclusion

Turkey is one of the countries who recognized the importance and danger of cyber space very early. With its developing globally-interconnected digital information and communications infrastructure, Turkey aware of cyber security risks can cause serious economic and national security challenges of today.

Turkey knows that she cannot succeed in securing her cyberspace without coordination and collaboration with her public and private sectors' institution and also with her allies.

Again, Turkey is too small a nation to have an offensive cyber policy, so it is much more feasible for Turkey to develop a defensive policy to counter cyber attacks than to focus on offensive cyber attack and exploitation strategies. At least for now,

Turkey's priority should be update and develop a defensive cyber security strategy against the real threats today.

What Turkey needs today is to design an effective umbrella mechanism to bring and coordinate all individual cyber security efforts to establish her national cyber security architecture. This architecture under the coordination of MOT should have quadruple mechanism with the Ministry of Transportation in the lead with the ICTA as its Operational Test Team and a Cyber Defense Foundation under the MOT as the coordination office supervising the Cyber National Guard Team. Finally, the military would establish CYBERCOM under the command of a two or three star general. CYBERCOM would be directly under TGS`s chain of command, would have direct coordination authority with MOT, and would have representatives from all services including gendarmerie. This course of action is suitable and feasible, and would foster the necessary efforts to protect the Turkish national information infrastructure from today's and tomorrow's cyberspace threats.

Endnotes

[1] James Andrew Lewis, "The Threat", *Government Executive* 43, no.10 (August 15, 2011): 20.

[2] U.S. Department of Defense, *Strategy For Operating in Cyberspace,* July 2011, 13.

[3] Darryl S. Shaw, *Cyberspace: What Senior Military Leaders Need to Know*, Strategy Research Project (Carlisle Barracks, PA: U.S. Army War College, March 18, 2010), 1.

[4] Jeffry Carr, *Inside Cyber Warfare* (Sebastopol,CA: O'Reilly, December 2009), 161.

[5] William J. Lynn III, "Defending a New Domain", *Foreign Affairs 89,* no.5 (September 2010 - October 2010): 97.

[6] Timothy K. Buenneyemer, "A Strategic Approach to Network Defense: Framing the Cloud", *Parameters* XLI, no. 3 (Autumn 2011): 43.

[7] P.W Singer and Noah Shachtman, “The Wrong War”, *Government Executive*, no. 43.10 (August 15, 2011): 32.

[8] Darrly S. Shaw, *Cyberspace : What Senior Military Leaders Need to Know*, 4.

[9] Robert A Miller, Daniel T. Kuehl,and Irving Lachow**,** “Cyber War: Issues in Attack and Defense”, *JFQ*, no. 61 (2nd quarter 2011): 20.

[10] Ibid.

[11] Charles G.Billo and Welton Chang, “Cyber Warfare”*,* November 2004, http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf (accessed November 29, 2011).

[12] Miller, Kuehl and Lachov **,** “Cyber War:” 19.

[13] Haly Laasme**,** “Estonia: Cyber Window into the Future of NATO”, *JFQ*, no. 63 (4th quarter 2011): 58-59.

[14] Larry Greenemeier, “The Fog of Cyberwar”, 13 June 2011, http://www.scientificamerican.com/article.cfm?id=fog-of-cyber-warfare (accessed November 29, 2011).

[15] Lewis, “The Threat”, 20.

[16] Lynn, “Defending a New Domain”, 97.

[17] Ronald Bailey, “Cyber war is Harder than It Looks”*, Reason 43*, no. 1 (May 2011): 50.

[18] Brian R.Salmons, “Review essay for Cyberwar and Cyberdeterence Book”, *JFQ*, no. 63 (4th Quarter 2011): 151.

[19] Ross M. Rustici, “Cyberweapons: Leveling the International Playing Field”, *Parameters*, volume XLI, no. 3 (Autumn 2011): 32.

[20] Carr, Inside Cyber Warfare, 4.

[21] Tarek Saadawi and Louis Jordan, eds., *Cyber Infrastructure Protection* (Carlisle Barracks, PA: U.S. Army War College, May 2011),v.

[22] John A. Mowchan, “Don`t Draw the Red Line”, *Proceedings 137,* no.10/1304 (October 2011): 17.

[23] Billo and Chang, “Cyber Warfare”, 18.

[24] Singer and Shachtman, “The Wrong War”, 34.

[25] Ibid.

[26] Lewis, “The Threat”, 17.

