SEVENTH FRAMEWORK PROGRAMME

Information & Communication Technologies
Trustworthy ICT

NETWORK OF EXCELLENCE

syssec

A European Network of Excellence in Managing Threats and Vulnerabilities in the Future Internet: *Europe for the World* [†]

Deliverable D2.9: Final Collection of White Papers

Abstract: This document contains the final collection of project White Papers. They have been published over the years on our website, and in many cases published through different dissemination channels. For those which appeared also as magazine papers, technical reports or in other forms, we have chosen to include their main delivery format, to better stress that we did not limit ourselves to place the whitepapers on the project website, but we took an aggressive dissemination approach through multiple channels. We feel that publishing these deliverables through multiple channels helped carry the message of the project and spread its excellent research results beyond the network of partners. In particular, from the feedback we received over the years, publishing the whitepapers in ERCIM news helped spreading our message to a large research/academic audience in a very fast way.

Responsible Partner	**Politecnico di Milano**
Contractual Date of Delivery	November 2014
Actual Date of Delivery	January 2015
Deliverable Dissemination Level	Public
Editor	Stefano Zanero

[†] The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 257007.

The *SysSec* consortium consists of:

FORTH-ICS	Coordinator	Greece
Politecnico Di Milano	Principal Contractor	Italy
Vrije Universiteit Amsterdam	Principal Contractor	The Netherlands
Institut Eurécom	Principal Contractor	France
IICT-BAS	Principal Contractor	Bulgaria
Technical University of Vienna	Principal Contractor	Austria
Chalmers University	Principal Contractor	Sweden
TUBITAK-BILGEM	Principal Contractor	Turkey

Document Revisions & Quality Assurance

Internal Reviewers

1. Davide Balzarotti (EURECOM)
2. Ali Rezaki (TUBITAK)

Revisions

Ver.	Date	By	Overview
1.2	26/1/2015	*Editor*	Fixed delivery date and changelog
1.1	18/1/2015	*Editor*	Added suggested comments to abstract.
1.0	12/1/2015	*Editor*	First complete draft.

Contents

1 Turkey's National Cyber Security Exercise 2011 Final Report

Authors TUBITAK on behalf of the SysSec consortium

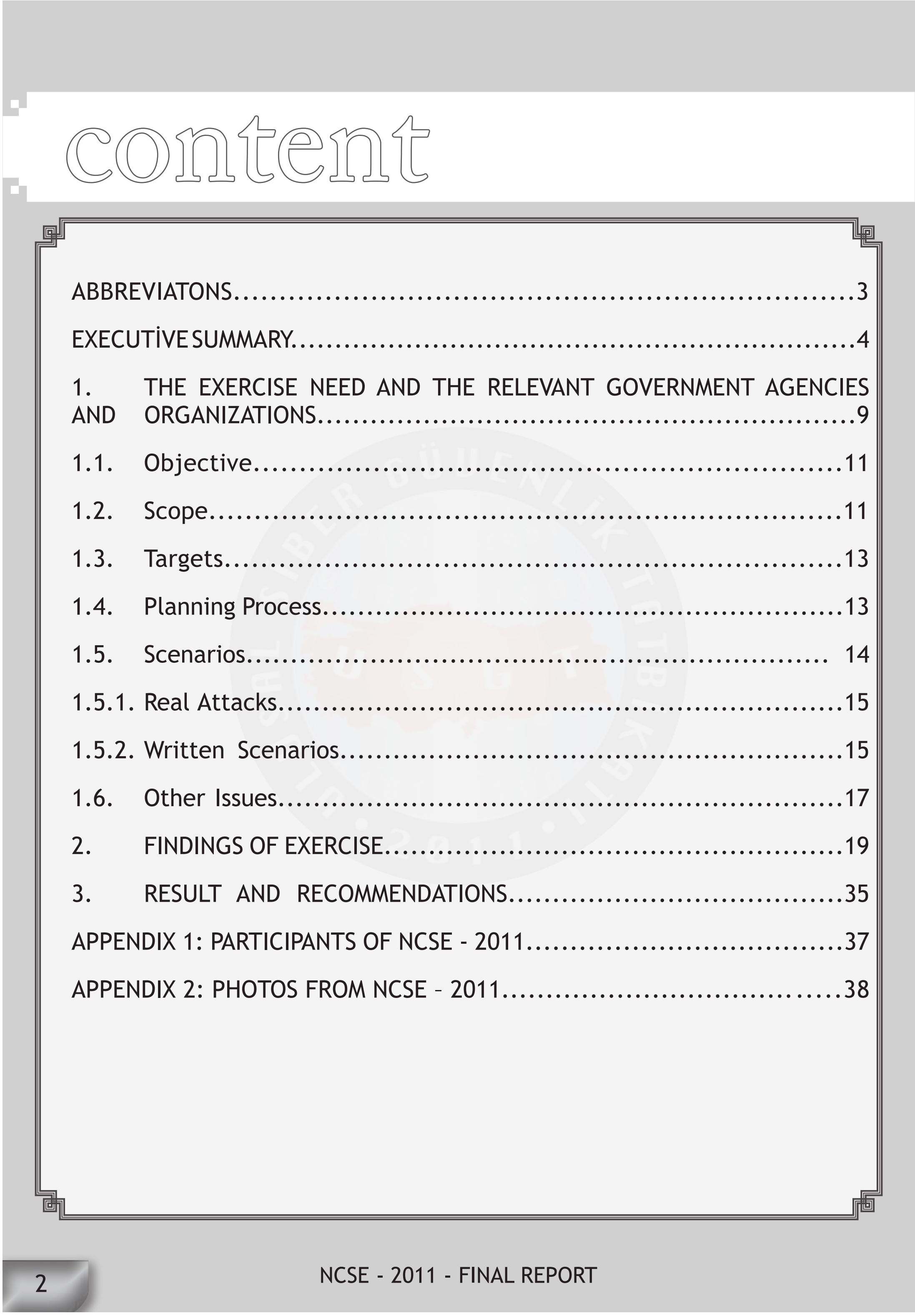
Dissemination SysSec website, and through TUBITAK's channels in Turkey

This whitepaper is the report of a national cybersecurity exercise led by TUBITAK, SysSec's partner. We decided to release it as a project whitepaper because we think it is a blueprint for organizing similar exercises in EU Member States, and generally worldwide.

NATIONAL CYBER SECURITY EXERCISE 2011
FINAL REPORT

25-28 January 2011

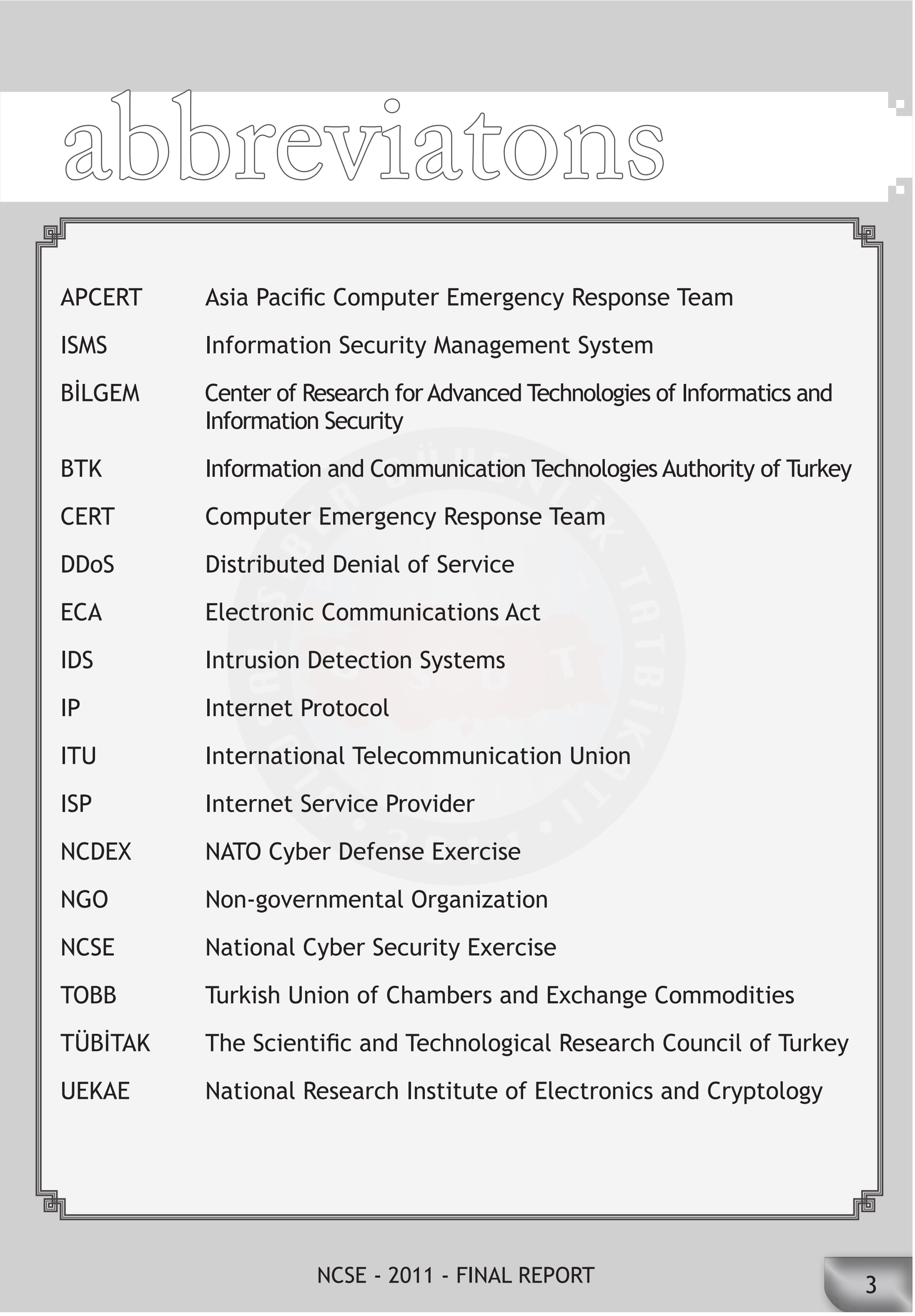
ISBN: 978-605-62506-1-3



content

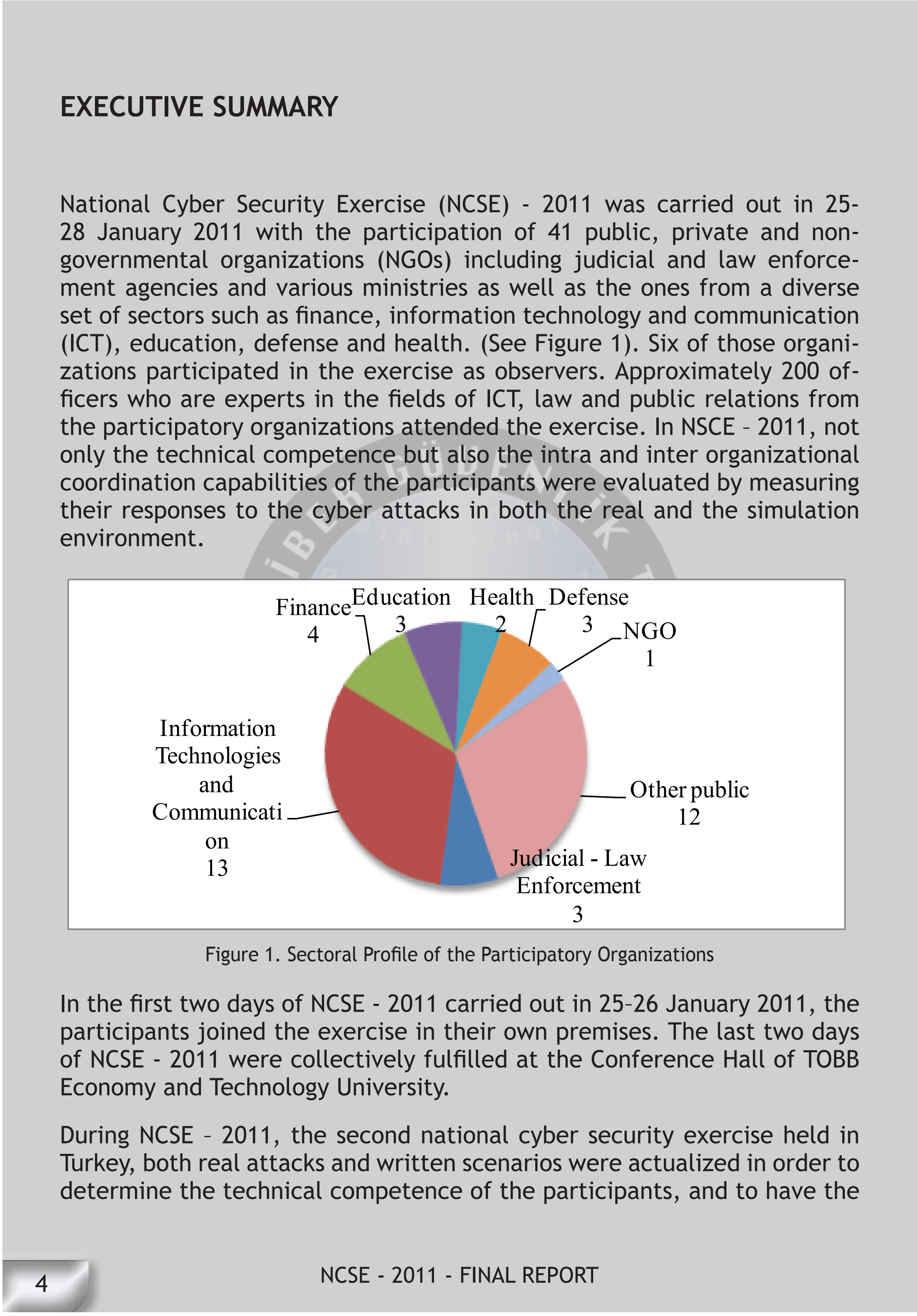
2

NCSE - 2011 - FINAL REPORT



abbreviatons

APCERT	Asia Pacific Computer Emergency Response Team
ISMS	Information Security Management System
BİLGEM	Center of Research for Advanced Technologies of Informatics and Information Security
BTK	Information and Communication Technologies Authority of Turkey
CERT	Computer Emergency Response Team
DDoS	Distributed Denial of Service
ECA	Electronic Communications Act
IDS	Intrusion Detection Systems
IP	Internet Protocol
ITU	International Telecommunication Union
ISP	Internet Service Provider
NCDEX	NATO Cyber Defense Exercise
NGO	Non-governmental Organization
NCSE	National Cyber Security Exercise
TOBB	Turkish Union of Chambers and Exchange Commodities
TÜBİTAK	The Scientific and Technological Research Council of Turkey
UEKAE	National Research Institute of Electronics and Cryptology



EXECUTIVE SUMMARY

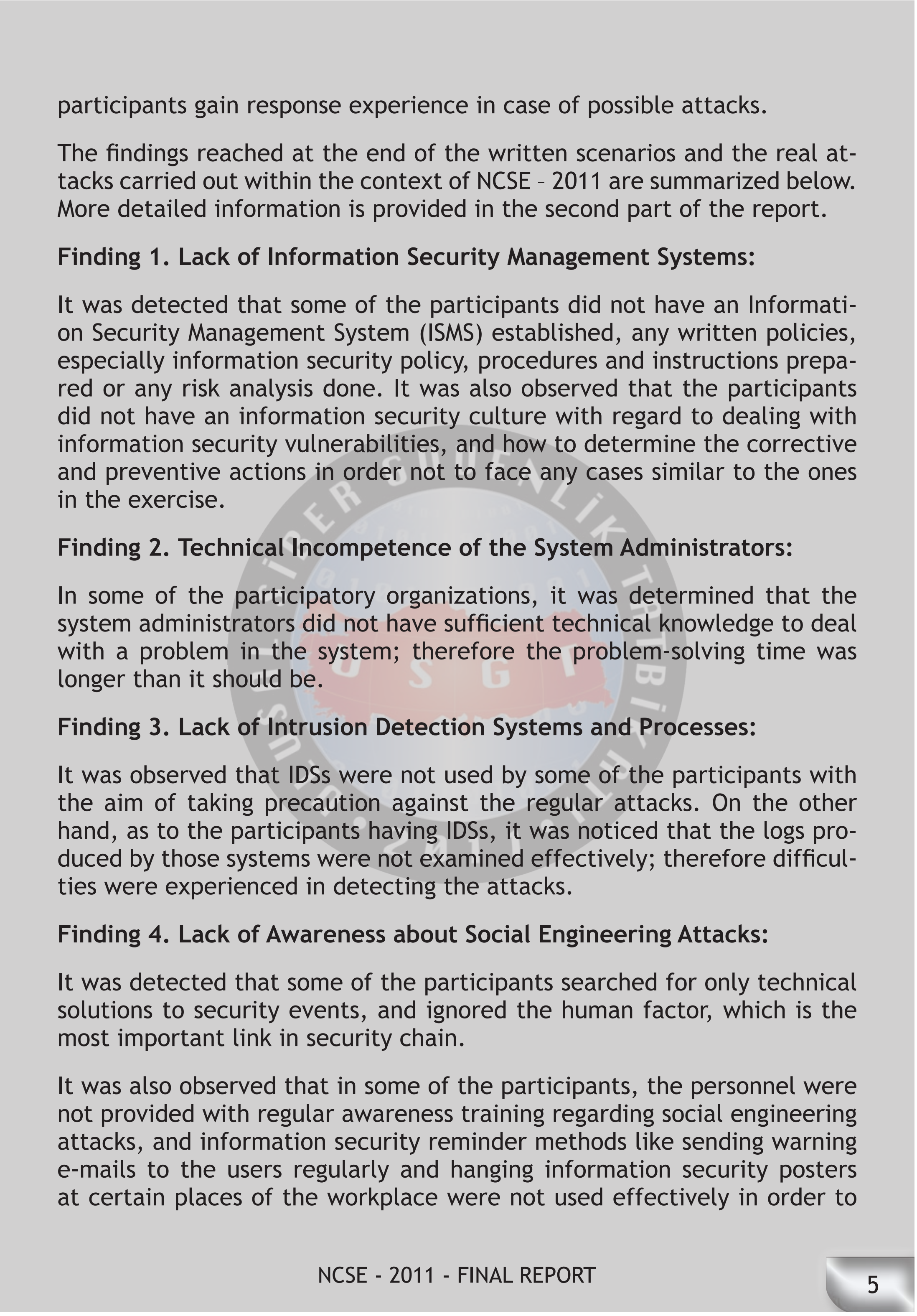
National Cyber Security Exercise (NCSE) - 2011 was carried out in 25-28 January 2011 with the participation of 41 public, private and non-governmental organizations (NGOs) including judicial and law enforcement agencies and various ministries as well as the ones from a diverse set of sectors such as finance, information technology and communication (ICT), education, defense and health. (See Figure 1). 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.

