ROLE OF THE EXERCISES IN CYBER SECURITY POLICY: TURKEY CASE

Muhterem Col
Information and Communication Technologies Agency
Ankara-Turkey

Lutfu Sagbansua
School of Economics and Administrative Sciences, Department of Business Administration,
Turgut Ozal University, Ankara-Turkey

Abstract

Cyber exercises are an important tool to assess the preparedness of a community against cyber crises, technology failures and critical information infrastructure incidents. Exercises enable the competent authorities to target specific weaknesses, increase cooperation across the critical information infrastructure sector, identify interdependencies, stimulate improvements in continuity planning, and generate a culture of cooperative effort to boost resilience in the cyber crisis cooperation area (ENISA). In this study, an overview of the global situation of cyber security is followed by the national cyber security situation of Turkey and evaluation of the security exercises conducted. A model for such exercises is provided along with summaries of findings and conclusions.

Keywords: Cyber security exercise, Cyber security policy, Turkey, ICT

1. Global Situation of Cyber Security Policy and Exercises

At the international level, there is no harmonized definition for cyber security[1] and the definition of cyber security varies from country to country[2].

Cyber security is defined by ITU 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".

Such variation influences different approaches to cyber security strategies among countries[3].

Cyber security strategies provide a strategic framework for a government's approach to cyber security[4].

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"

1.1 Cyber Security Policy

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

1 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.

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

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

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

approaches. The Anglosphere[5] 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")[6]. [Governmental Efforts and Strategies to Reinforce Security in Cyberspace]

1.2 Cyber Security Exercises

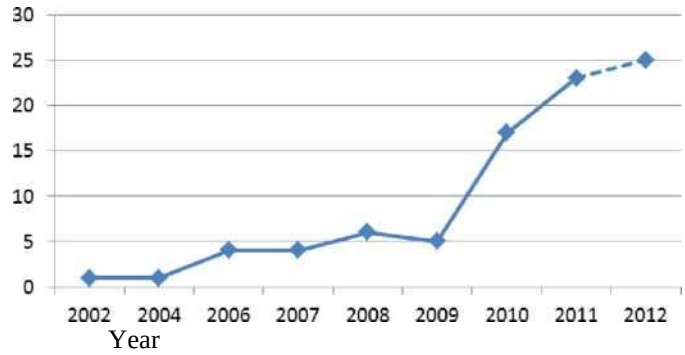
Exercises are an effective tool to assess preparedness and to identify areas for improvement absent the consequences of an actual incident. By engaging in the full exercise process – from planning through evaluation – participants are also able to establish and strengthen relationships that result in improved awareness, policy development, and information sharing. [https://www.us-cert.gov/sites/default/files/publications/infosheet_Cyber%20Exercises.pdf]

In its 2009 Communication on Critical Information Infrastructure Protection COM(20 09)-149[7], the European Commission invited Member States to 'organise regular exercises for large scale network security incident response and disaster recovery'. The Tallinn Ministerial Conference, which took place in 2009, subsequently built on the five pillars of the CIIP Action Plan, stressing that 'A joint EU exercise on Critical Information Infrastructure Protection should be organised and staged by 2010, in line with the Commission's action plan'.

As an ultimate confirmation of the importance of exercising at both the national and pan-European level, the Council Resolution published in December 2009 stated that 'Member States should organise national exercises and/or participate in regular European exercises in the area of Network and Information Security'. ENISA fulfils a significant role in this by supporting Member States in providing appropriate responses to emergencies.

Supporting EU-wide cyber security preparedness exercises is one of the main items on the Digital Agenda for Europe COM(2010),[8] the new policy plan of the European Commission which emphasises the need for Member States to carry out large-scale attack simulations and test mitigation strategies in cooperation with the Commission. Here, ENISA's newly proposed mandate again highlights the significance of cyber security preparedness exercises in enhancing trust and confidence in online services across Europe, as well as the exchange of good practices in this area [ENISA].
Figure 1 shows the number of cyber exercises per year. We see that the majority of the exercises, around 71%, in this stocktaking were conducted in the last three years (2010-2012). This figure shows that governments and private organisations take cyber threats seriously. Based on the trend observed, we can expect the number of cyber exercises to increase in the coming years [ENISA].

Figure 1: The cyber exercises collected by year



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.

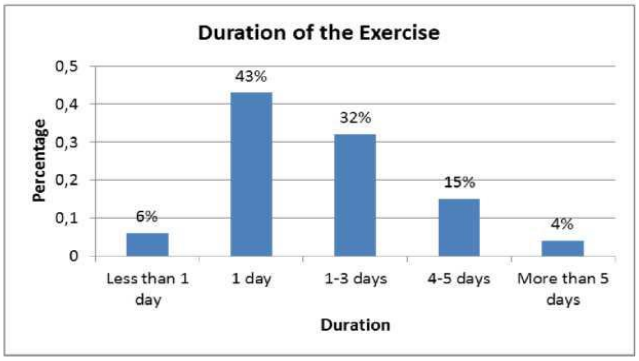
[6]Levin, Securing Cyberspace: A Comparative Review of Strategies

[7] http://ec.europa.eu/information society/policy/nis/strategy/activities/dip/index en.htm

[8] http://ec.europa.eu/digital-agenda/

Figure 2 displays the duration of the cyber exercises we examined. We found that that 43% of the exercises were one-day events, 32% of the exercises continued for two to three days and 19% of the exercises took more than three days. We can see that approximately 75% (based on 81% of overalldata gathered) of the exercises lasted for one to three days, which indicates that even a short period of time can be sufficient to execute a cyber exercise.