[27] Singer and Shachtman, “The Wrong War”, 32.

[28] Billo and Chang, “Cyber Warfare”, 3.

[29] Daniel Gallington, “The Challenge”, *Government Executive 43*, no.10 (August 15, 2011): 22.

[30] Aliya Sternstein, “Dangerous Liaisons”, *Government Executive 43*, no.10 (August 15, 2011): 12.

[31] *McAfee Home Page,“ Global Energy Cyberattacks: Night Dragon”,* http://www.mcafee.com (accessed November 22, 2011).

[32] *Command Five Home Page*, http://www.commandfive.com/papers/C5_APT_SKHack.pdf (accessed January 3, 2012).

[33] Mowchan, “Don`t Draw the Red Line”, 17.

[34] Gary D Brown.**,** “Why Iran Didn`t Admit Stuxnet was an Attack”, *JFQ*, no. 63 (4th quarter 2011): 71.

[35] Ibid.

[36] Lech J. Janczewski and Andrew M. Colaric, *Cyber Warfare and Cyber Terrorism,* (Hersey, NY: Information Science Reference, 2008), x.

[37] Sternstein, “Dangerous Liaisons”, 10.

[38] Ibid.

[39] Laura Mather, “Comment: Cybersecurity requires a multi-layered approach**.”** April 21, 2011, http://www.infosecurity-magazine.com/view/17542/comment-cybersecurity-requires-a-multilayered-approach, (accessed February 12, 2012).

[40] Jeffry, *Inside Cyber Warfare,*1.

[41] *Convention Committee On Cybercrime (T-CY) Home Page*, http://www.conventions.coe.int/treaty/en/treaties/html/185.htm (accessed February 12, 2012).

[42] Laasme**,** “Estonia:” 60.

[43] Ibid.

[44] Stuart Malawer*, “*Cyberwarfare: Law & Policy Proposals for U.S. & Global Governance”*,* February, 2010, http://www.ssrn.com/abstract=1437002 (accessed November 23, 2011).

[45] Article 5 of the Washington Treaty: The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defense recognized by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.

Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security.

[46] Brown**,** "Why Iran Didn`t Admit Stuxnet was an Attack", 71.

[47] Lewis, "The Threat", 18.

[48] Ibid.

[49] Mowchan, "Don`t Draw the Red Line", 18.

[50] Singer and Shachtman, "The Wrong War", 32.

[51] *McAfee Home Page," Global Energy Cyberattacks: Night Dragon",* http://www.mcafee.com (accessed November 22, 2011).

[52] Sternstein, "Dangerous Liaisons", 12.

[53] Ibid.

[54] Barrack Obama, "Remarks by the President on Securing our Nation's Cyber Infrastructure," May 29, 2009, http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure (accessed November 11, 2011).

[55] US Department of Defense, *International Strategy for Cyberspace,* May 2011, 8.

[56] Ibid., 14.

[57] Ibid., 4.

[58] US Department of Defense, *Strategy for Operating in Cyberspace,* July 2011, 13.

[59] Ibid., 5.

[60] Ibid., 8.

[61] Ibid., 9.

[62] Ibid., 10.

[63] *US Department of State Home Page,* http://www.state.gov/s/l/2004/78080.htm (accessed March 13, 2012).

[64] Gallington, "The Challenge" 26.

[65] Executive Office of the President, Cyberspace Policy Review (Washington, DC: Executive Office of the President, 2009), http://www.whitehouse.gov/cybersecurity, (accessed November 23, 2011).

[66] Ibid.

[67] US Department of Defense, *U.S. Cyber Command Fact Sheet,* 25 May 2010 http://www.defense.gov/home/features/2010/0410_cybersec (accessed November 1, 2011).

[68] Jonathan Masters, "Confronting the Cyber Threat", May 23, 2011, http://www.cfr.org/technology-and-foreign-policy/confronting-cyber-threat/p15577 (accessed November 23, 2011).

[69] Lynn, "Defending a New Domain", 97.

[70] Burak E. Bekdil and Umit Enginsoy, " Turkey Seeks Cyber security Architecture", *Defense News,* November 14, 2011.

[71] Ibid.

[72] Ibid.

[73] Umit Enginsoy, "Turkey Centralizes Efforts for National Cyber Security", *Hurriyet Daily News,* November 21, 2011.

[74] Bekdil and Enginsoy, " Turkey Seeks Cyber security Architecture."