Finance 4
Education 3
Health 2
Defense 3
NGO 1
Information Technologies and Communicati on 13
Other public 12
Judicial - Law Enforcement 3

Figure 1. Sectoral Profile of the Participatory Organizations

In the first two days of NCSE - 2011 carried out in 25–26 January 2011, the participants joined the exercise in their own premises. The last two days of NCSE - 2011 were collectively fulfilled at the Conference Hall of TOBB Economy and Technology University.

During NCSE – 2011, the second national cyber security exercise held in Turkey, both real attacks and written scenarios were actualized in order to determine the technical competence of the participants, and to have the



participants gain response experience in case of possible attacks.

The findings reached at the end of the written scenarios and the real attacks carried out within the context of NCSE – 2011 are summarized below. More detailed information is provided in the second part of the report.

Finding 1. Lack of Information Security Management Systems:

It was detected that some of the participants did not have an Information Security Management System (ISMS) established, any written policies, especially information security policy, procedures and instructions prepared or any risk analysis done. It was also observed that the participants did not have an information security culture with regard to dealing with information security vulnerabilities, and how to determine the corrective and preventive actions in order not to face any cases similar to the ones in the exercise.

Finding 2. Technical Incompetence of the System Administrators:

In some of the participatory organizations, it was determined that the system administrators did not have sufficient technical knowledge to deal with a problem in the system; therefore the problem-solving time was longer than it should be.

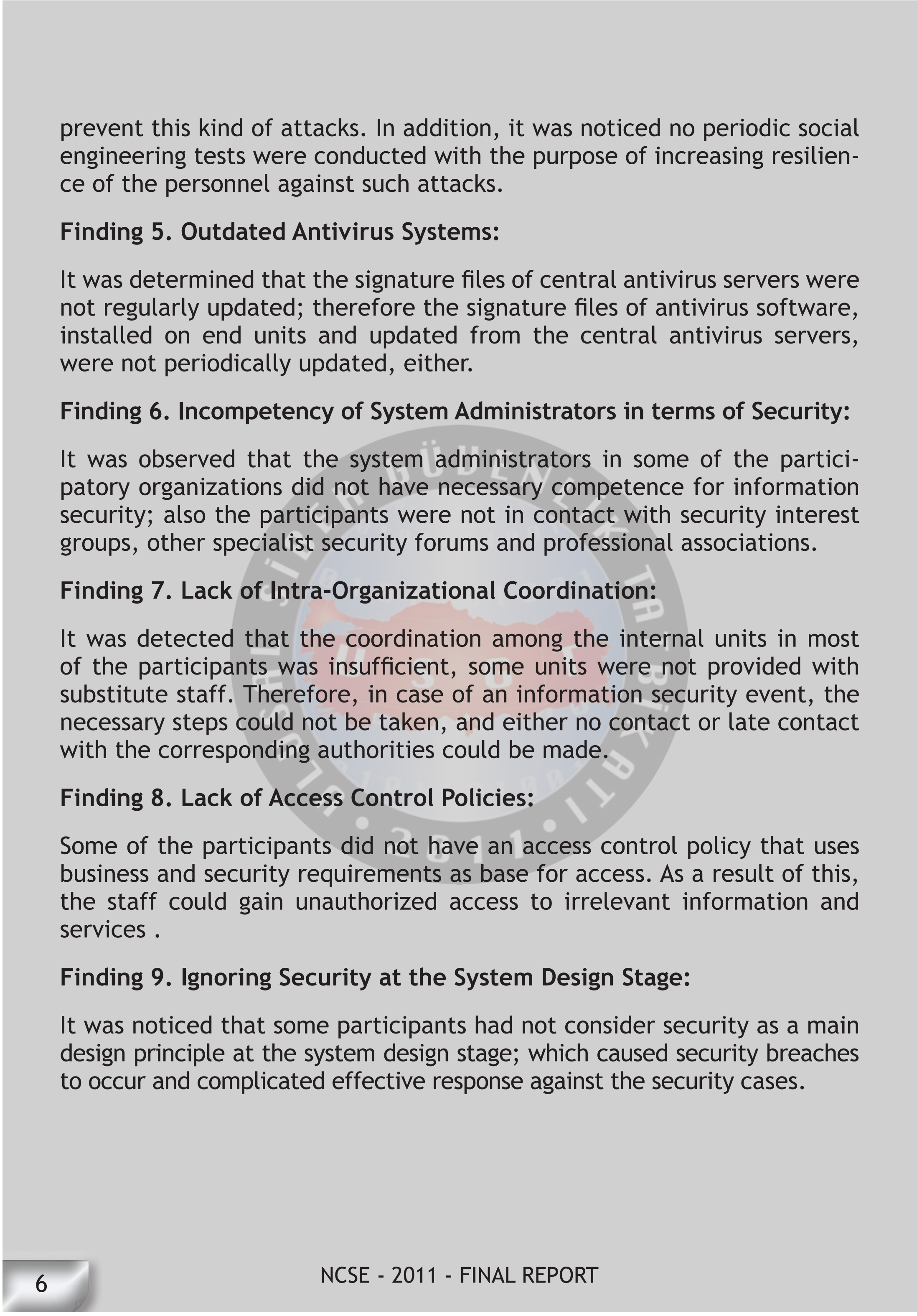
Finding 3. Lack of Intrusion Detection Systems and Processes:

It was observed that IDSs were not used by some of the participants with the aim of taking precaution against the regular attacks. On the other hand, as to the participants having IDSs, it was noticed that the logs produced by those systems were not examined effectively; therefore difficulties were experienced in detecting the attacks.

Finding 4. Lack of Awareness about Social Engineering Attacks:

It was detected that some of the participants searched for only technical solutions to security events, and ignored the human factor, which is the most important link in security chain.

It was also observed that in some of the participants, the personnel were not provided with regular awareness training regarding social engineering attacks, and information security reminder methods like sending warning e-mails to the users regularly and hanging information security posters at certain places of the workplace were not used effectively in order to



prevent this kind of attacks. In addition, it was noticed no periodic social engineering tests were conducted with the purpose of increasing resilience of the personnel against such attacks.

Finding 5. Outdated Antivirus Systems:

It was determined that the signature files of central antivirus servers were not regularly updated; therefore the signature files of antivirus software, installed on end units and updated from the central antivirus servers, were not periodically updated, either.

Finding 6. Incompetency of System Administrators in terms of Security:

It was observed that the system administrators in some of the participatory organizations did not have necessary competence for information security; also the participants were not in contact with security interest groups, other specialist security forums and professional associations.

Finding 7. Lack of Intra-Organizational Coordination:

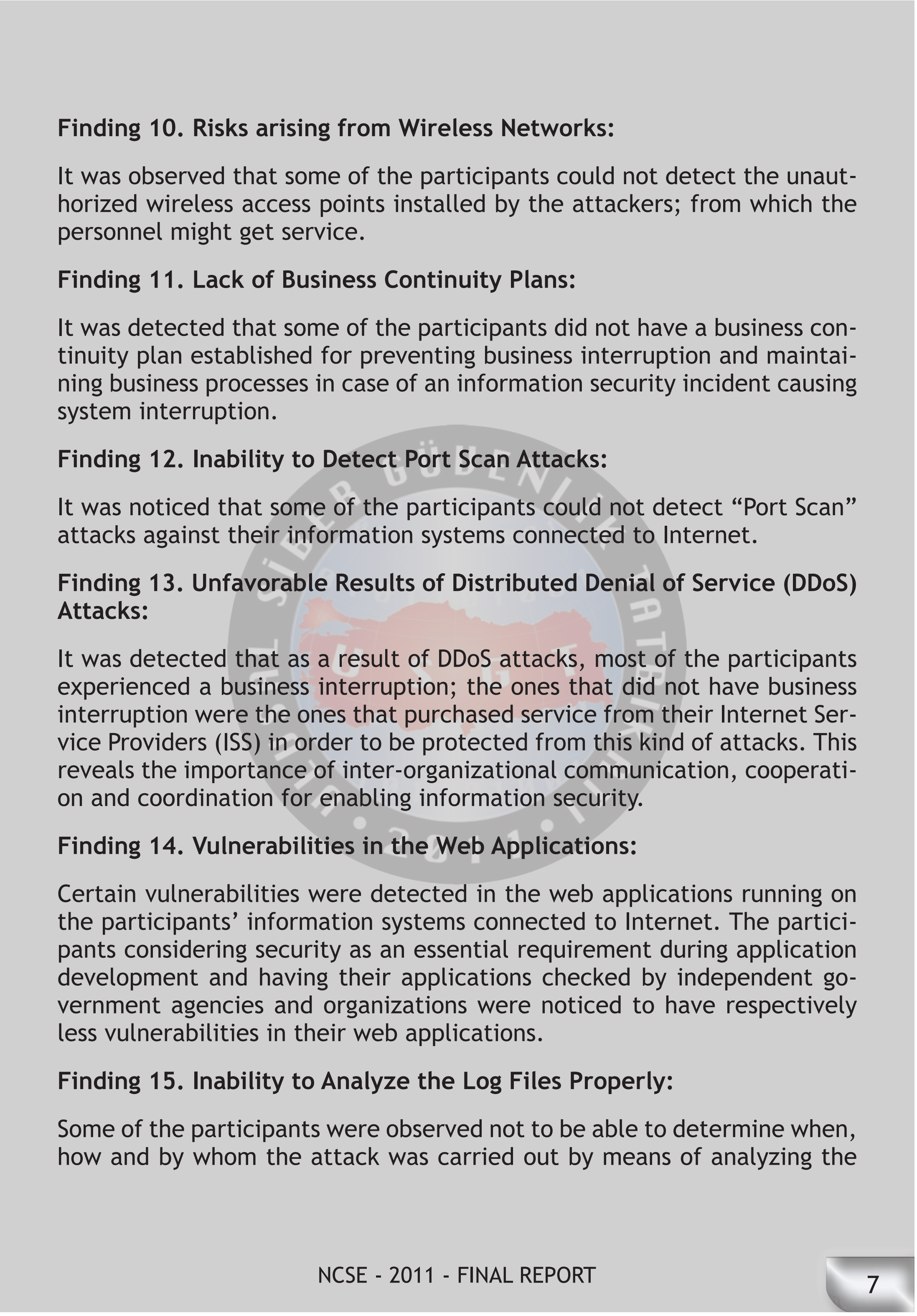
It was detected that the coordination among the internal units in most of the participants was insufficient, some units were not provided with substitute staff. Therefore, in case of an information security event, the necessary steps could not be taken, and either no contact or late contact with the corresponding authorities could be made.

Finding 8. Lack of Access Control Policies:

Some of the participants did not have an access control policy that uses business and security requirements as base for access. As a result of this, the staff could gain unauthorized access to irrelevant information and services .

Finding 9. Ignoring Security at the System Design Stage:

It was noticed that some participants had not consider security as a main design principle at the system design stage; which caused security breaches to occur and complicated effective response against the security cases.



Finding 10. Risks arising from Wireless Networks:

It was observed that some of the participants could not detect the unauthorized wireless access points installed by the attackers; from which the personnel might get service.

Finding 11. Lack of Business Continuity Plans:

It was detected that some of the participants did not have a business continuity plan established for preventing business interruption and maintaining business processes in case of an information security incident causing system interruption.

Finding 12. Inability to Detect Port Scan Attacks:

It was noticed that some of the participants could not detect "Port Scan" attacks against their information systems connected to Internet.

Finding 13. Unfavorable Results of Distributed Denial of Service (DDoS) Attacks:

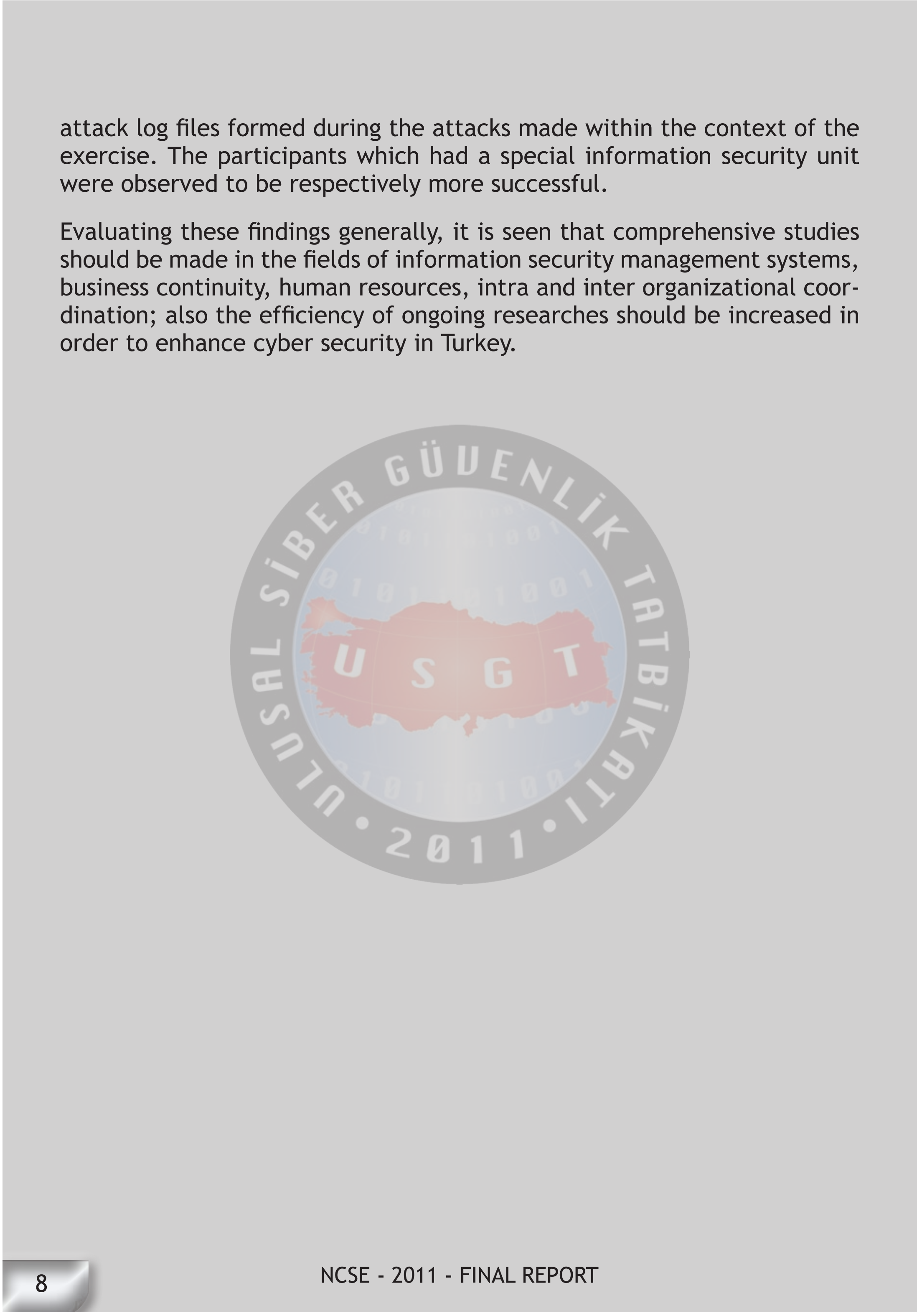
It was detected that as a result of DDoS attacks, most of the participants experienced a business interruption; the ones that did not have business interruption were the ones that purchased service from their Internet Service Providers (ISS) in order to be protected from this kind of attacks. This reveals the importance of inter-organizational communication, cooperation and coordination for enabling information security.

Finding 14. Vulnerabilities in the Web Applications:

Certain vulnerabilities were detected in the web applications running on the participants' information systems connected to Internet. The participants considering security as an essential requirement during application development and having their applications checked by independent government agencies and organizations were noticed to have respectively less vulnerabilities in their web applications.

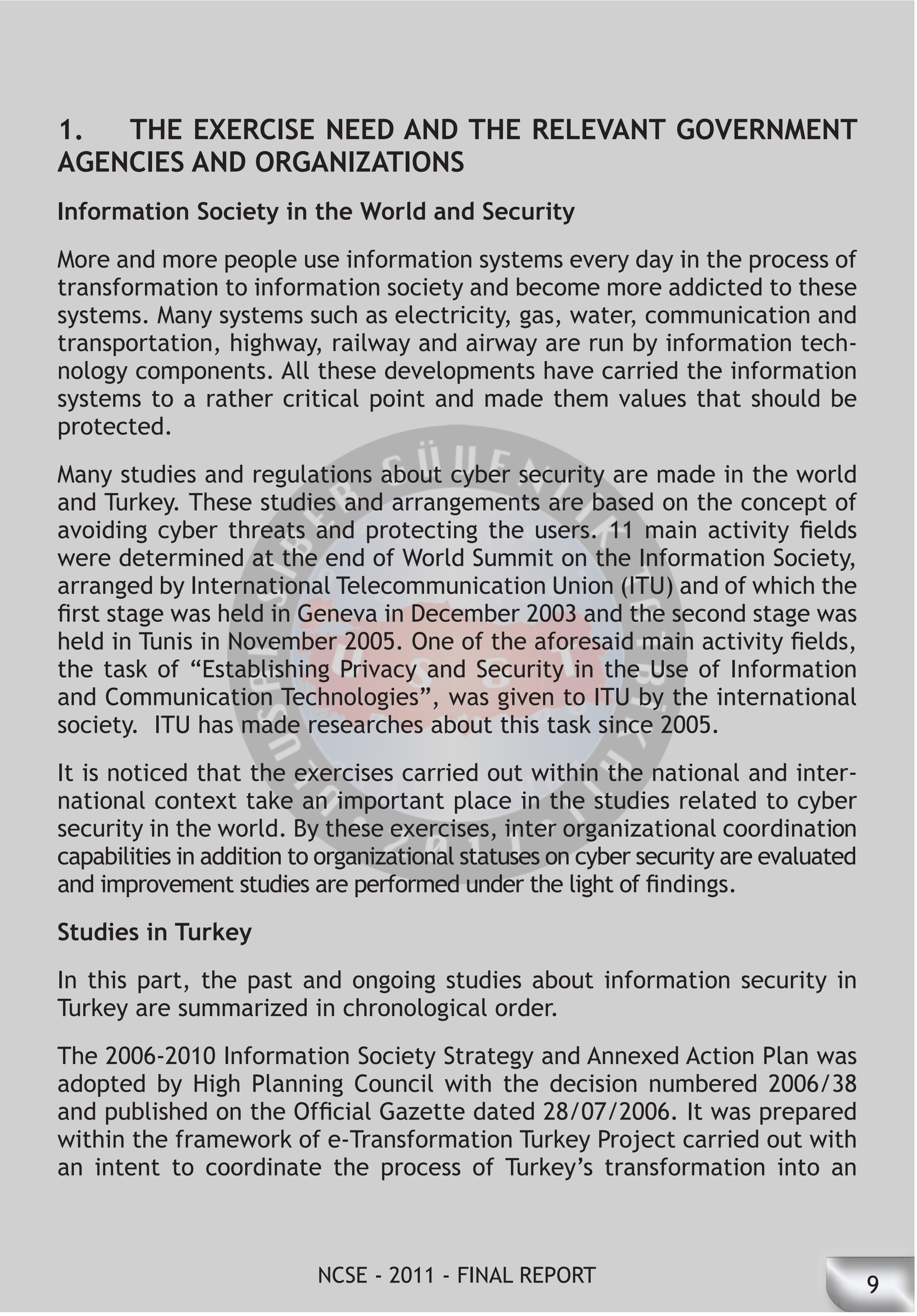
Finding 15. Inability to Analyze the Log Files Properly:

Some of the participants were observed not to be able to determine when, how and by whom the attack was carried out by means of analyzing the



attack log files formed during the attacks made within the context of the exercise. The participants which had a special information security unit were observed to be respectively more successful.