Figure 2: Duration of the cyber exercises examined



More specifically, we looked at the situation of cyber exercises in Europe. Figure 4 shows the map of Europe and the number of national exercises organised by European countries. For this stocktaking, we included both EU and EFTA countries (31 countries in total).

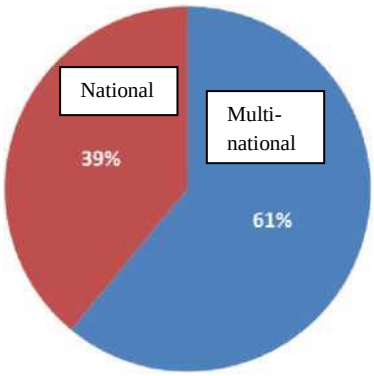
Between 2002 and 2012 six countries organised a national exercise three times. In the same period four countries organised two national cyber exercises, and 12 countries conducted one national exercise. Thus, 22 European countries in total have already organised one or more national cyber exercise. Cyprus, Malta, Luxembourg and the Czech Republic have not yet conducted such an exercise. However, these countries were involved in international exercises.

Compared to data ENISA gathered in 2010, we observe a slight increase in the number of national and international cyber exercises in Europe (Figure 3). Two years ago, 20 countries organised a national exercise.

This current stocktaking reveals that some countries have organised two or even three cyber exercises, while others have just completed one.

Figure 3 shows that approximately two-thirds of the exercises (based on 97% of overall data gathered) were national exercises and approximately one-third were multinational exercises. This indicates a tendency towards cooperation at the international level, even though matters of national security are usually domestic concerns. The cross border nature of cyber threats gives rise to the need for international cooperation. Based on these results, we anticipate that the trend of a growing number of multinational exercises will continue.

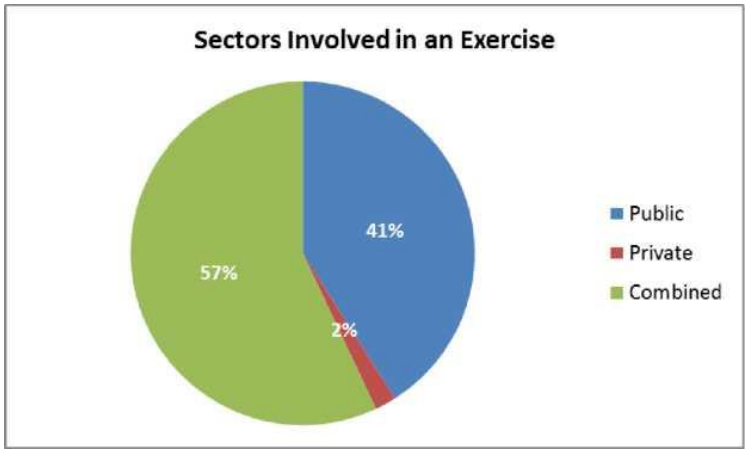
Figure 3: National and Multinational Exercises



In total, 64% (based on 94% of overall data gathered) of the multinational exercises involved more than 10 countries, 13% involved 6-10 countries and 13% involved 3-5 countries.

Another interesting aspect of cyber exercises is the participation of sectors, and more specifically the participation of the public and private sectors. As Figure 4 shows, we found that 57% of the exercises (based on 88% of overall data gathered) combined the public and private sector, while 41% involved only the public sector. We found that only one exercise in this stocktaking took place with only the private sector involved. This is an interesting finding that demonstrates that the private sector could be more proactive with testing security and contingency plans, as they are the owners of the infrastructure and the actual experts in the subject. Public-private cooperation occurs in more than half of the exercises, which is attributed to the fact that private stakeholders play a critical role in the area of cyber crisis cooperation. As such, public-private cooperation in cyber exercises is likely to increase in the coming years.

Figure 4: Sectors involved in the exercise



The number of participants in the exercises ranged from 20 to more than 75 people; this of course depends on the sectors and number of countries involved in the exercise.

2. National Cyber Security Policy of Turkey

2.1 ICT sector

In Turkey, the use of information and communication technologies (ICTs) has been spreading rapidly and ICTs are playing important roles in all aspects of our lives. In addition to public sector organizations, organizations which provide services in critical infrastructure sectors like energy, water resources, health, transportation, communication and financial services have also been heavily using information and communication systems. These systems improve the quality and the speed of the services being provided, thus helping organizations work more productively, contributing to the improvement of living standards. *[National Cyber Security Strategy and 2013-2014 Action Plan]*

Turkish electronic communications market has been liberalized and regulated since the establishment of the Telecommunications Authority in 2000. Then in 2008, Electronic Communications Law has come into force to remove the legislative untidiness, establish competition in the sector, lessen the uncertainties for operators and allocate resources to R&D. And the name of the Authority has changed to Information and Communication Technologies Authority (BTK) (BTK, 2013a).

Legal Framework

The By-Law comprises all the operators authorized by BTK and requires them to comply with the TS ISO/IEC 27001 standard and also specifies the measures which must be taken by the operators in order to avoid or decrease the risks caused by threats and weaknesses regarding physical area security, data security, hardware-software security and personnel reliability (BTK, 2013b).

Additionally, operators are obliged to prepare annual reports about security of electronic communications and BTK has the power to audit the operators whether they meet the requirements of the By-Law or not (BTK, 2013b).

Moreover, a secondary regulation was published by BTK to determine the details about the implementation of TS ISO/IEC 27001 standard dictated by the By-Law. "The Communiqué on the Implementation of TS ISO IEC 27001 Standard within the Scope of Security of Electronic Communications" was published in the Turkish Official Gazette

numbered 27730 and came into force on 15th of October 2010. The Communiqué requires ISO/IEC 27001 certification for the operators which carries personal voice and or data traffic and has an annual net sales more than 1.000.000 Turkish Liras (approximately €426.000) (BTK, 2013c).

Market Facts

Some facts about Turkish electronic communications market are given in Table 1 and Table 2. As of June 2013, there are 464 operators providing electronic communications services in the market with 742 authorizations (BTK, 2013d).

Table 1. Number of Authorizations Based on Authorization Type in Turkish Market (Nov. 14th, 2013)

Authorization Type	Services	Number of Authorizations
Authorization Agreement	Satellite and Cable TV Services	1
Concession Agreement	GSM Services	3
	IMT-2000/UMTS Services	3
	Several Telecommunication Services	1
Authorized by Notification	Satellite Telecommunication Services	32
	Satellite Platform Services	8
	Infrastructure Operation Services	101
	Internet Service Providers	237
	Fixed Telephony Services	42
	Cable TV Services	17
	GMPCS Mobile Telephony Services	5
	GSM 1800 Services on Air Vehicles	1
	Mobile Virtual Network Operator Services	35
Authorized by Right of Use	GMPCS Mobile Telephony Services	2
	PMR/PAMR Services	80
	Infrastructure Operation Services	7
	Fixed Telephony Services	8
	Directory Enquiry Services	207
	Mobile Virtual Network Operator Services	11
TOTAL		**801**

In 2012, total net sales of operators approximately worth of 31 billion Turkish Liras (approximately €13,19 billion) while the total investment is about 5,77 billion Turkish Liras (approximately €2,45 billion). The fixed penetration rate has decreased to 18,3% while the mobile penetration rate has increased to 89,5% and the number of broadband subscribers has exceeded 20 million (BTK, 2013e).

Table 2: Market Stats (BTK, 2013e)

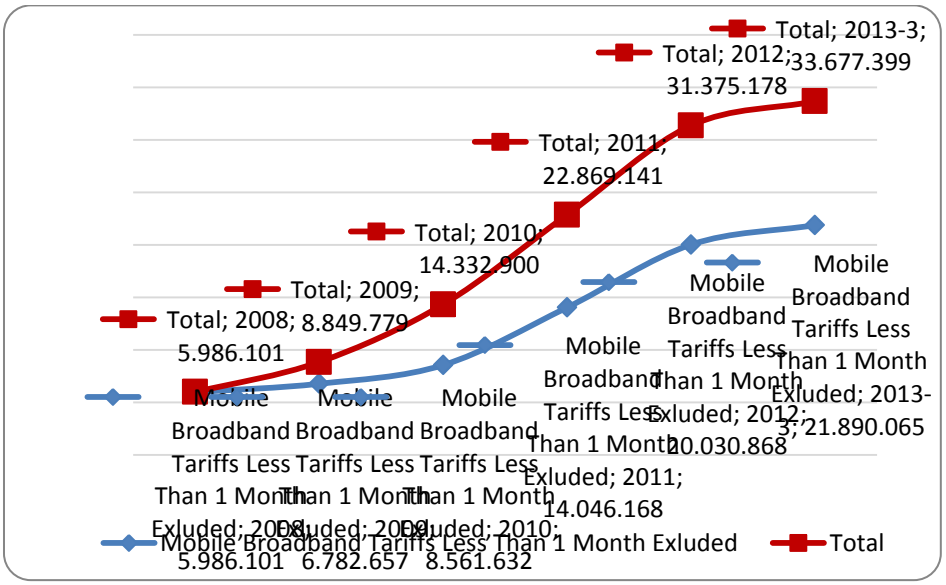
Market Statistic	Years	
	2011	2012
Net Sales (1000 TL)	27.160.427	30.877.544
Investment (1000 TL)	5.600.663	5.761.549
Fixed Penetration (%)	20,6	18,3
Mobile Penetration (%)	87,4	89,5
Broadband Subscribers	14.046.168	20.030.868

- The number of broadband subscribers, which was 6 million in 2008, has reached 33.7 million
- Number of internet subscribers in Turkey increased by 4.9% as compared to the previous quarter thanks to the increase in number of mobile, cable and especially fibre internet subscribers. Annual growth rate of total number of internet subscribers has reached to 11%.
- Number of xDSL subscribers in the third quarter and is realized as 6.7 million.
- Number of mobile broadband subscribers (computer and mobile handset) is around 25.5 million.