Evaluating these findings generally, it is seen that comprehensive studies should be made in the fields of information security management systems, business continuity, human resources, intra and inter organizational coordination; also the efficiency of ongoing researches should be increased in order to enhance cyber security in Turkey.



1. THE EXERCISE NEED AND THE RELEVANT GOVERNMENT AGENCIES AND ORGANIZATIONS

Information Society in the World and Security

More and more people use information systems every day in the process of transformation to information society and become more addicted to these systems. Many systems such as electricity, gas, water, communication and transportation, highway, railway and airway are run by information technology components. All these developments have carried the information systems to a rather critical point and made them values that should be protected.

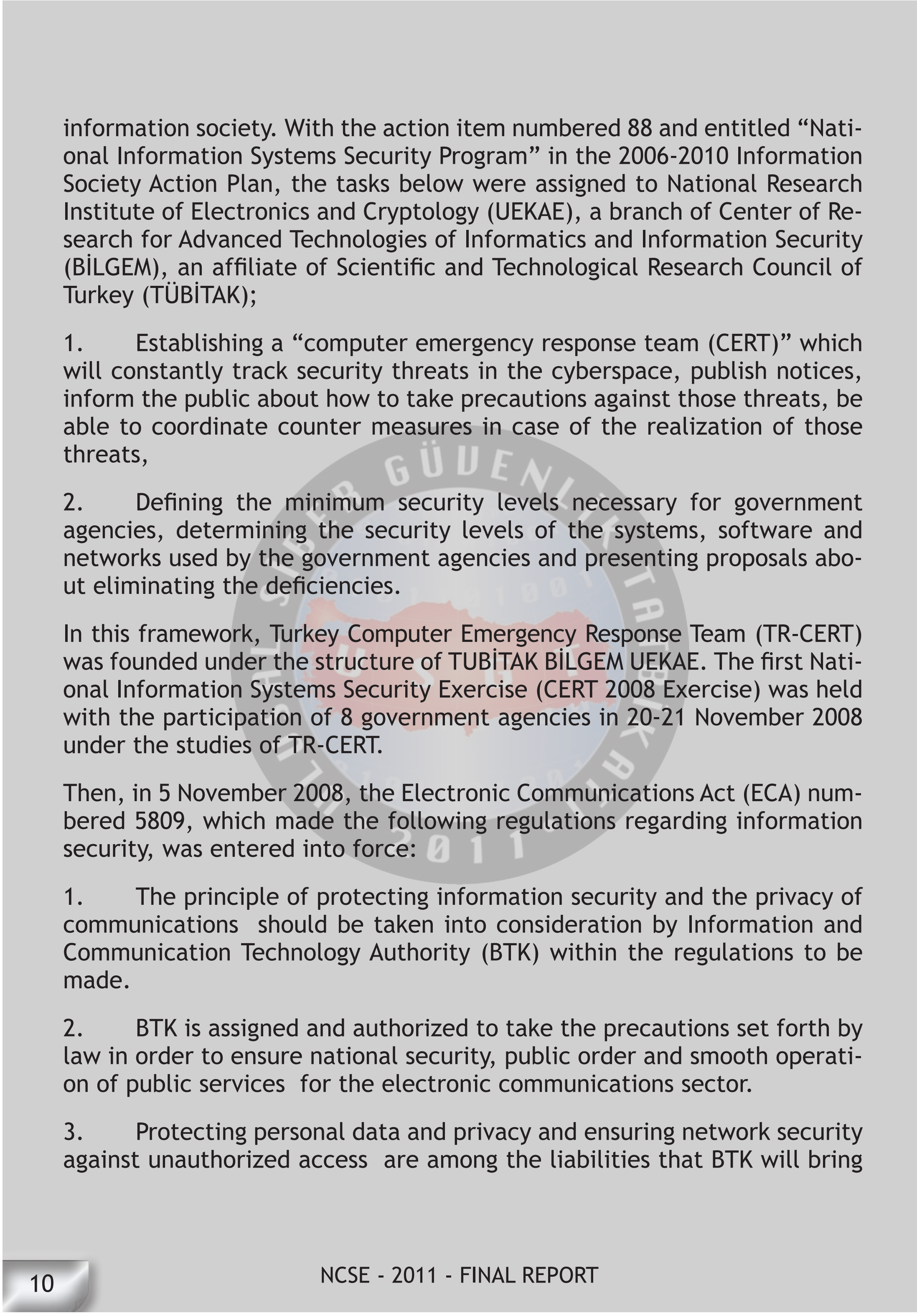
Many studies and regulations about cyber security are made in the world and Turkey. These studies and arrangements are based on the concept of avoiding cyber threats and protecting the users. 11 main activity fields were determined at the end of World Summit on the Information Society, arranged by International Telecommunication Union (ITU) and of which the first stage was held in Geneva in December 2003 and the second stage was held in Tunis in November 2005. One of the aforesaid main activity fields, the task of “Establishing Privacy and Security in the Use of Information and Communication Technologies”, was given to ITU by the international society. ITU has made researches about this task since 2005.

It is noticed that the exercises carried out within the national and international context take an important place in the studies related to cyber security in the world. By these exercises, inter organizational coordination capabilities in addition to organizational statuses on cyber security are evaluated and improvement studies are performed under the light of findings.

Studies in Turkey

In this part, the past and ongoing studies about information security in Turkey are summarized in chronological order.

The 2006-2010 Information Society Strategy and Annexed Action Plan was adopted by High Planning Council with the decision numbered 2006/38 and published on the Official Gazette dated 28/07/2006. It was prepared within the framework of e-Transformation Turkey Project carried out with an intent to coordinate the process of Turkey’s transformation into an



information society. With the action item numbered 88 and entitled “National Information Systems Security Program” in the 2006-2010 Information Society Action Plan, the tasks below were assigned to National Research Institute of Electronics and Cryptology (UEKAE), a branch of Center of Research for Advanced Technologies of Informatics and Information Security (BİLGEM), an affiliate of Scientific and Technological Research Council of Turkey (TÜBİTAK);

1. Establishing a “computer emergency response team (CERT)” which will constantly track security threats in the cyberspace, publish notices, inform the public about how to take precautions against those threats, be able to coordinate counter measures in case of the realization of those threats,

2. Defining the minimum security levels necessary for government agencies, determining the security levels of the systems, software and networks used by the government agencies and presenting proposals about eliminating the deficiencies.

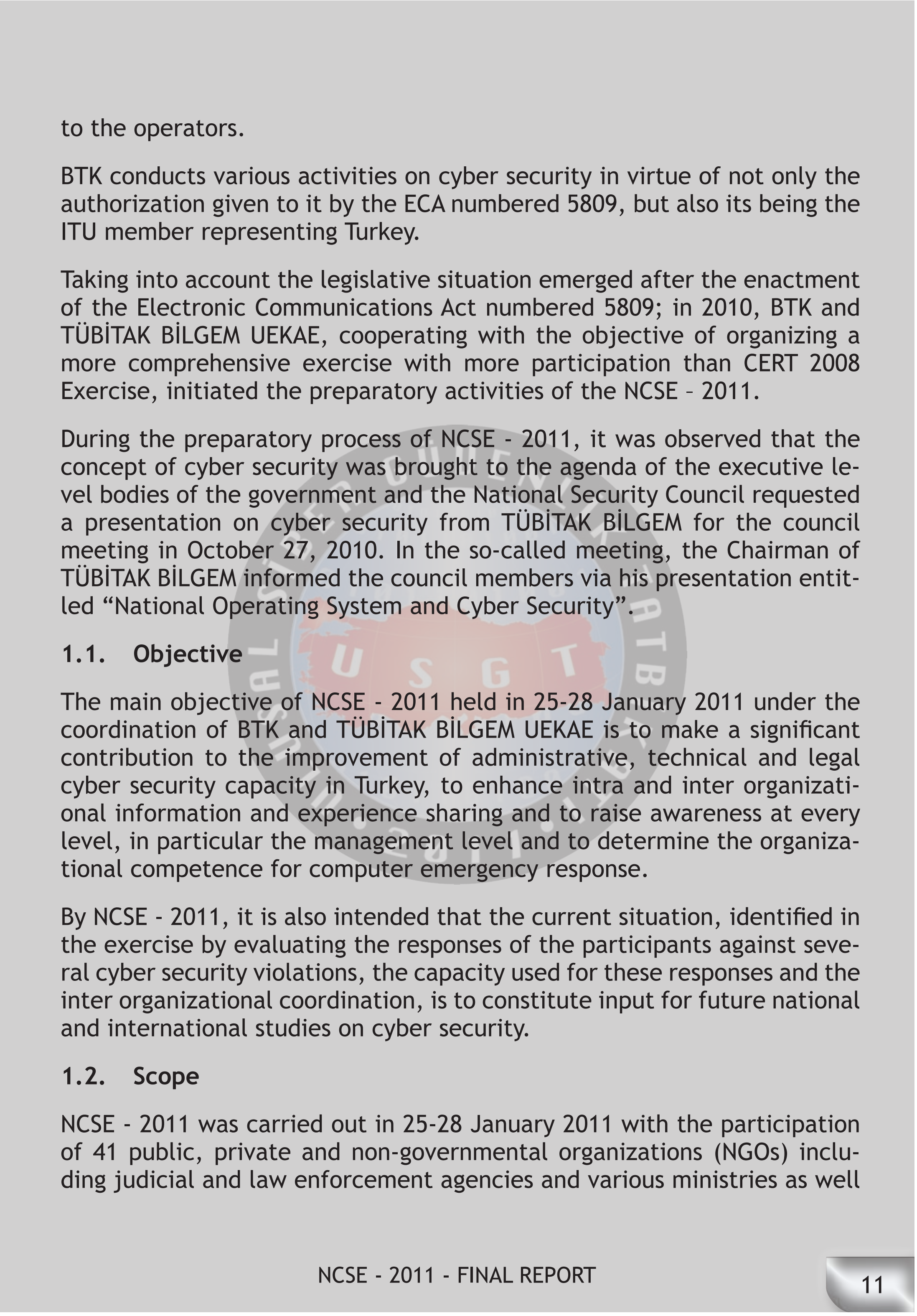
In this framework, Turkey Computer Emergency Response Team (TR-CERT) was founded under the structure of TUBİTAK BİLGEM UEKAE. The first National Information Systems Security Exercise (CERT 2008 Exercise) was held with the participation of 8 government agencies in 20-21 November 2008 under the studies of TR-CERT.

Then, in 5 November 2008, the Electronic Communications Act (ECA) numbered 5809, which made the following regulations regarding information security, was entered into force:

1. The principle of protecting information security and the privacy of communications should be taken into consideration by Information and Communication Technology Authority (BTK) within the regulations to be made.

2. BTK is assigned and authorized to take the precautions set forth by law in order to ensure national security, public order and smooth operation of public services for the electronic communications sector.

3. Protecting personal data and privacy and ensuring network security against unauthorized access are among the liabilities that BTK will bring



to the operators.

BTK conducts various activities on cyber security in virtue of not only the authorization given to it by the ECA numbered 5809, but also its being the ITU member representing Turkey.

Taking into account the legislative situation emerged after the enactment of the Electronic Communications Act numbered 5809; in 2010, BTK and TÜBİTAK BİLGEM UEKAE, cooperating with the objective of organizing a more comprehensive exercise with more participation than CERT 2008 Exercise, initiated the preparatory activities of the NCSE – 2011.

During the preparatory process of NCSE - 2011, it was observed that the concept of cyber security was brought to the agenda of the executive level bodies of the government and the National Security Council requested a presentation on cyber security from TÜBİTAK BİLGEM for the council meeting in October 27, 2010. In the so-called meeting, the Chairman of TÜBİTAK BİLGEM informed the council members via his presentation entitled "National Operating System and Cyber Security".

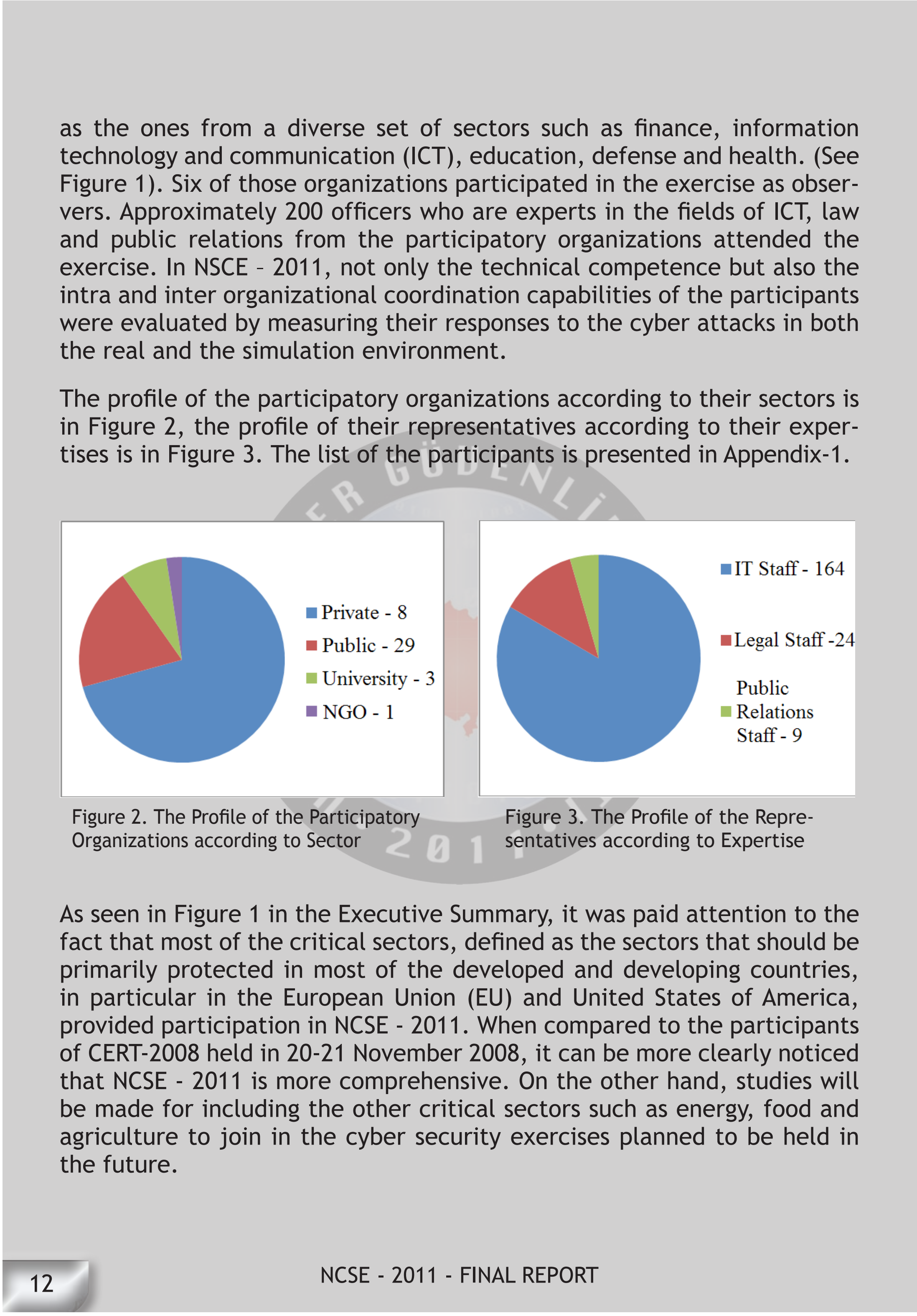
1.1. Objective

The main objective of NCSE - 2011 held in 25-28 January 2011 under the coordination of BTK and TÜBİTAK BİLGEM UEKAE is to make a significant contribution to the improvement of administrative, technical and legal cyber security capacity in Turkey, to enhance intra and inter organizational information and experience sharing and to raise awareness at every level, in particular the management level and to determine the organizational competence for computer emergency response.

By NCSE - 2011, it is also intended that the current situation, identified in the exercise by evaluating the responses of the participants against several cyber security violations, the capacity used for these responses and the inter organizational coordination, is to constitute input for future national and international studies on cyber security.