Table 3: Number of Internet Subscriptions

	2012 Q3	2013 Q2	2013 Q3	Quarterly Growth Rate (2013 Q2-2013 Q3)	Annual Growth Rate (2012 Q3-2013 Q3)
XDSL	6.602.030	6.644.571	6.662.999	0,3%	0,9%
Mobile Internet from Computer	1.875.653	1.786.670	1.783.396	-0,2%	-4,9%
Mobile Internet from Mobile Headset	20.708.330	22.248.371	23.708.766	6,6%	14,5%
Cable Internet	492.765	491.852	483.046	-1,8%	-2,0%
Fiber	548.493	860.871	967.309	12,4%	76,4%
Other	142.753	126.824	120.159	-5,3%	-15,8%
Total	**30.370.024**	**32.159.159**	**33.725.675**	**4,9%**	**11,0%**

Figure 5: Number of Broadband Internet Subscribers*

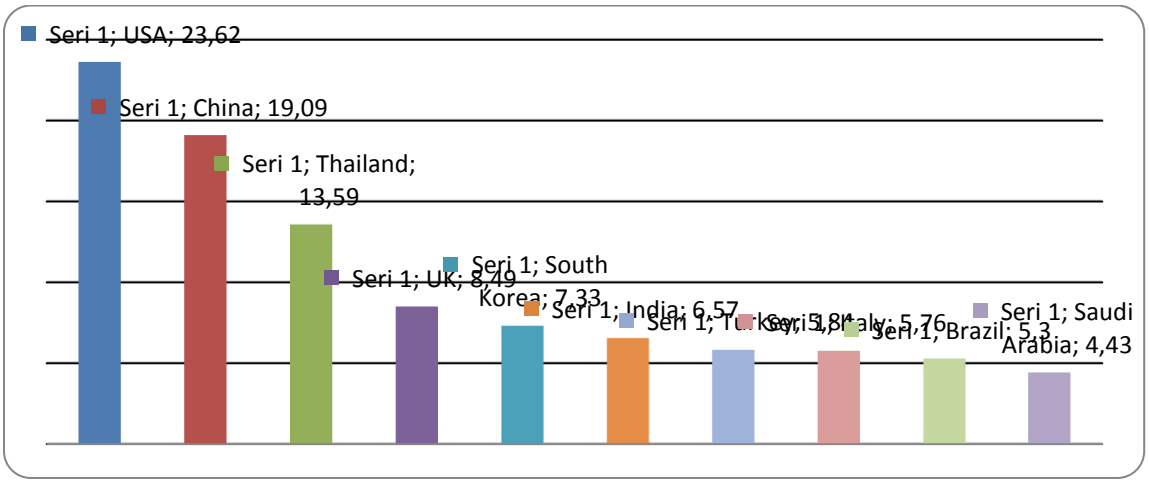


(*) Fixed, mobile, cable modem, fiber etc. all means of broadband access are included.
(*)Mobile broadband ratio given here is updated. Currently, it includes the subscribers who have used packages less than one month period, who have used packages longer than one month period and who have accessed internet without any packages. Previously, it was just consisted of the subscribers who had packages longer than one month period.

2.2 National Cyber Security strategy

There are top 10 source countries for DDOS attacks in Q4 2013 in Figure 6. The United States was the main source of DDOS attacks during Q4 of 2013, accounting for 23.62 percent of attacks. China took second place this quarter at 19.09 percent relinquishing its spot as the number one source of DDOS attacks. Turkey ranked seventh with 5.84 percent the top 10 source countries for DDOS attacks in quarter four of 2013.

Figure 6: Top 10 source countries for DDOS attacks in Q4 2013



Source: Prolexic

As our public sector organizations use ICTs to provide services at an increased rate, it has become an important aspect of our national security and competitiveness to ensure the security of information and communication technologies. The vulnerabilities inherent in ICTs may cause denial of service or abuse of service attacks, resulting in potential loss of lives, high scale economic losses, disturbance of public order and/or threats to national security.
It is a fact that cyber space offers opportunities of anonymity and deniability forattacks on information systems and data. The tools and knowledge required for attacks are often cheap and easy to get, and it has been observed that anyone or any systems across the world can participate in cyber-attacks, either knowingly or unknowingly. And it is deemed almost impossible to determine who finances and organizes these enduring and advanced cyber-attacks that target the information systems and data of critical infrastructures. These facts and conditions reveal the asymmetrical nature of the risks and threats in cyber space, making them even more difficult to tackle.

In light of this context, the Decision made by the Council of Ministers on the "Execution, Management and Coordination of National Cyber Security Activities" was published in the Official Gazette dated 20th October 2012, numbered 28447 and came into force. Pursuant to this cabinet decision;

"In order to determine the precautions to be taken for cyber security, to approve - and to ensure implementation and coordination of – the plans, schedules, reports, procedures, principles and standards that have been prepared, a Cyber Security Council has been established, which is to be presided by the Minister of Transport, Maritime Affairs and Communications and which is to consist of the undersecretaries of the Ministries of Foreign Affairs, Interior, National Defense, Transport, Maritime Affairs and Communications, including the undersecretaries of Public Order and Security, National Intelligence Organization, Head of Communication, Electronic and Information Systems of Turkish General Staff, Head of Information And Communication Technologies Authority, Head of The - Scientific And Technological Research Council, Head of Financial Crimes Investigation Council, Telecommunications Communication.

Presidency and the top managers of the ministries and the public organizations that are to be determined by the Minister of Transport, Maritime Affairs and Communications".

The cabinet decision has also assigned to the Ministry of Transport, Maritime Affairs and Communications the duty to prepare policies, strategies and action plans on ensuring cyber security at the national level. All public organizations and agencies, natural and legal persons, are obliged to perform the duties assigned in the framework of the policies, strategies and action plans determined by the Cyber Security Council, and to comply with the procedures, principles and standards that were also determined by the Council.

The action plan which was prepared pursuant to this decision defines the activities intended to be carried out within the term 2013-2014, and it also includes the periodical activities beyond these terms as well as the activities that should always be carried out such as training and awareness-raising activities *[National Cyber Security Strategy and 2013-2014 Action Plan]*.

The deadlines for some of the actions are determined, and those actions which are envisioned to be repeated periodically and carried out constantly are particularly specified. There are a total of 29 action items scheduled to take place in 2013-2014 *[National Cyber Security Strategy and 2013-2014 Action Plan]*.

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[9]. On June 20, 2013, another decision on the national cyber security strategy and action plan for the years 2013-2014 came into force.[10] 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 [Governmental Efforts and Strategies to Reinforce Security in Cyberspace].

3. Cyber Security Exercises in Turkey

4.

In the fight against cyber attacks, effective cooperationn of the institutions operating in the critical sectors with the internet servis providers operating in the electronic communications sector is very crucial. This fact triggered ICTA, which is the regulatory body for the electronic communications sector and which has been focused on cyber security for the last few years, to contemplate a new cyber security exercise with the participation of internet access providers. Yet, the increase in the number of cyber attacks targeting public institutions in Turkey in the last year had supported this idea.

Although awareness on cyber security has also increased in Turkey, too, there is still room for improvement. Various studies on the subject of cyber security of Turkey have been conducted recently (Senturk etal. 2013; Gurkaynak etal. 2013).

Within last three years, three exercises have been organsized in Turkey. These are;

- I.National Cyber Security Exercise (NCSE'11)

I.National Cyber Security Exercise (NCSE'11) was carried out in 25- 28 January 2011 with the participation of 41 public, private and non-governmental organizations (NGOs) including judicial and law enforcement agencies and various ministries as well as the ones from a diverse set of sectors such as finance, information technology and communication (ICT), education, defense and health. Six of those organizations participated in the exercise as observers.

Approximately 200 officers who are experts in the fields of ICT, law and public relations from the participatory organizations attended the exercise. In NSCE – 2011, not only the technical competence but also the intra and inter organizational coordination capabilities of the participants were evaluated by measuring their responses to the cyber attacks in both the real and the simulation environment.

[9] 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

[10] 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

- Cyber Shield Exercise'12

"Cyber Shield Exercise'12" was held in May 2012, under the coordination of ICTA and with the participation of 12 operators representing 99,9% of Turkey national internet infrastructure and comprising internet access providers which have the largest market shares in the sector and operators which provide 3rd generation (3G) internet access services. Cyber Shield Exercise is considered to be an effective and successful example of public-private cooperation.

"Cyber Shield Exercise 2012" was organized and realized by active participation of more than 50 experts from the sector more than 30 experts from ICTA. Real Distributed Denial of Service (DDoS) attacks were directed to the test systems of the participants between May 8-22, 2012 and the sufficiency of the security measures taken against those attacks were assessed. Throughout the real DDoS attacks directed to each access provider one-by-one, more than 100 Terabits of attack traffic was sent to the target systems in total. This traffic was directed to the target systems from 150 different sources locating in Turkey and also in other countries abroad. In addition to real attacks, written scenarios were also sent to the participants between May 23-28, 2012 and their responses to these scenarios were analyzed.

In summary, "Cyber Shield Exercise 2012" was emerged as a thematic exercise which aims to test both DDoS attacks that occupy an increasingly important place among cyber attacks and defensive activities against these at internet access providers' level. "Cyber Shield Exercise 2012" which contributes to national cyber security efforts is an exercise performed with the actors in the electronic communications sector.

- II.National Cyber Security Exercise (NCSE'13)

With the coordinaton of Ministry of Transport, Maritime Affairs and Communications (MTMC) ICTA and The Scientific and Technological Research Council of Turkey (TUBITAK) National Cyber Security Exercise has been held between 24 December 2012 and 11 January 2013 with participation of 61 public and private organizations. The exercise includes organizations of critical importance in sectors such as electronic communication, energy, defence, finance, and health. The scenarios are composed of; real attacks (DDoS, web security scan, port scan, log analysis, web application test, social engineering), written scenarios (6 real cyber attack scenarios), cyber security contest (4 teams of 5 members to conquer systems with pre-designed gaps).
In the last three years in Turkey, information of cyber security exercises are summarized in Table 4 and Table 5.

Table 4: Date and Coordinator of the Exercises

Exercise Name	**Date**	**Coordinator**
1st National Cyber Security Exercise	25-28 Jan. 2011	ICTA-TÜBİTAK
Cyber Shield Exercise	May 08-22, 2012	ICTA
2nd National Cyber Security Exercise	24 Dec.-2012 Jan. 2013	MTMC-ICTA-TÜBİTAK

Table 5: Participants of the Exercises

Exercise Name	**Number of Participants**	**Sector**	**Staff**
1st National Cyber Security Exercise	41	public/private/NGO	200
Cyber Shield Exercise	12	public/private	80
2nd National Cyber Security Exercise	61	public/private/NGO	300

Process of Exercise

There are two main phase in process of exercise:

Preparation Phase

Planning:

The preparatory meetings with the participants formed as the most principal part of the planning in the preparation phase.