1.2. Scope

NCSE - 2011 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



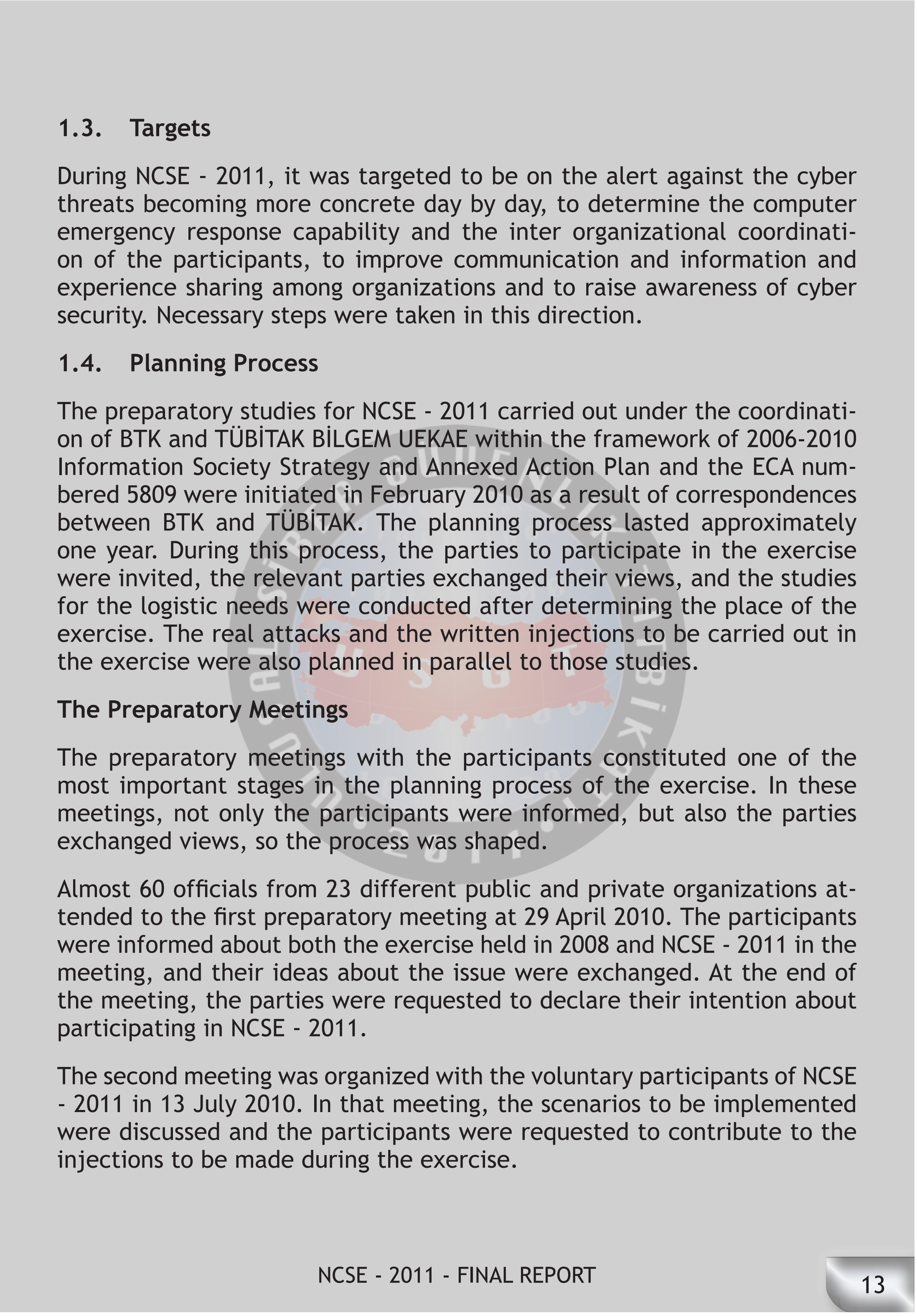
as the ones from a diverse set of sectors such as finance, information technology and communication (ICT), education, defense and health. (See Figure 1). Six of those organizations participated in the exercise as observers. Approximately 200 officers who are experts in the fields of ICT, law and public 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.

The profile of the participatory organizations according to their sectors is in Figure 2, the profile of their representatives according to their expertises is in Figure 3. The list of the participants is presented in Appendix-1.

Figure 2. The Profile of the Participatory Organizations according to Sector

Figure 3. The Profile of the Representatives according to Expertise

As seen in Figure 1 in the Executive Summary, it was paid attention to the fact that most of the critical sectors, defined as the sectors that should be primarily protected in most of the developed and developing countries, in particular in the European Union (EU) and United States of America, provided participation in NCSE - 2011. When compared to the participants of CERT-2008 held in 20-21 November 2008, it can be more clearly noticed that NCSE - 2011 is more comprehensive. On the other hand, studies will be made for including the other critical sectors such as energy, food and agriculture to join in the cyber security exercises planned to be held in the future.



1.3. Targets

During NCSE - 2011, it was targeted to be on the alert against the cyber threats becoming more concrete day by day, to determine the computer emergency response capability and the inter organizational coordination of the participants, to improve communication and information and experience sharing among organizations and to raise awareness of cyber security. Necessary steps were taken in this direction.

1.4. Planning Process

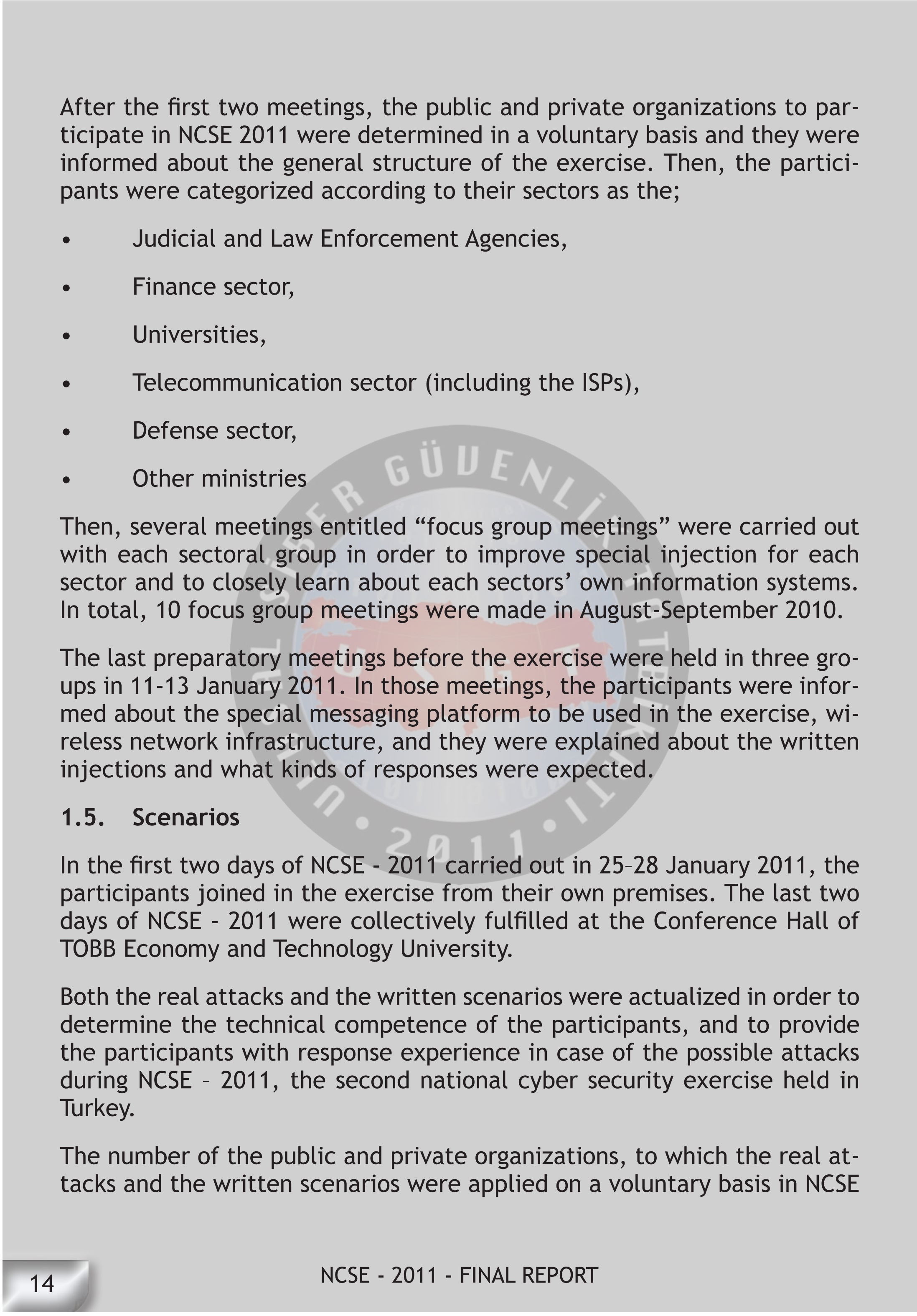
The preparatory studies for NCSE - 2011 carried out under the coordination of BTK and TÜBİTAK BİLGEM UEKAE within the framework of 2006-2010 Information Society Strategy and Annexed Action Plan and the ECA numbered 5809 were initiated in February 2010 as a result of correspondences between BTK and TÜBİTAK. The planning process lasted approximately one year. During this process, the parties to participate in the exercise were invited, the relevant parties exchanged their views, and the studies for the logistic needs were conducted after determining the place of the exercise. The real attacks and the written injections to be carried out in the exercise were also planned in parallel to those studies.

The Preparatory Meetings

The preparatory meetings with the participants constituted one of the most important stages in the planning process of the exercise. In these meetings, not only the participants were informed, but also the parties exchanged views, so the process was shaped.

Almost 60 officials from 23 different public and private organizations attended to the first preparatory meeting at 29 April 2010. The participants were informed about both the exercise held in 2008 and NCSE - 2011 in the meeting, and their ideas about the issue were exchanged. At the end of the meeting, the parties were requested to declare their intention about participating in NCSE - 2011.

The second meeting was organized with the voluntary participants of NCSE - 2011 in 13 July 2010. In that meeting, the scenarios to be implemented were discussed and the participants were requested to contribute to the injections to be made during the exercise.



After the first two meetings, the public and private organizations to participate in NCSE 2011 were determined in a voluntary basis and they were informed about the general structure of the exercise. Then, the participants were categorized according to their sectors as the;

- Judicial and Law Enforcement Agencies,
- Finance sector,
- Universities,
- Telecommunication sector (including the ISPs),
- Defense sector,
- Other ministries

Then, several meetings entitled “focus group meetings” were carried out with each sectoral group in order to improve special injection for each sector and to closely learn about each sectors’ own information systems. In total, 10 focus group meetings were made in August-September 2010.

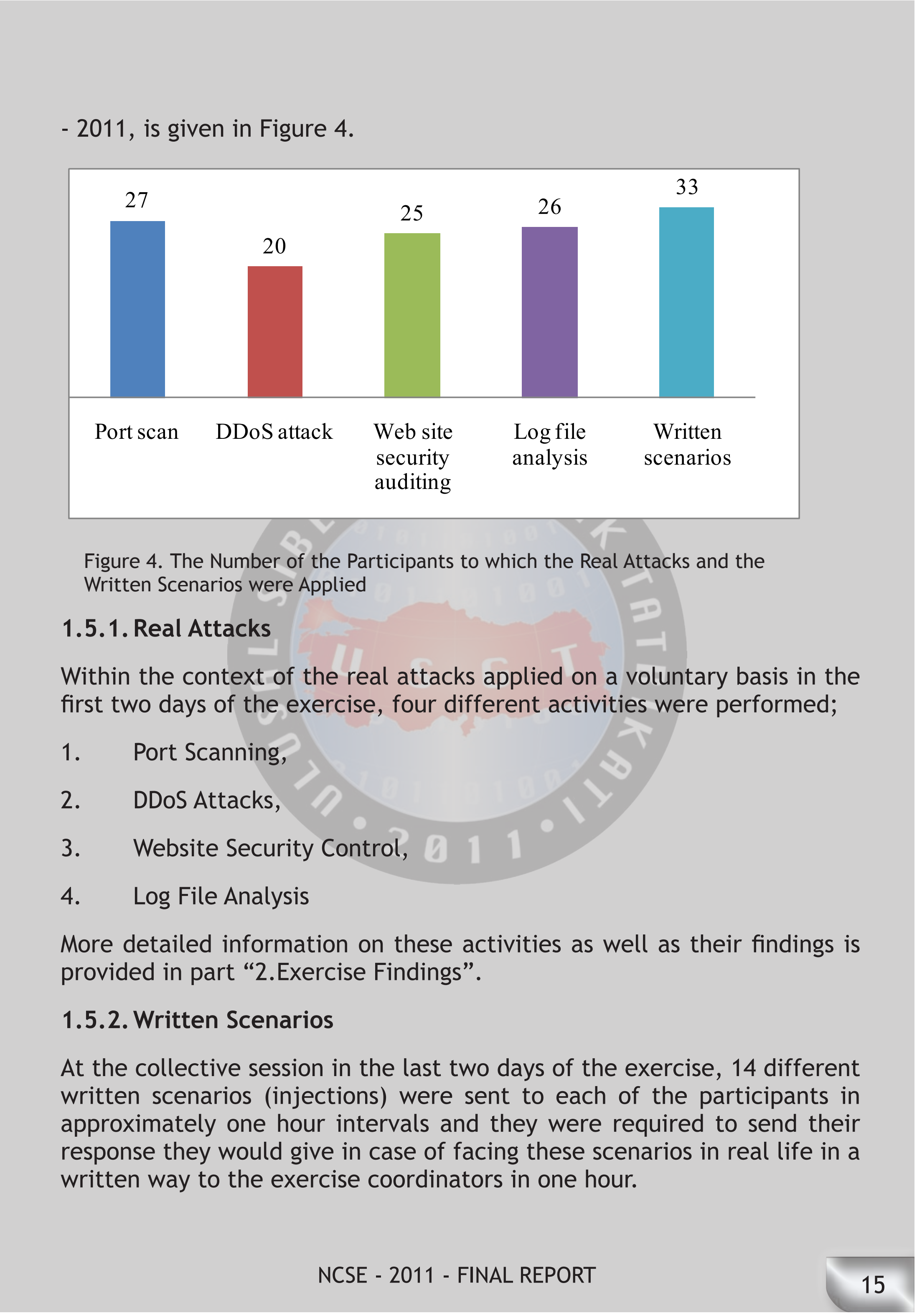
The last preparatory meetings before the exercise were held in three groups in 11-13 January 2011. In those meetings, the participants were informed about the special messaging platform to be used in the exercise, wireless network infrastructure, and they were explained about the written injections and what kinds of responses were expected.

1.5. Scenarios

In the first two days of NCSE - 2011 carried out in 25–28 January 2011, the participants joined in the exercise from their own premises. The last two days of NCSE - 2011 were collectively fulfilled at the Conference Hall of TOBB Economy and Technology University.

Both the real attacks and the written scenarios were actualized in order to determine the technical competence of the participants, and to provide the participants with response experience in case of the possible attacks during NCSE – 2011, the second national cyber security exercise held in Turkey.

The number of the public and private organizations, to which the real attacks and the written scenarios were applied on a voluntary basis in NCSE



- 2011, is given in Figure 4.

27
20
25
26
33
Port scan
DDoS attack
Web site security auditing
Log file analysis
Written scenarios

Figure 4. The Number of the Participants to which the Real Attacks and the Written Scenarios were Applied

1.5.1. Real Attacks

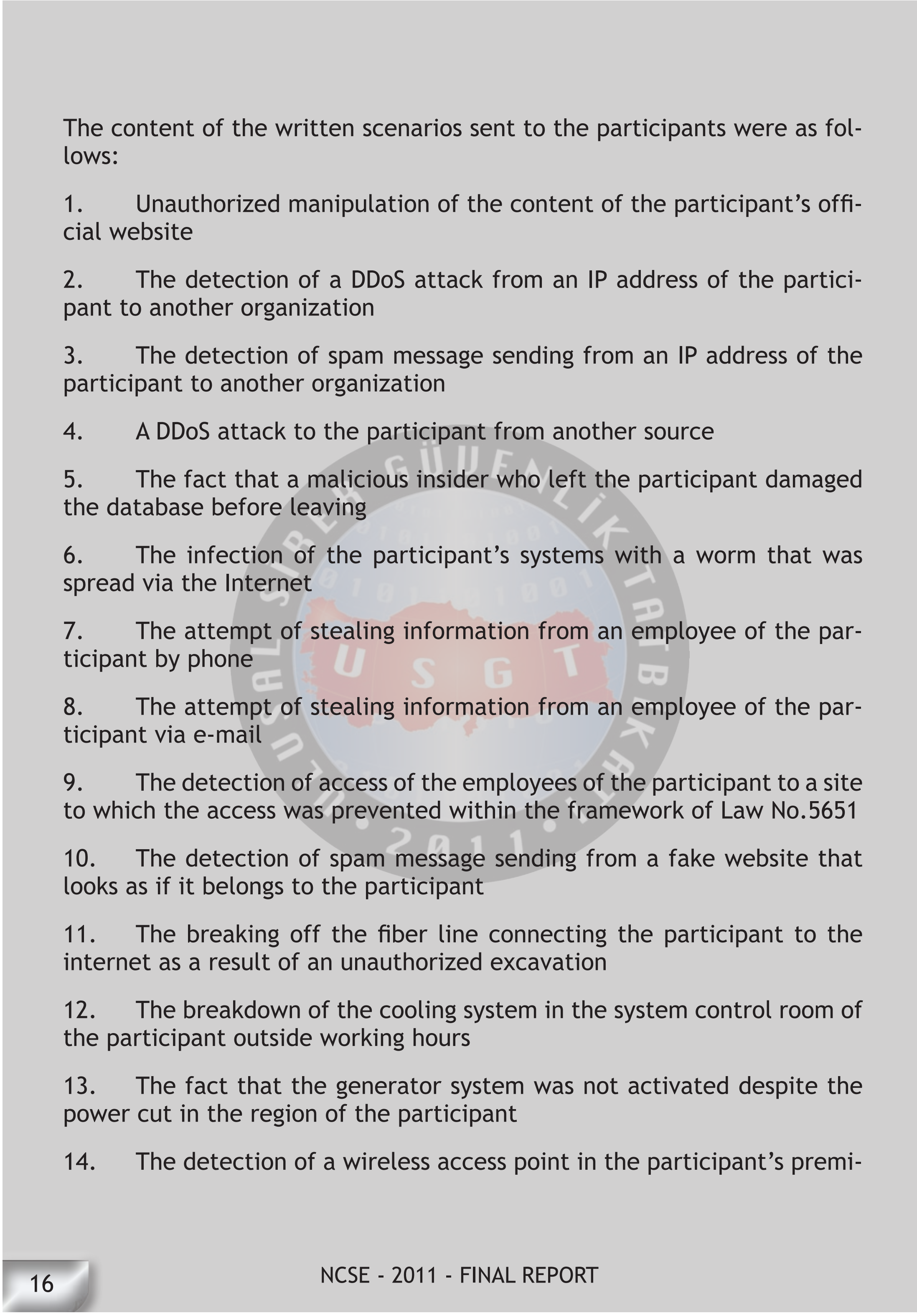
Within the context of the real attacks applied on a voluntary basis in the first two days of the exercise, four different activities were performed;

1. Port Scanning,
2. DDoS Attacks,
3. Website Security Control,
4. Log File Analysis

More detailed information on these activities as well as their findings is provided in part "2.Exercise Findings".

1.5.2. Written Scenarios

At the collective session in the last two days of the exercise, 14 different written scenarios (injections) were sent to each of the participants in approximately one hour intervals and they were required to send their response they would give in case of facing these scenarios in real life in a written way to the exercise coordinators in one hour.



The content of the written scenarios sent to the participants were as follows:

1. Unauthorized manipulation of the content of the participant's official website

2. The detection of a DDoS attack from an IP address of the participant to another organization

3. The detection of spam message sending from an IP address of the participant to another organization

4. A DDoS attack to the participant from another source

5. The fact that a malicious insider who left the participant damaged the database before leaving

6. The infection of the participant's systems with a worm that was spread via the Internet

7. The attempt of stealing information from an employee of the participant by phone

8. The attempt of stealing information from an employee of the participant via e-mail

9. The detection of access of the employees of the participant to a site to which the access was prevented within the framework of Law No.5651

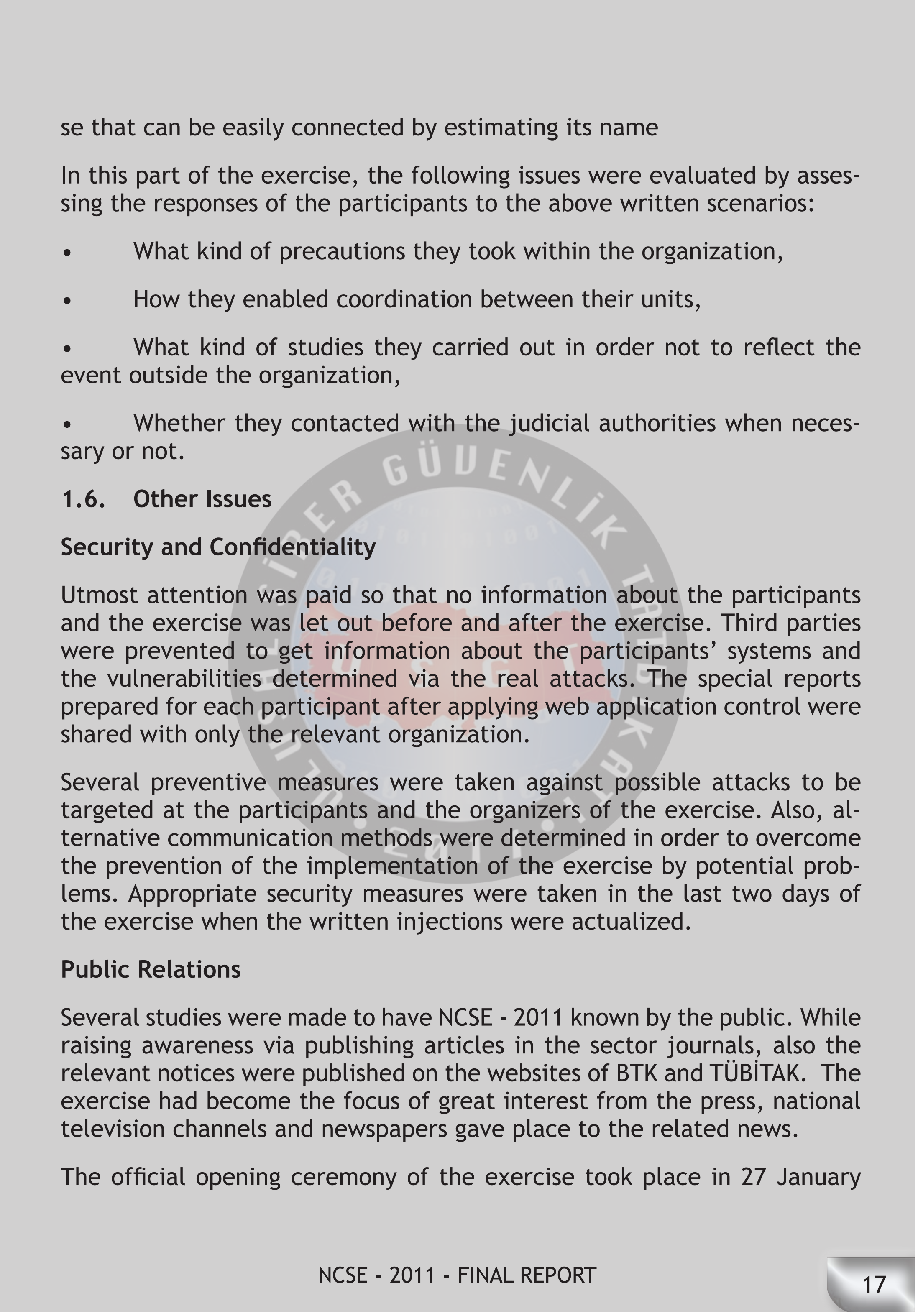
10. The detection of spam message sending from a fake website that looks as if it belongs to the participant

11. The breaking off the fiber line connecting the participant to the internet as a result of an unauthorized excavation

12. The breakdown of the cooling system in the system control room of the participant outside working hours

13. The fact that the generator system was not activated despite the power cut in the region of the participant

14. The detection of a wireless access point in the participant's premi-



se that can be easily connected by estimating its name

In this part of the exercise, the following issues were evaluated by assessing the responses of the participants to the above written scenarios:

- What kind of precautions they took within the organization,
- How they enabled coordination between their units,
- What kind of studies they carried out in order not to reflect the event outside the organization,
- Whether they contacted with the judicial authorities when necessary or not.

1.6. Other Issues

Security and Confidentiality

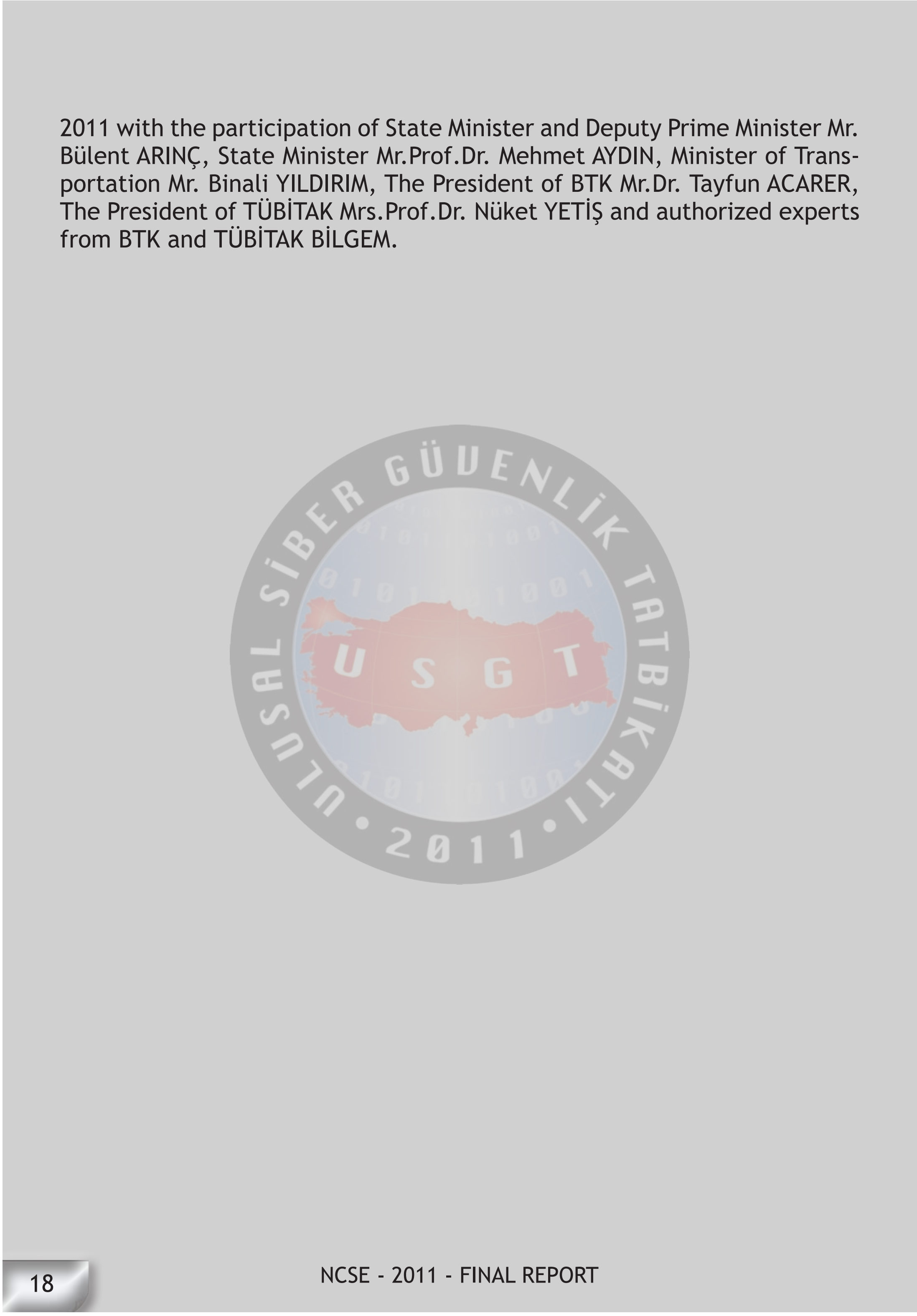
Utmost attention was paid so that no information about the participants and the exercise was let out before and after the exercise. Third parties were prevented to get information about the participants' systems and the vulnerabilities determined via the real attacks. The special reports prepared for each participant after applying web application control were shared with only the relevant organization.

Several preventive measures were taken against possible attacks to be targeted at the participants and the organizers of the exercise. Also, alternative communication methods were determined in order to overcome the prevention of the implementation of the exercise by potential problems. Appropriate security measures were taken in the last two days of the exercise when the written injections were actualized.

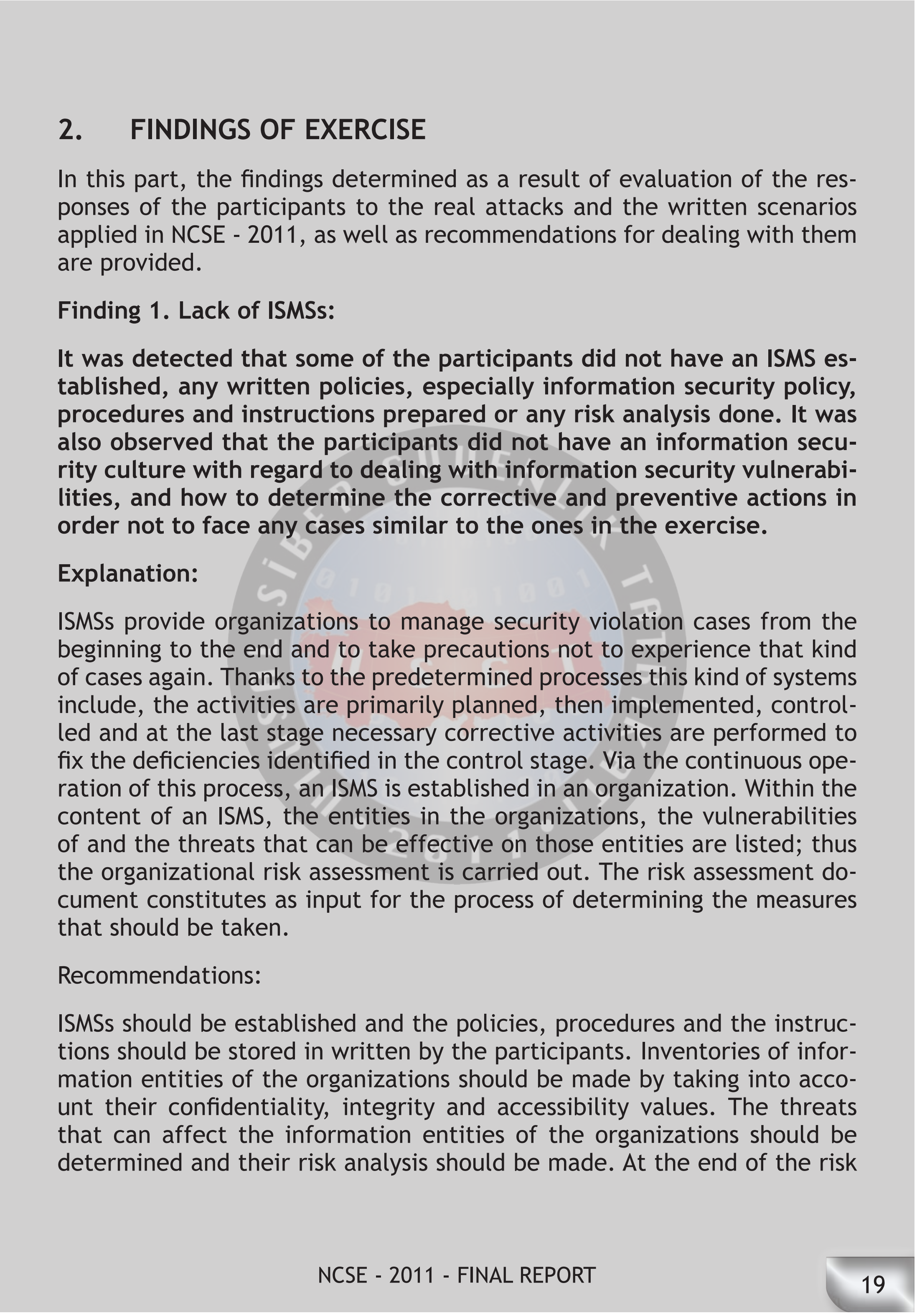
Public Relations

Several studies were made to have NCSE - 2011 known by the public. While raising awareness via publishing articles in the sector journals, also the relevant notices were published on the websites of BTK and TÜBİTAK. The exercise had become the focus of great interest from the press, national television channels and newspapers gave place to the related news.

The official opening ceremony of the exercise took place in 27 January



2011 with the participation of State Minister and Deputy Prime Minister Mr. Bülent ARINÇ, State Minister Mr.Prof.Dr. Mehmet AYDIN, Minister of Transportation Mr. Binali YILDIRIM, The President of BTK Mr.Dr. Tayfun ACARER, The President of TÜBİTAK Mrs.Prof.Dr. Nüket YETİŞ and authorized experts from BTK and TÜBİTAK BİLGEM.



2. FINDINGS OF EXERCISE

In this part, the findings determined as a result of evaluation of the responses of the participants to the real attacks and the written scenarios applied in NCSE - 2011, as well as recommendations for dealing with them are provided.

Finding 1. Lack of ISMSs:

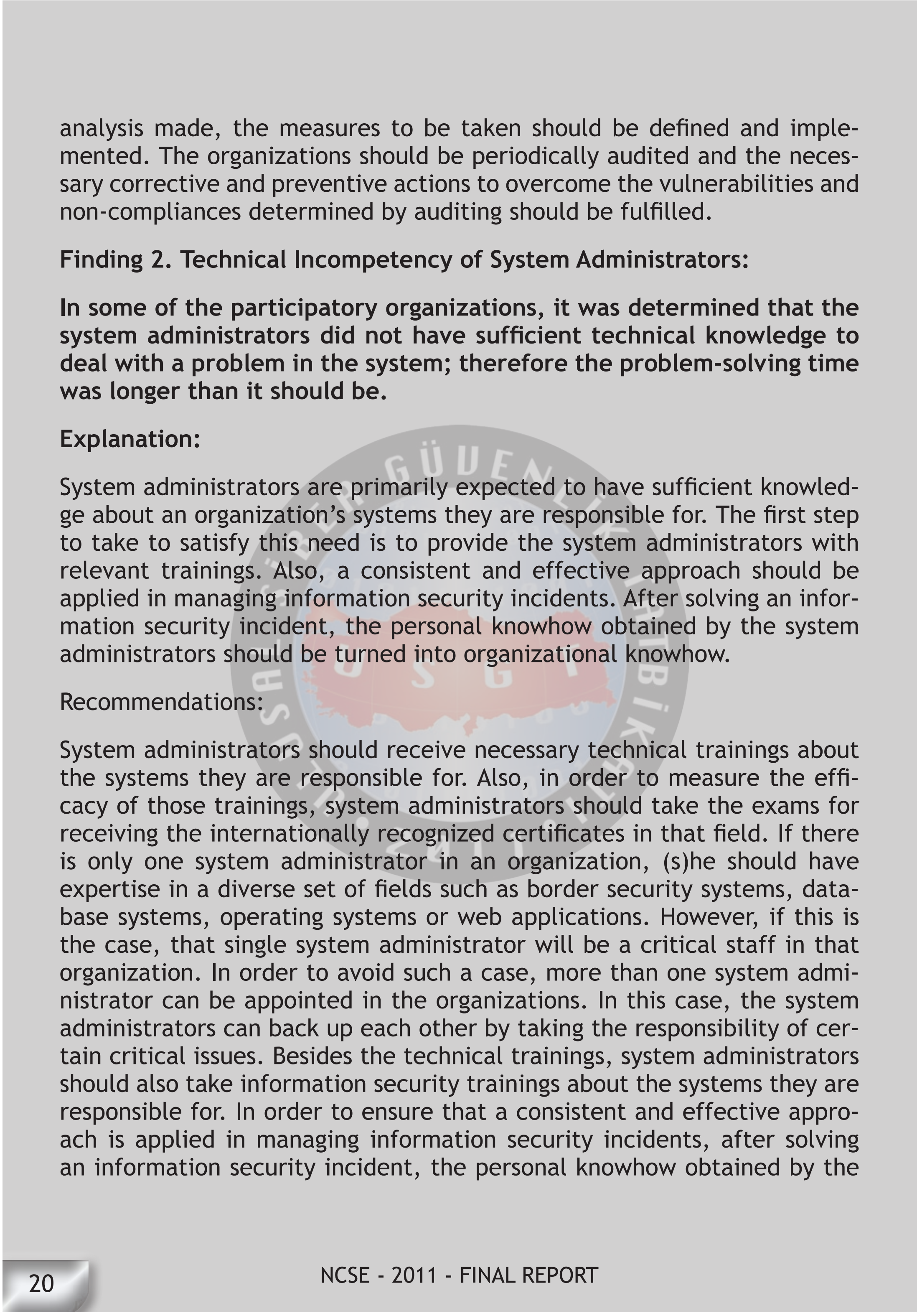
It was detected that some of the participants did not have an ISMS established, any written policies, especially information security policy, procedures and instructions prepared or any risk analysis done. It was also observed that the participants did not have an information security culture with regard to dealing with information security vulnerabilities, and how to determine the corrective and preventive actions in order not to face any cases similar to the ones in the exercise.

Explanation:

ISMSs provide organizations to manage security violation cases from the beginning to the end and to take precautions not to experience that kind of cases again. Thanks to the predetermined processes this kind of systems include, the activities are primarily planned, then implemented, controlled and at the last stage necessary corrective activities are performed to fix the deficiencies identified in the control stage. Via the continuous operation of this process, an ISMS is established in an organization. Within the content of an ISMS, the entities in the organizations, the vulnerabilities of and the threats that can be effective on those entities are listed; thus the organizational risk assessment is carried out. The risk assessment document constitutes as input for the process of determining the measures that should be taken.

Recommendations:

ISMSs should be established and the policies, procedures and the instructions should be stored in written by the participants. Inventories of information entities of the organizations should be made by taking into account their confidentiality, integrity and accessibility values. The threats that can affect the information entities of the organizations should be determined and their risk analysis should be made. At the end of the risk



analysis made, the measures to be taken should be defined and implemented. The organizations should be periodically audited and the necessary corrective and preventive actions to overcome the vulnerabilities and non-compliances determined by auditing should be fulfilled.

Finding 2. Technical Incompetency of System Administrators:

In some of the participatory organizations, it was determined that the system administrators did not have sufficient technical knowledge to deal with a problem in the system; therefore the problem-solving time was longer than it should be.

Explanation:

System administrators are primarily expected to have sufficient knowledge about an organization's systems they are responsible for. The first step to take to satisfy this need is to provide the system administrators with relevant trainings. Also, a consistent and effective approach should be applied in managing information security incidents. After solving an information security incident, the personal knowhow obtained by the system administrators should be turned into organizational knowhow.