In these meetings;

- Briefings on the attack scenarios were given,
- Detailed information about the information systems of each participant was received, with their security services being in the first place,
- Target test systems, to which real attacks would be performed, were requested from participants to be established according to some predetermined configurations
- Briefings on the secure communication platform to be used between ICTA and the participants during the exercise were given,
- Written scenarios to be applied after the real attacks and ICTA's expectations about the participants' responses to those scenarios were discussed.

Installation of Necessary Systems

The infrastructure built for performing the attacks was comprised of many different sources located inside and outside Turkey. In addition, specific software for this exercise was developed in order to improve the attack capacity further.

Exercise participants had established target test systems in their own premises and they tried to respond to the attacks directed to those systems during the exercise.

In addition, in the preparatory meetings, it was indicated to the participants that they should take all the necessary measures to protect their real (live) systems from any damages by DDoS attacks to be applied in the exercise and to ensure the security of the web applications on their test systems against any potential cyber attacks coming outside the exercise.

Within the body of ICTA, a secure communication platform to be used between ICTA and the participants for all necessary communications during the exercise was established.

Implementation Phase

Offensive

In this part, participants took place in their own premises and a fully day allocated for each. During those specified days real attacks were directed to test systems of each ISP from the Exercise Center.
Many different written scenarios were sent through the secure communication platform to each of the participants during exercises and the participants were requested to describe their potential interventions to make in case of encountering with these scenarios in real life.

Defensive

The actions performed by ISPs to detect and prevent the real attacks applied during the exercise were monitored from the Exercise Center in real time. Attacks were conducted for each ISP on a specified day, at random and different times. In this context, it was expected from the ISPs to detect the type and the extent of the attack, to react to the attack as soon as possible, and to contact with an upper level SP in case of becoming incapable of blocking the attack. Also, the participants were requested to notify BTK immediately in the event that any attack had approached to an extent of damaging their systems.

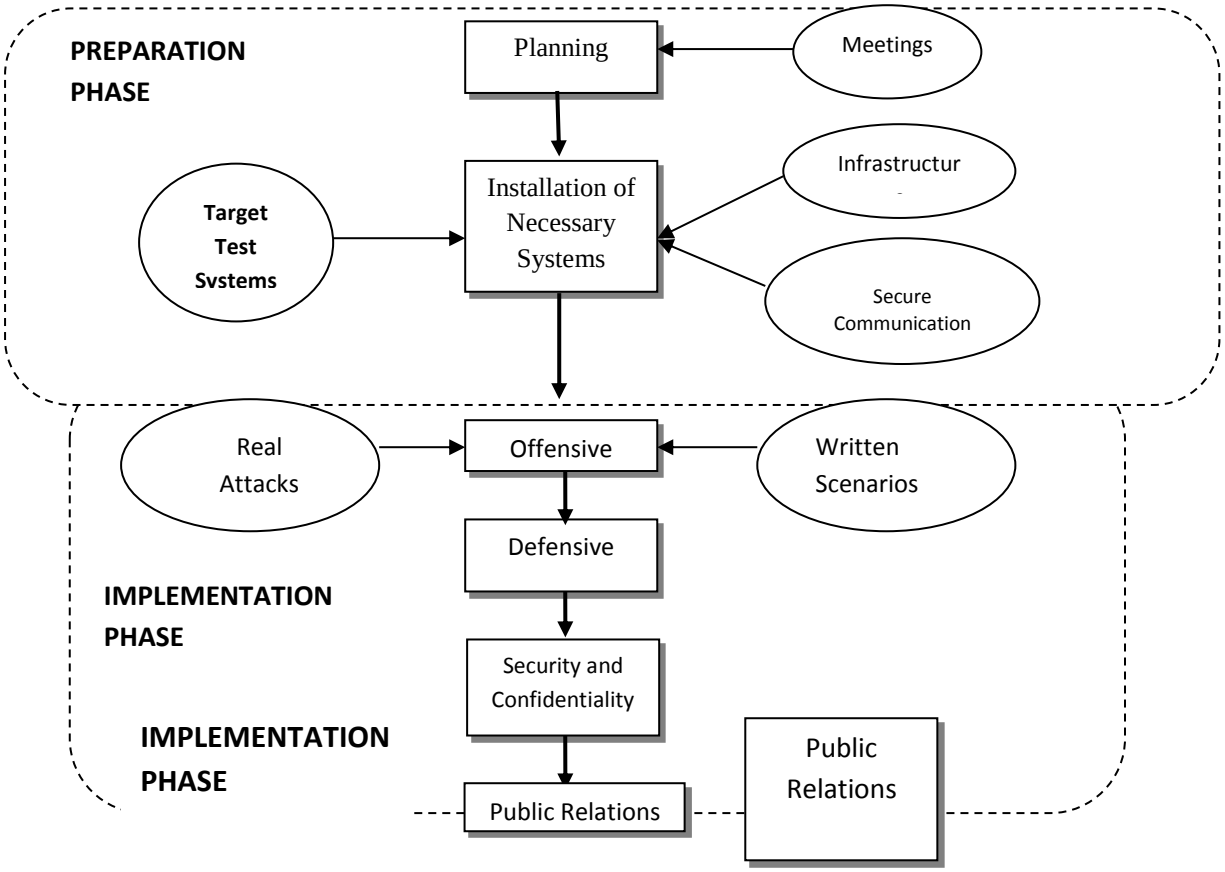
Security and Confidentiality

In order to avoid the potential negative impact of possible problems on the progress of the exercise, a secure communication platform was established to be used for communication between the participants and the Exercise Center and participants were ensured to use this platform by during the exercise. Also, it was ensured to keep the implementation dates of the real attacks confidential and not to share them publicly in order to prevent any potential cyber attacks targeting the participants during the exercise.