Recommendations:

System administrators should receive necessary technical trainings about the systems they are responsible for. Also, in order to measure the efficacy of those trainings, system administrators should take the exams for receiving the internationally recognized certificates in that field. If there is only one system administrator in an organization, (s)he should have expertise in a diverse set of fields such as border security systems, database systems, operating systems or web applications. However, if this is the case, that single system administrator will be a critical staff in that organization. In order to avoid such a case, more than one system administrator can be appointed in the organizations. In this case, the system administrators can back up each other by taking the responsibility of certain critical issues. Besides the technical trainings, system administrators should also take information security trainings about the systems they are responsible for. In order to ensure that a consistent and effective approach is applied in managing information security incidents, after solving an information security incident, the personal knowhow obtained by the system administrators should be turned into organizational knowhow by identifying policies and procedures to measure and monitor the kinds, existence frequencies and the financial damage of information security incidents.

Finding 3. Lack of Intrusion Detection Systems and Processes:

It was observed that IDSs were not used by some of the participants with the aim of taking precaution against the regular attacks. On the other hand, as to the participants having IDSs, it was noticed that the logs produced by those systems were not examined effectively; therefore difficulties were experienced in detecting the attacks.

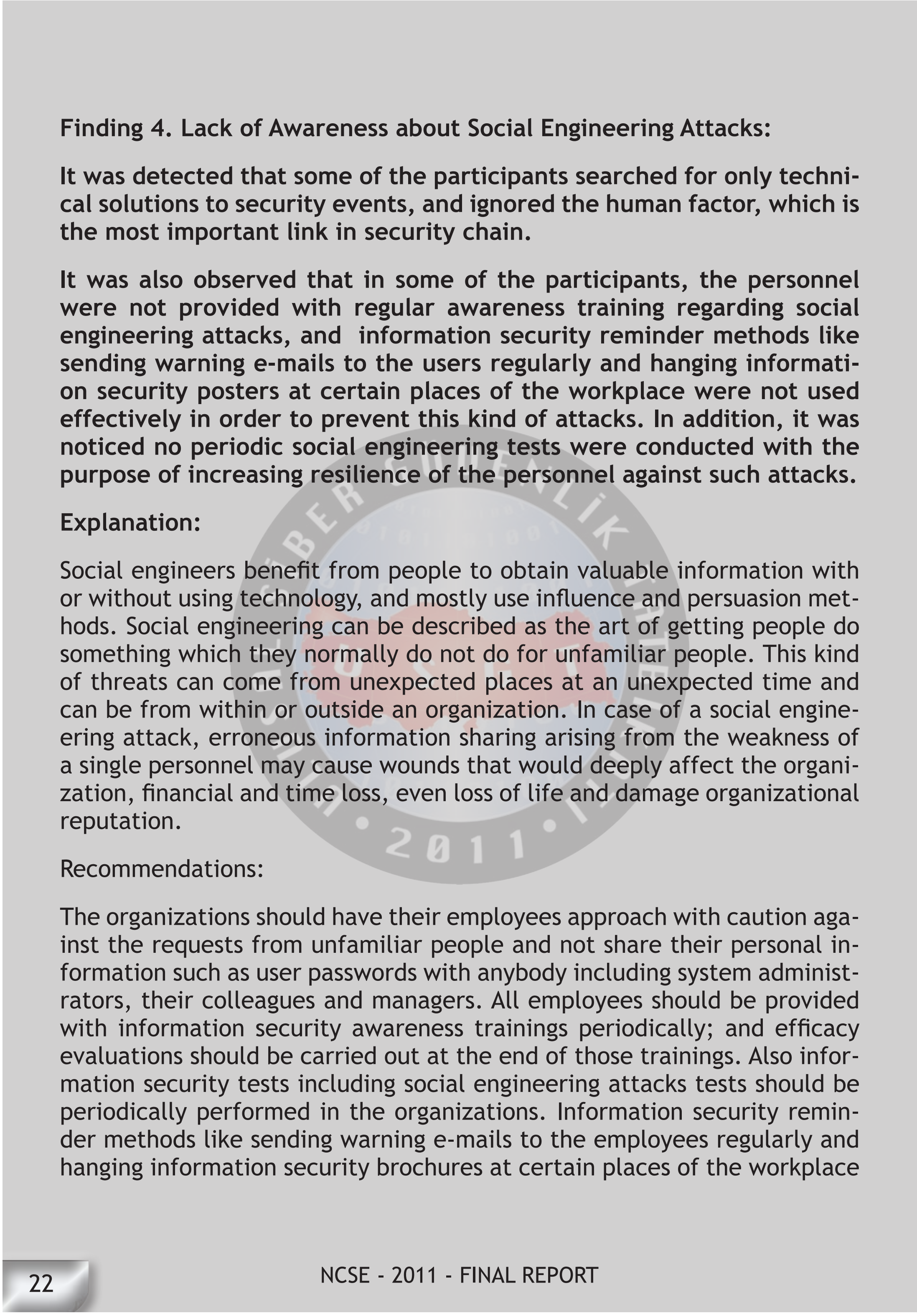
Explanation:

IDSs provide organizations to examine the received data packages and store the records of attacks or information collection activities via identified signs. IDSs are located on two points, one in the front and one on the back of firewall, in small and medium-sized networks. As to the large networks, IDS sensors can be installed on any point considered as necessary, further on the servers considered as important.

IDSs are not plug and play devices like many security hardware and software. The efficient use of IDSs depends on configuring them according to security needs to be determined after the installation, and the regular examination of the records the produced by them.

Recommendations:

The organizations which do not have an IDS should definitely have one and locate the system considering the complexities of their networks. Also, the system administrators should attend trainings about these systems, if possible take the related exams and receive their certificates. The system administrators should configure the IDSs properly according to the security needs of the systems they are responsible for, the records these systems produce should be regularly examined and reported. As the efficacy of these systems cannot be tracked instantly in application, the policies and procedures providing the efficient use of them should be identified by producing daily, weekly and monthly reports.



Finding 4. Lack of Awareness about Social Engineering Attacks:

It was detected that some of the participants searched for only technical solutions to security events, and ignored the human factor, which is the most important link in security chain.

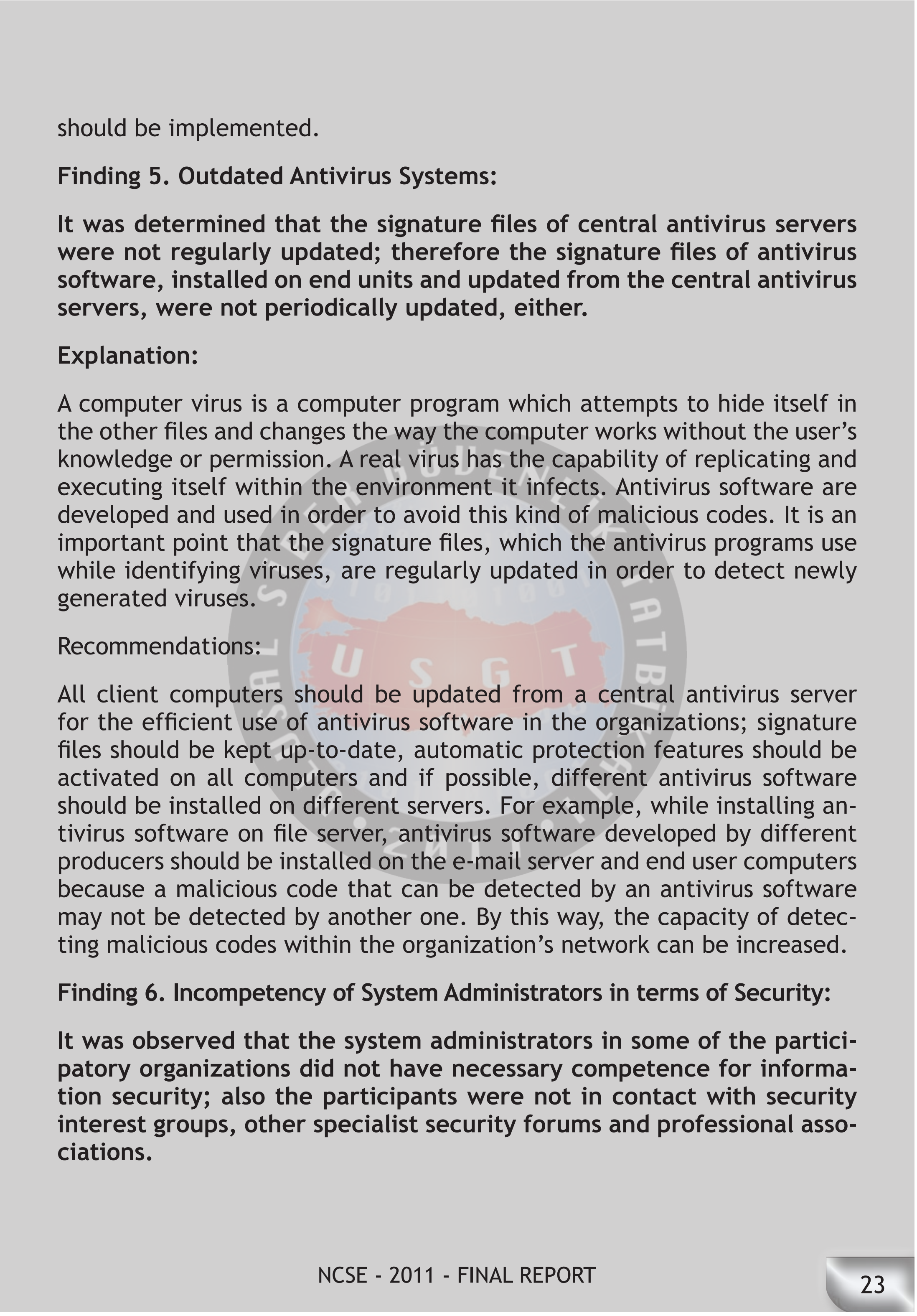
It was also observed that in some of the participants, the personnel were not provided with regular awareness training regarding social engineering attacks, and information security reminder methods like sending warning e-mails to the users regularly and hanging information security posters at certain places of the workplace were not used effectively in order to prevent this kind of attacks. In addition, it was noticed no periodic social engineering tests were conducted with the purpose of increasing resilience of the personnel against such attacks.

Explanation:

Social engineers benefit from people to obtain valuable information with or without using technology, and mostly use influence and persuasion methods. Social engineering can be described as the art of getting people do something which they normally do not do for unfamiliar people. This kind of threats can come from unexpected places at an unexpected time and can be from within or outside an organization. In case of a social engineering attack, erroneous information sharing arising from the weakness of a single personnel may cause wounds that would deeply affect the organization, financial and time loss, even loss of life and damage organizational reputation.

Recommendations:

The organizations should have their employees approach with caution against the requests from unfamiliar people and not share their personal information such as user passwords with anybody including system administrators, their colleagues and managers. All employees should be provided with information security awareness trainings periodically; and efficacy evaluations should be carried out at the end of those trainings. Also information security tests including social engineering attacks tests should be periodically performed in the organizations. Information security reminder methods like sending warning e-mails to the employees regularly and hanging information security brochures at certain places of the workplace



should be implemented.

Finding 5. Outdated Antivirus Systems:

It was determined that the signature files of central antivirus servers were not regularly updated; therefore the signature files of antivirus software, installed on end units and updated from the central antivirus servers, were not periodically updated, either.

Explanation:

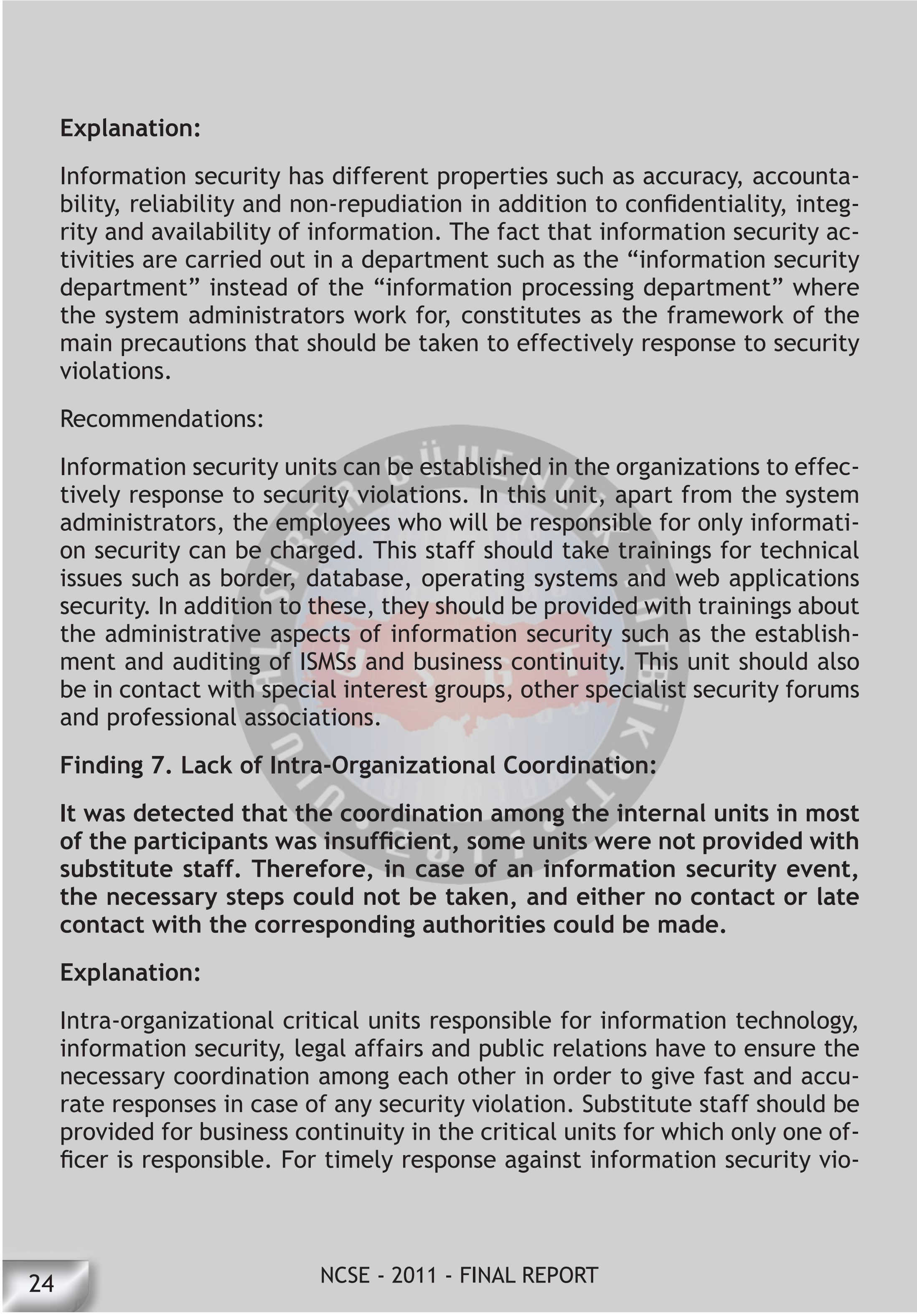
A computer virus is a computer program which attempts to hide itself in the other files and changes the way the computer works without the user's knowledge or permission. A real virus has the capability of replicating and executing itself within the environment it infects. Antivirus software are developed and used in order to avoid this kind of malicious codes. It is an important point that the signature files, which the antivirus programs use while identifying viruses, are regularly updated in order to detect newly generated viruses.

Recommendations:

All client computers should be updated from a central antivirus server for the efficient use of antivirus software in the organizations; signature files should be kept up-to-date, automatic protection features should be activated on all computers and if possible, different antivirus software should be installed on different servers. For example, while installing antivirus software on file server, antivirus software developed by different producers should be installed on the e-mail server and end user computers because a malicious code that can be detected by an antivirus software may not be detected by another one. By this way, the capacity of detecting malicious codes within the organization's network can be increased.

Finding 6. Incompetency of System Administrators in terms of Security:

It was observed that the system administrators in some of the participatory organizations did not have necessary competence for information security; also the participants were not in contact with security interest groups, other specialist security forums and professional associations.



Explanation:

Information security has different properties such as accuracy, accountability, reliability and non-repudiation in addition to confidentiality, integrity and availability of information. The fact that information security activities are carried out in a department such as the “information security department” instead of the “information processing department” where the system administrators work for, constitutes as the framework of the main precautions that should be taken to effectively response to security violations.

Recommendations:

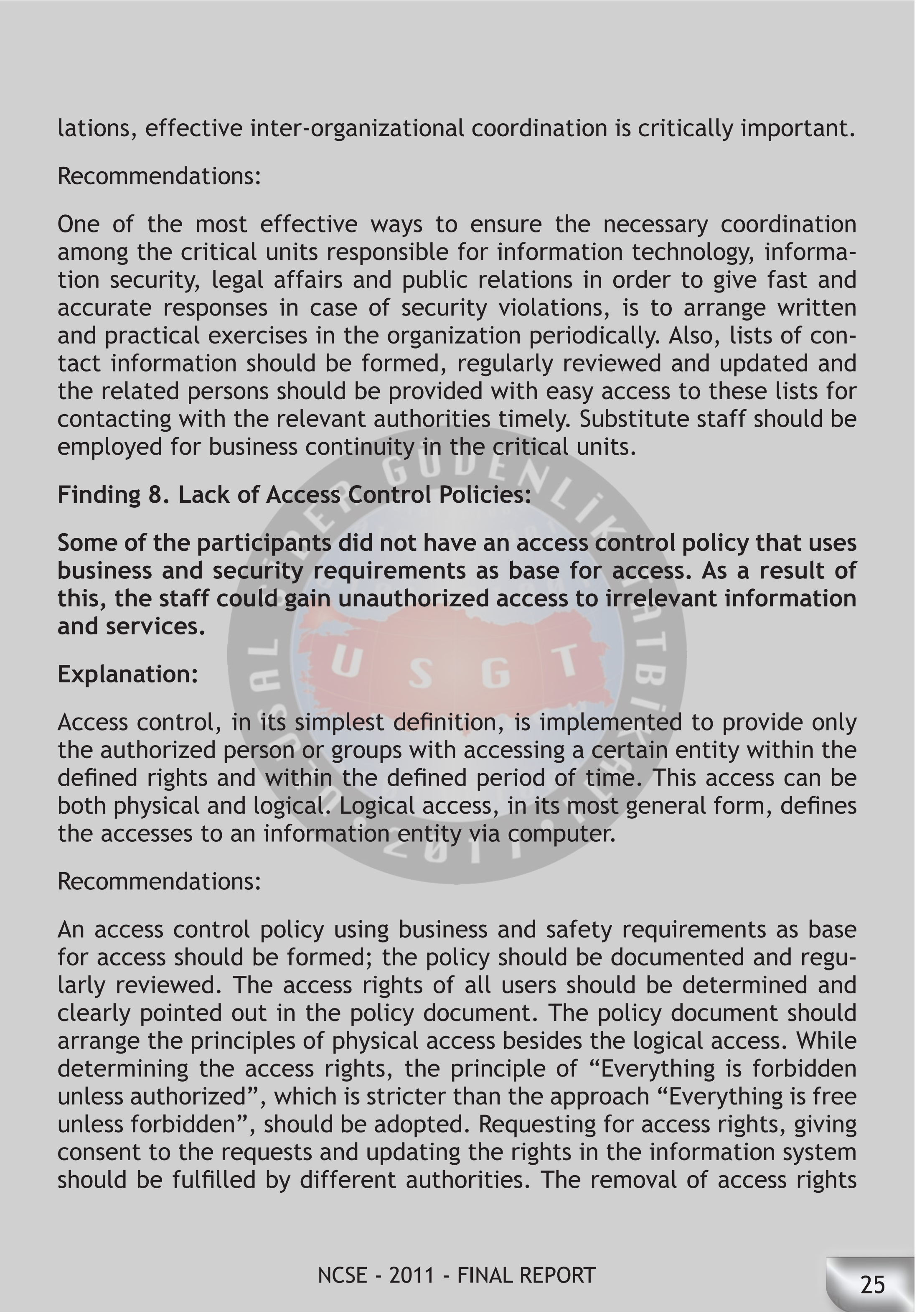
Information security units can be established in the organizations to effectively response to security violations. In this unit, apart from the system administrators, the employees who will be responsible for only information security can be charged. This staff should take trainings for technical issues such as border, database, operating systems and web applications security. In addition to these, they should be provided with trainings about the administrative aspects of information security such as the establishment and auditing of ISMSs and business continuity. This unit should also be in contact with special interest groups, other specialist security forums and professional associations.

Finding 7. Lack of Intra-Organizational Coordination:

It was detected that the coordination among the internal units in most of the participants was insufficient, some units were not provided with substitute staff. Therefore, in case of an information security event, the necessary steps could not be taken, and either no contact or late contact with the corresponding authorities could be made.

Explanation:

Intra-organizational critical units responsible for information technology, information security, legal affairs and public relations have to ensure the necessary coordination among each other in order to give fast and accurate responses in case of any security violation. Substitute staff should be provided for business continuity in the critical units for which only one officer is responsible. For timely response against information security vio-



lations, effective inter-organizational coordination is critically important.

Recommendations:

One of the most effective ways to ensure the necessary coordination among the critical units responsible for information technology, information security, legal affairs and public relations in order to give fast and accurate responses in case of security violations, is to arrange written and practical exercises in the organization periodically. Also, lists of contact information should be formed, regularly reviewed and updated and the related persons should be provided with easy access to these lists for contacting with the relevant authorities timely. Substitute staff should be employed for business continuity in the critical units.

Finding 8. Lack of Access Control Policies:

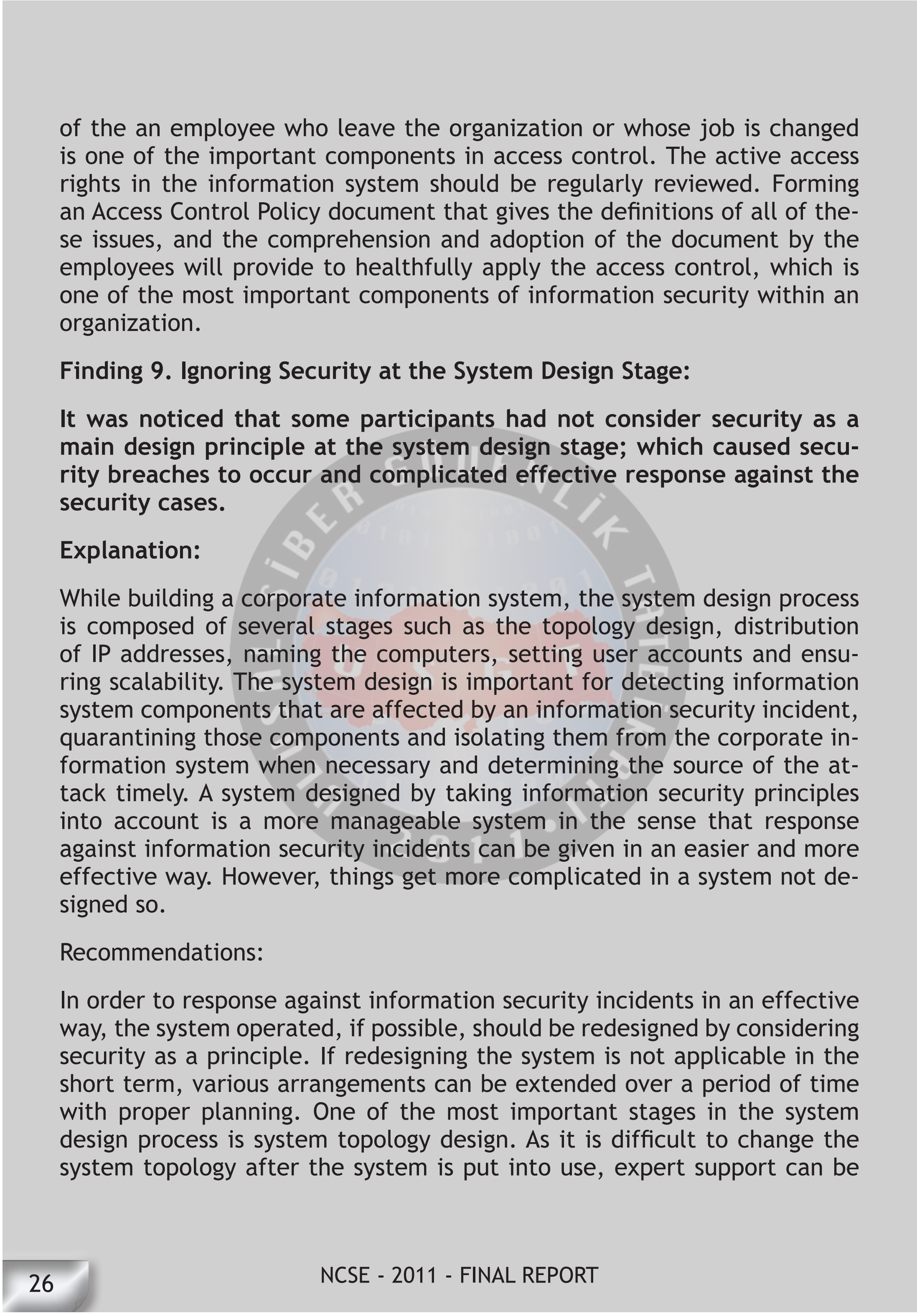
Some of the participants did not have an access control policy that uses business and security requirements as base for access. As a result of this, the staff could gain unauthorized access to irrelevant information and services.

Explanation:

Access control, in its simplest definition, is implemented to provide only the authorized person or groups with accessing a certain entity within the defined rights and within the defined period of time. This access can be both physical and logical. Logical access, in its most general form, defines the accesses to an information entity via computer.

Recommendations:

An access control policy using business and safety requirements as base for access should be formed; the policy should be documented and regularly reviewed. The access rights of all users should be determined and clearly pointed out in the policy document. The policy document should arrange the principles of physical access besides the logical access. While determining the access rights, the principle of “Everything is forbidden unless authorized”, which is stricter than the approach “Everything is free unless forbidden”, should be adopted. Requesting for access rights, giving consent to the requests and updating the rights in the information system should be fulfilled by different authorities. The removal of access rights



of the an employee who leave the organization or whose job is changed is one of the important components in access control. The active access rights in the information system should be regularly reviewed. Forming an Access Control Policy document that gives the definitions of all of these issues, and the comprehension and adoption of the document by the employees will provide to healthfully apply the access control, which is one of the most important components of information security within an organization.

Finding 9. Ignoring Security at the System Design Stage:

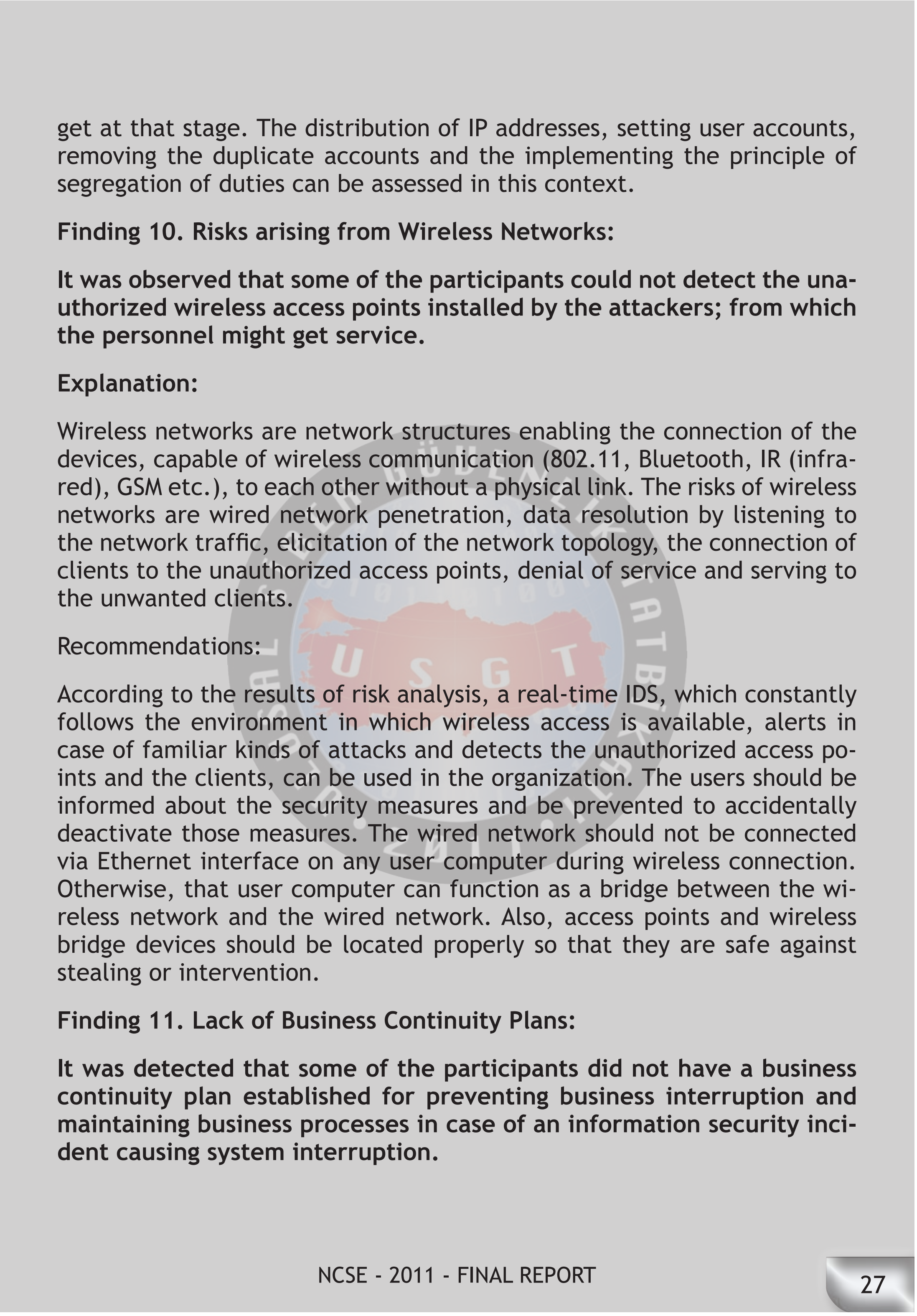
It was noticed that some participants had not consider security as a main design principle at the system design stage; which caused security breaches to occur and complicated effective response against the security cases.

Explanation:

While building a corporate information system, the system design process is composed of several stages such as the topology design, distribution of IP addresses, naming the computers, setting user accounts and ensuring scalability. The system design is important for detecting information system components that are affected by an information security incident, quarantining those components and isolating them from the corporate information system when necessary and determining the source of the attack timely. A system designed by taking information security principles into account is a more manageable system in the sense that response against information security incidents can be given in an easier and more effective way. However, things get more complicated in a system not designed so.

Recommendations:

In order to response against information security incidents in an effective way, the system operated, if possible, should be redesigned by considering security as a principle. If redesigning the system is not applicable in the short term, various arrangements can be extended over a period of time with proper planning. One of the most important stages in the system design process is system topology design. As it is difficult to change the system topology after the system is put into use, expert support can be



get at that stage. The distribution of IP addresses, setting user accounts, removing the duplicate accounts and the implementing the principle of segregation of duties can be assessed in this context.

Finding 10. Risks arising from Wireless Networks:

It was observed that some of the participants could not detect the unauthorized wireless access points installed by the attackers; from which the personnel might get service.

Explanation:

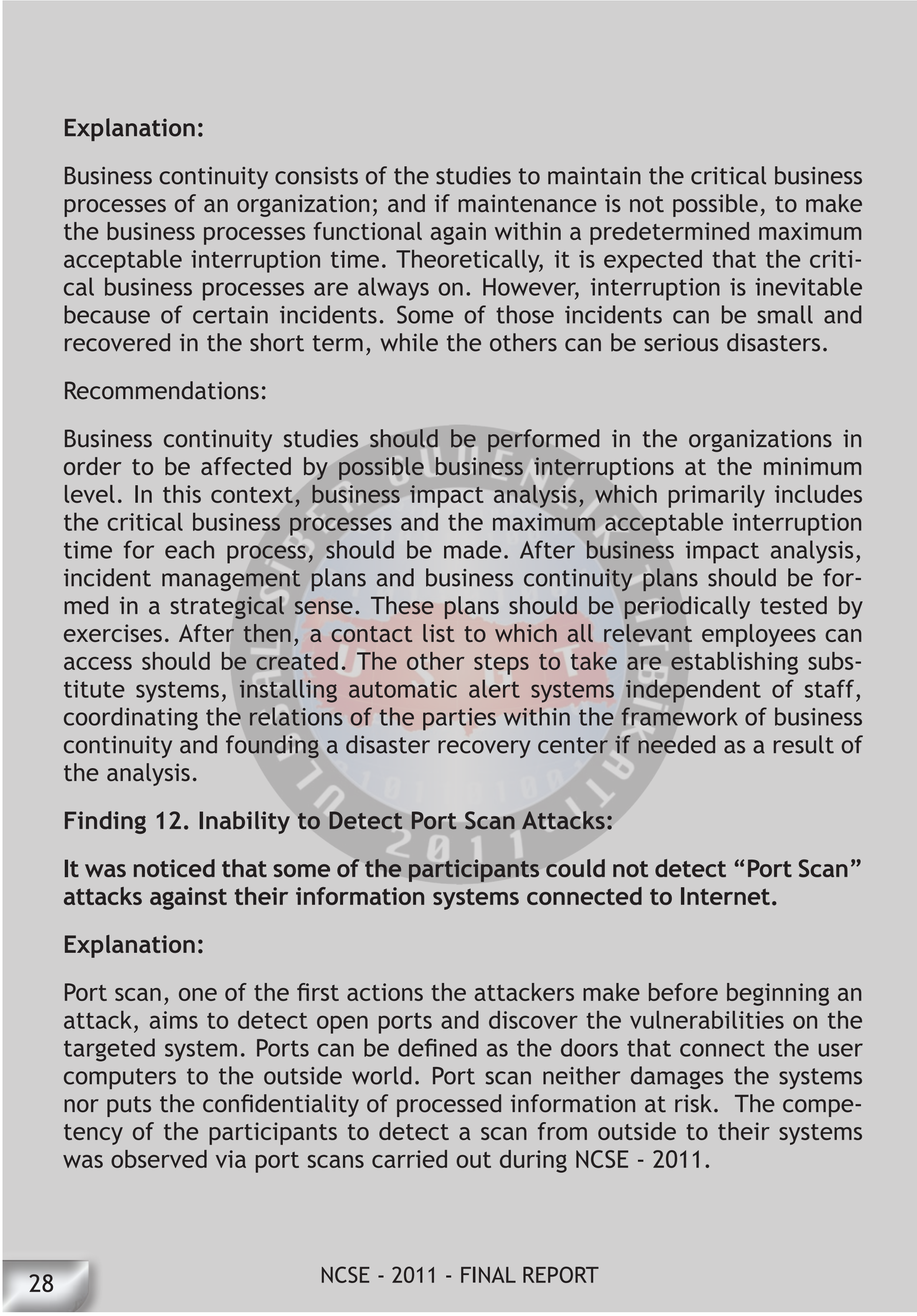
Wireless networks are network structures enabling the connection of the devices, capable of wireless communication (802.11, Bluetooth, IR (infra-red), GSM etc.), to each other without a physical link. The risks of wireless networks are wired network penetration, data resolution by listening to the network traffic, elicitation of the network topology, the connection of clients to the unauthorized access points, denial of service and serving to the unwanted clients.

Recommendations:

According to the results of risk analysis, a real-time IDS, which constantly follows the environment in which wireless access is available, alerts in case of familiar kinds of attacks and detects the unauthorized access points and the clients, can be used in the organization. The users should be informed about the security measures and be prevented to accidentally deactivate those measures. The wired network should not be connected via Ethernet interface on any user computer during wireless connection. Otherwise, that user computer can function as a bridge between the wireless network and the wired network. Also, access points and wireless bridge devices should be located properly so that they are safe against stealing or intervention.

Finding 11. Lack of Business Continuity Plans:

It was detected that some of the participants did not have a business continuity plan established for preventing business interruption and maintaining business processes in case of an information security incident causing system interruption.



Explanation:

Business continuity consists of the studies to maintain the critical business processes of an organization; and if maintenance is not possible, to make the business processes functional again within a predetermined maximum acceptable interruption time. Theoretically, it is expected that the critical business processes are always on. However, interruption is inevitable because of certain incidents. Some of those incidents can be small and recovered in the short term, while the others can be serious disasters.

Recommendations:

Business continuity studies should be performed in the organizations in order to be affected by possible business interruptions at the minimum level. In this context, business impact analysis, which primarily includes the critical business processes and the maximum acceptable interruption time for each process, should be made. After business impact analysis, incident management plans and business continuity plans should be formed in a strategical sense. These plans should be periodically tested by exercises. After then, a contact list to which all relevant employees can access should be created. The other steps to take are establishing substitute systems, installing automatic alert systems independent of staff, coordinating the relations of the parties within the framework of business continuity and founding a disaster recovery center if needed as a result of the analysis.

Finding 12. Inability to Detect Port Scan Attacks:

It was noticed that some of the participants could not detect "Port Scan" attacks against their information systems connected to Internet.