Public Relations

Any leakage of information regarding the exercise findings to the public before the Final Event of the Exercise was prevented. Only some general information about and the preparation and implementation processes and the findings of the exercise was shared with the public in the Final Event. Various activities were carried out to increase public awareness about the exercise during and after the Final Event.

Figure 7: Process of Exercise



5. Discussion of the findings

The following list shows which objectives were mentioned most often in the general:

- Build awareness about cyber threats
- Examine the capabilities of participating organisations to prepare for, and respond to the effects of cyber-attacks;
- Identify and highlight roles, responsibilities and authorities for responding, as well as to test decision-making and procedures between public and private actors;
- Assess cyber security emergency readiness (prepare, test and evaluate (national) procedures and processes);
- Raise awareness of infrastructure interdependency issues with a particular focus on cyber security;
- Build trust among states; enhancing interstate and interagency cooperation.
- Be prepared against cyber threats and attacks,
- Improve the response capabilities of institutions against cyber incidents,
- Enhance the coordination among relevant institutions,
- Improve the administrative, technical and legal capacity on cyber security,

- Contribute to sharing of information and experience among institutions as
- well as to raise awareness at all levels, especially among IT managers and
- other executives,
- Emphasize the critical role of internet access providers in cyber security.

As this list shows, raising awareness and building trust are important objectives of cyber exercises. In addition to the objectives, we found that procedures, plans, protocols, capabilities and players are all tested during the exercises [ENISA].

Summary of the main findings

Below we have listed (in no particular order) the main findings from ENISA's survey. This survey of national and international cyber exercises shows that countries engage in a variety of cyber exercises. The research presented in this report is not exhaustive as the results capture only 85 exercises of 84 countries (national or multinational, European or global) from 2002 to 2012.

However, we do think our stocktaking presents a good overview of the status quo and in this section we draw the main conclusions from the findings during our research.

1. The number of cyber exercises has increased in the past few years all over the world Cyber exercises are becoming increasingly more common, with the number of exercises rising sharply since 2010. This may have been caused by the overall policy context that supports and boosts cyber exercises, cyber exercise and by the increasing threat of cyber incidents and attacks. Many exercises are part of an exercise series and take place on a yearly basis. This shows that interest and activity in the field of cyber exercises persists and that this trend will most likely continue in the coming years. We observed that many countries actively engage in this field and are preparing to carry out cyber exercises in the (near) future, both domestically and in international cooperation. In addition, the media seem to report more frequently on the cyber exercises.

2. Cyber crisis cooperation efforts are in constant development Not only are cyber exercises more frequent and widespread, but there is also a constant development of cyber crisis cooperation initiatives. Cyber security is an urgent matter which receives increasingly more attention in European countries. The growing attention is spurred by the fact that societies face ever more complex and potentially devastating cyber-related contingencies and challenges. The participants in the *1st International Conference on Cyber Crisis Cooperation: Cyber Exercises* stressed the need for more exchange of good practices in the area of cyber crisis cooperation (e.g. regarding exercises and conferences) in order to learn from each other's experiences, lessons and solutions.

3. Most European countries participate in national and multinational cyber exercises Most EU and EFTA countries participate in both national and multinational exercises. This implies that efforts on a national level can be combined and complemented with efforts on a multinational level and that (inter)national cyber crisis cooperation expands during these exercises. For countries with limited national capacity (for instance to organise a national exercise), it is very helpful to participate in multinational exercises in order to ensure that their national preparedness meets the required standards. The fact that cyber crises do not stop at the border of a country also provides a strong incentive for larger countries to help neighbours with more limited capacity, and emphasises the need to jointly organise multinational exercises.

4. Public-private-NGOs liaison is essential due to private sector ownership of most critical information infrastructures Since many private sector stakeholders are involved in the protecting, managing and employing of critical information infrastructure, we consider it promising that private and public sector actors cooperate in many cyber exercises (about half of the exercises involve both public and private sector participants). However, the trend that critical information infrastructure is increasingly more owned by private stakeholders, shows the need to intensify public-private cooperation in cyber exercises in the future.

5. More attention must be paid to exercise management tools The cyber exercise field seems to show an under-appreciation of exercise management tools. Exercise management tools can assist in exercise execution and preparation (e.g. when inexperienced people prepare to organise an exercise). During the 1st International Conference on Cyber Crisis Cooperation: Cyber Exercises several exercise management tools were presented and good practices were exchanged. However, the work in this area is still progressing and many exercises do not yet employ any exercise management tools. We believe the use of these tools will grow significantly and become more relevant in the years to come.

6. Advance the use of planning, monitoring and evaluation methods Planning, monitoring and evaluation are crucial for exercise pay off, e.g. improvement of plans and procedures, policy changes, and planning and enhancement of new exercises. Planning is essential to guarantee an effective and successful exercise. It is crucial that organisers have enough time to plan, execute and evaluate exercises. The global cyber exercise community should exchange good practices regarding the planning process in order to help organisers prepare better for an exercise. The monitoring and evaluation process is made more efficient when good practices are shared among several exercise organisers. As this stocktaking yielded limited evidence of the use of monitoring and evaluation methods, we stress the fact that it is essential to gain ground in this respect. Monitoring and evaluation methods can further help exercise organisers to structure feedback and generate lessons learned. [ENISA]

The specific findings

Via the three exercises in Turkey, a significant step was taken regarding the improvement of national coordination capability in responding to cyber incidents, sharing of information and experience, creation of consciousness and awareness, and ultimately enhancement of Turkey's national cyber security competence. Moreover, considerable success was also achieved in emphasizing the crucial role of internet access providers as important actors of electronic communications sector in which the cyber attacks take place.

The specific findings compiled during the exercises are summarized below.

1. DDoS Attacks are Preventable Cyber Shield Exercise which was carried out with high traffic volumes and real attacks proved that DDoS attacks can be prevented with an effective and rapid coordination and accurate counter measures.

It was observed from Cyber Shield Exercise that, in case adequate measures against DDoS attacks are taken, possible destructive effects are preventable. Contrary to misperception in the public, this finding demonstrated that DDoS attacks, as in the case of other cyber attacks, can be prevented as long as proper and effective measures are taken.

2. Demonstrating that DDoS Attacks are Avoidable at Access Providers Level It was observed in the offensive and defensive stages of the implementation phase that; the access providers performed well as a whole in terms of coordination within and across the organizations, accurately detecting, quickly responding to and preventing different types of cyber attacks. In addition, it was assessed that the DDoS attacks could be prevented at the access providers level and if the process of responding to DDoS attacks executed successfully such attacks would be substantially eliminated.

The aim of DDoS attacks is to use up resources of target systems and fill up the access line with high amount of traffic in order to make these systems unable to respond to legal requests. The exercise demonstrated that, rather than measures at the end-user or customer's side, counter actions at the access providers' side where the resources are much higher would be successful responding to DDoS attacks.

3. Importance of Co-ordination between Access Providers Rapid, based on verified information and team-defense-based co-ordination was of critical importance in preventing attacks effectively during Exercises. The exercises revealed the need for a mechanism to coordinate cyber defense among access providers at combating cyber attacks across the country.

Some measures taken by different access providers in response to different attacks were found to be more effective. Whenever an access provider couldn't prevent an attack on its own, it was observed that the attack could be prevented by the backbone provider's measures. In this regard, importance of effective co-operation and information sharing was observed and rather than individual efforts, it was concluded that teamwork and co-ordination are among the success factors at effective combating with DDoS attacks.

4. Importance of Preparedness before Cyber Attacks Happen It was observed that before attacks ocur, preparing systems technically and determining internal and inter-agency coordination processes increase the performance in terms of response time, effectiveness and successful ness of actions taken. Before being exposed to a cyber attack, improvement efforts and strengthening systems, task-sharing among the staff were important factors at eliminating attacks successfully.

5. Efficient Use of Network Security Tools Using of network security devices -in particular IDS, IPS and DDoS prevention toolsand configuring them effectively was one of the most important steps of successful response to cyber attacks.

Network security devices which are important tools of preventing cyber attacks were effectively configured and used by access providers, in general. Therefore effective results have been obtained, in this regard.

6. The Importance of Technical Expertise Level to Intervene in Cyber Attacks While responding to attacks; timely and appropriate methods as well as experienced staff are of critical importance in order to prevent likely costs associated with cyber attacks. The experienced staff of access providers, with regard to timely and appropriately countering to attacks, played an important role in minimizing potential damages

7. Successful Achievement of the Exercise Regarding Both the Organizers and the Participants At the end of the all three exercises, the objectives and targets set prior to the exercise were achieved with great success. In this context, it was observed that the exercise was organized successfully and the participants performed well as a whole.
Access providers participating in the exercise, organizer institutions and the public has benefited from the three exercises. The exercises have also contributed to increasing the level of national awareness about the fight against cyber attacks.

5. Conclusions

Via these three Exercises 2012, a significant step was taken regarding the improvement of national coordination capability and sharing of information and experience in responding to cyber incidents, creation of consciousness and awareness, and ultimately the enhancement of Turkey's national cyber security competence. Also, considerable success was achieved in terms of emphasizing the critical role of internet access providers, that are important actors of the electronic communications infrastructure on which the cyber attacks take place, in national cyber security.
Turkey has good experience on cyber security exercises. Repetition of such exercises at regular intervals is critically important for the improvement of national cyber security culture. Hence, more comprehensive exercises, including different types of cyber attacks in addition to the DDoS attacks, are envisaged to be organized by ICTA in the future.

References

[1] Luiijf, H., Besseling, K., Spoelstra, M., De Graaf, P. 2011. Ten National Cyber Security Strategies: a comparison, CRITIS 2011 - 6th International Conference on Critical information infrastructures Security, September, 2011.
[2] Lewis, J. 2003. Cyber security: turning national solutions into international cooperation. Vol. 24. Csis.
[3] European Network and Information Security Agency ("ENISA"), National Cyber Security Strategies, Practical Guide on Development and Execution, December, 2012.
[4] Levin, Securing Cyberspace: A Comparative Review of Strategies
[5] 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
[6] 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
[7] Senturk, H., Cil, C. Z., Sagiroğlu, S. Cyber Security Analysis of Turkey. International Journal of Information Security Science, Vol.1, No. 4.
[8] Gurkaynak, G., Yılmaz, I. and Taskiran, N. P. 2013. Governmental Efforts and Strategies to Reinforce Security in Cyberspace. International Law Research; Vol. 2, No. 1; 2013.