Explanation:

Port scan, one of the first actions the attackers make before beginning an attack, aims to detect open ports and discover the vulnerabilities on the targeted system. Ports can be defined as the doors that connect the user computers to the outside world. Port scan neither damages the systems nor puts the confidentiality of processed information at risk. The competency of the participants to detect a scan from outside to their systems was observed via port scans carried out during NCSE - 2011.

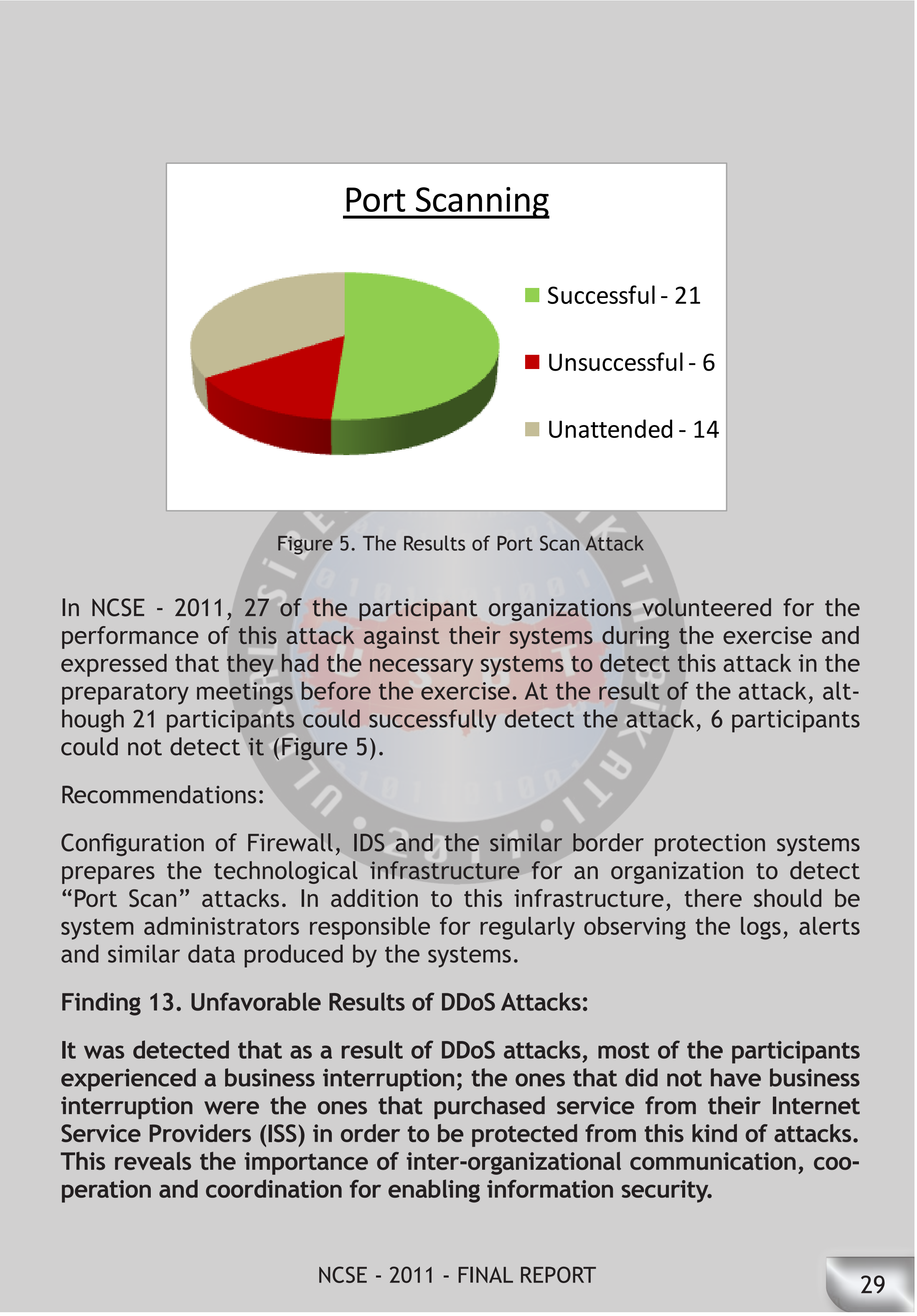


Figure 5. The Results of Port Scan Attack

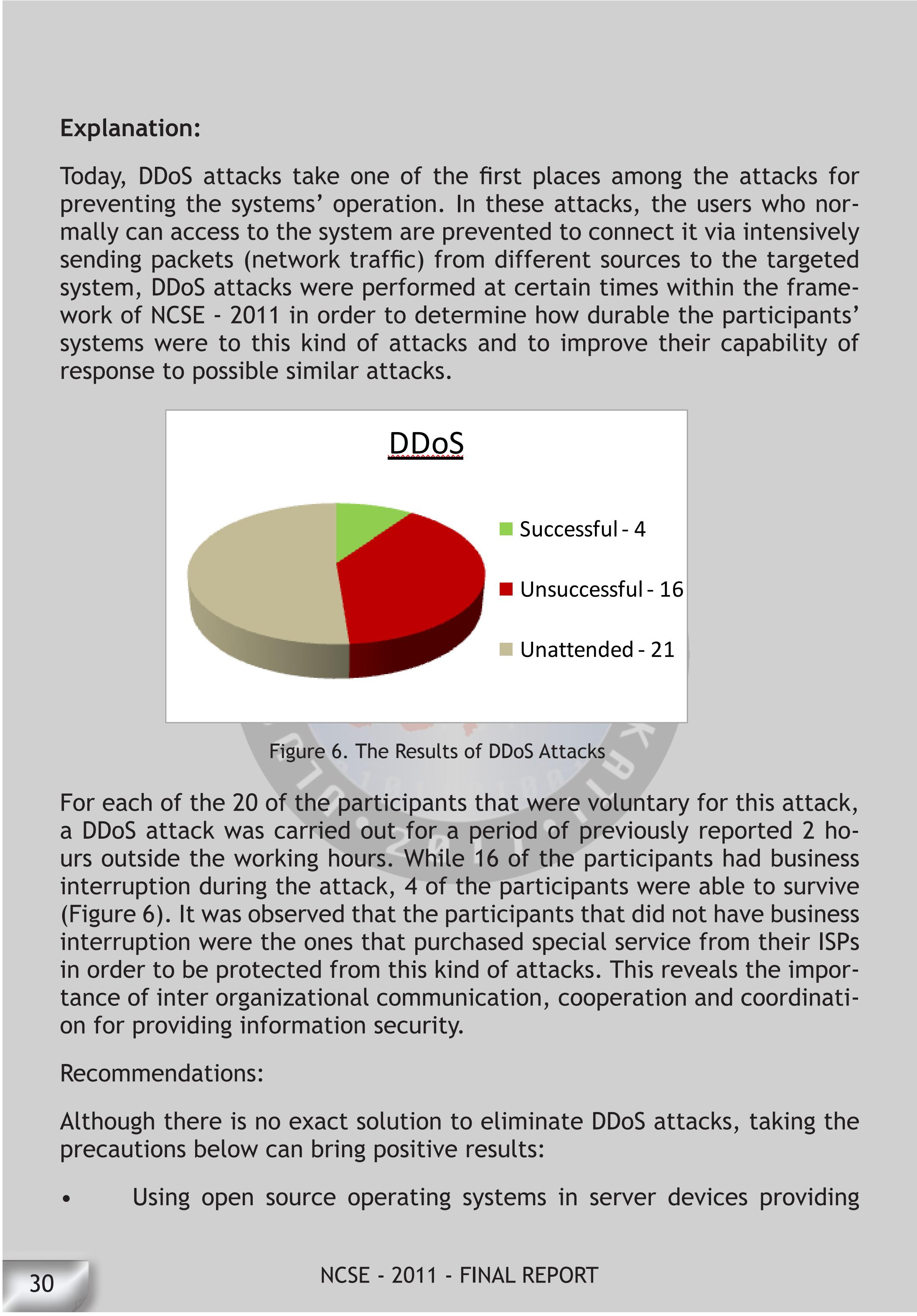
In NCSE - 2011, 27 of the participant organizations volunteered for the performance of this attack against their systems during the exercise and expressed that they had the necessary systems to detect this attack in the preparatory meetings before the exercise. At the result of the attack, although 21 participants could successfully detect the attack, 6 participants could not detect it (Figure 5).

Recommendations:

Configuration of Firewall, IDS and the similar border protection systems prepares the technological infrastructure for an organization to detect "Port Scan" attacks. In addition to this infrastructure, there should be system administrators responsible for regularly observing the logs, alerts and similar data produced by the systems.

Finding 13. Unfavorable Results of DDoS Attacks:

It was detected that as a result of DDoS attacks, most of the participants experienced a business interruption; the ones that did not have business interruption were the ones that purchased service from their Internet Service Providers (ISS) in order to be protected from this kind of attacks. This reveals the importance of inter-organizational communication, cooperation and coordination for enabling information security.



Explanation:

Today, DDoS attacks take one of the first places among the attacks for preventing the systems’ operation. In these attacks, the users who normally can access to the system are prevented to connect it via intensively sending packets (network traffic) from different sources to the targeted system, DDoS attacks were performed at certain times within the framework of NCSE - 2011 in order to determine how durable the participants’ systems were to this kind of attacks and to improve their capability of response to possible similar attacks.

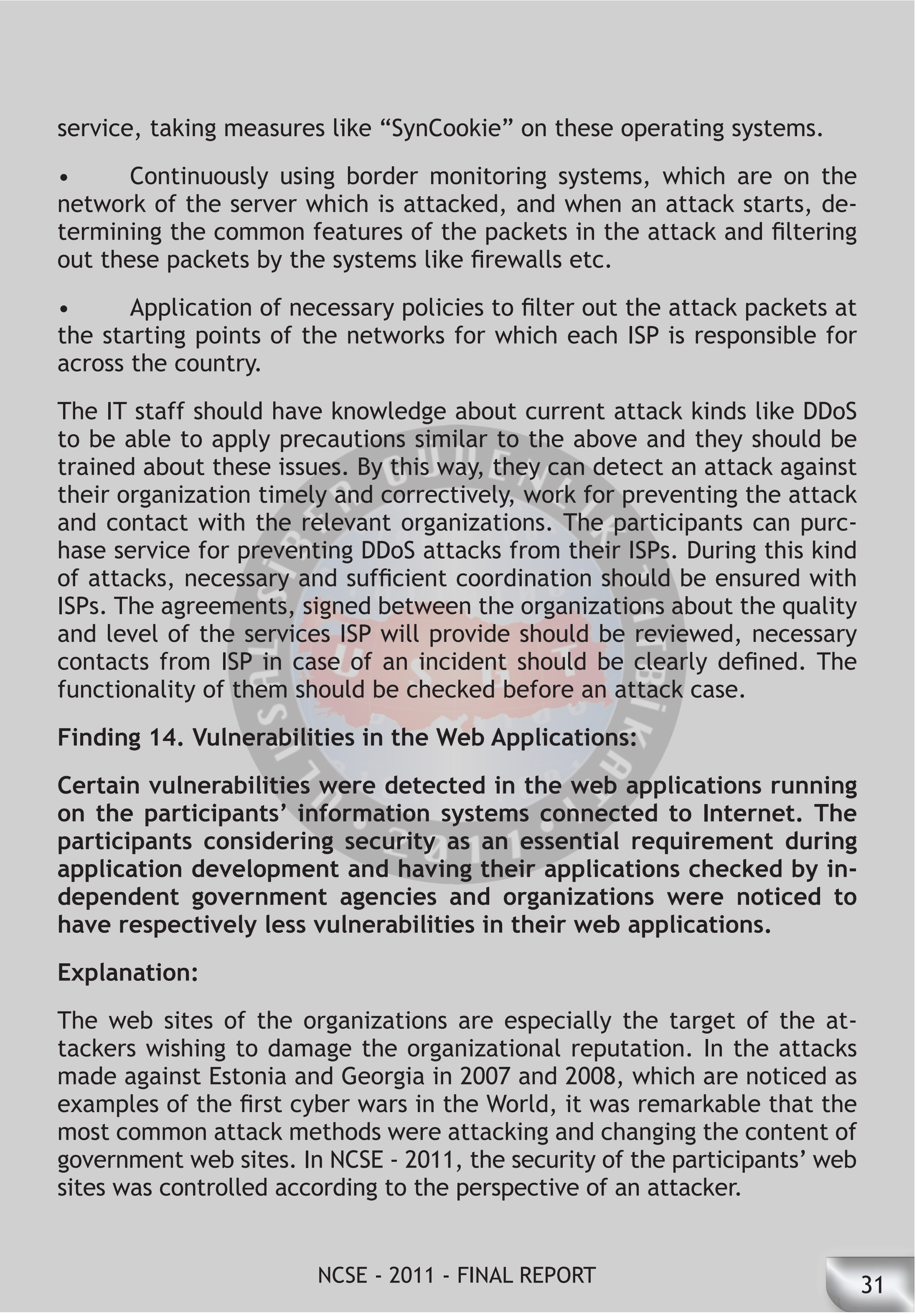
Figure 6. The Results of DDoS Attacks

For each of the 20 of the participants that were voluntary for this attack, a DDoS attack was carried out for a period of previously reported 2 hours outside the working hours. While 16 of the participants had business interruption during the attack, 4 of the participants were able to survive (Figure 6). It was observed that the participants that did not have business interruption were the ones that purchased special service from their ISPs in order to be protected from this kind of attacks. This reveals the importance of inter organizational communication, cooperation and coordination for providing information security.

Recommendations:

Although there is no exact solution to eliminate DDoS attacks, taking the precautions below can bring positive results:

- Using open source operating systems in server devices providing



service, taking measures like "SynCookie" on these operating systems.

- Continuously using border monitoring systems, which are on the network of the server which is attacked, and when an attack starts, determining the common features of the packets in the attack and filtering out these packets by the systems like firewalls etc.

- Application of necessary policies to filter out the attack packets at the starting points of the networks for which each ISP is responsible for across the country.

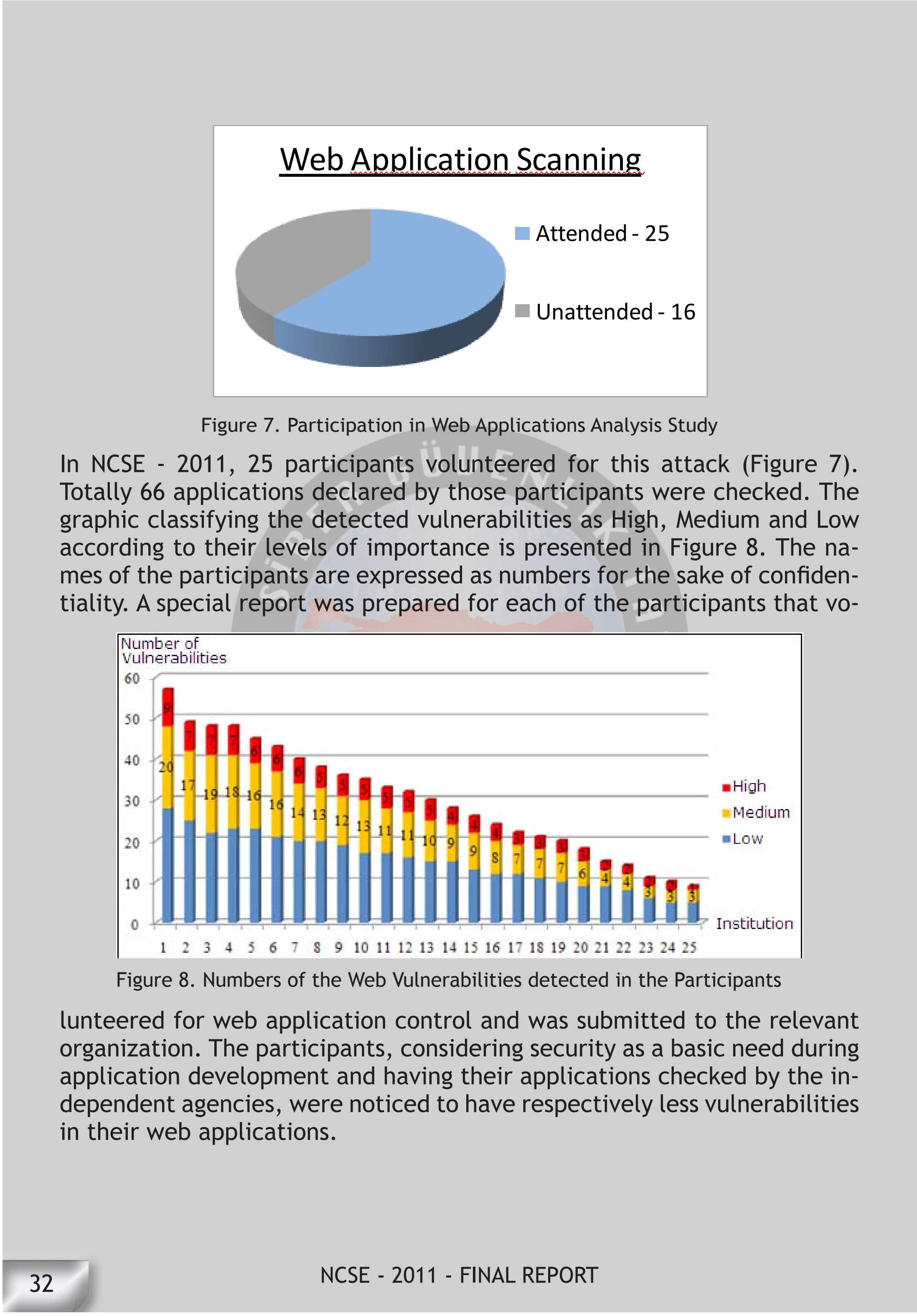
The IT staff should have knowledge about current attack kinds like DDoS to be able to apply precautions similar to the above and they should be trained about these issues. By this way, they can detect an attack against their organization timely and correctively, work for preventing the attack and contact with the relevant organizations. The participants can purchase service for preventing DDoS attacks from their ISPs. During this kind of attacks, necessary and sufficient coordination should be ensured with ISPs. The agreements, signed between the organizations about the quality and level of the services ISP will provide should be reviewed, necessary contacts from ISP in case of an incident should be clearly defined. The functionality of them should be checked before an attack case.

Finding 14. Vulnerabilities in the Web Applications:

Certain vulnerabilities were detected in the web applications running on the participants' information systems connected to Internet. The participants considering security as an essential requirement during application development and having their applications checked by independent government agencies and organizations were noticed to have respectively less vulnerabilities in their web applications.

Explanation:

The web sites of the organizations are especially the target of the attackers wishing to damage the organizational reputation. In the attacks made against Estonia and Georgia in 2007 and 2008, which are noticed as examples of the first cyber wars in the World, it was remarkable that the most common attack methods were attacking and changing the content of government web sites. In NCSE - 2011, the security of the participants' web sites was controlled according to the perspective of an attacker.

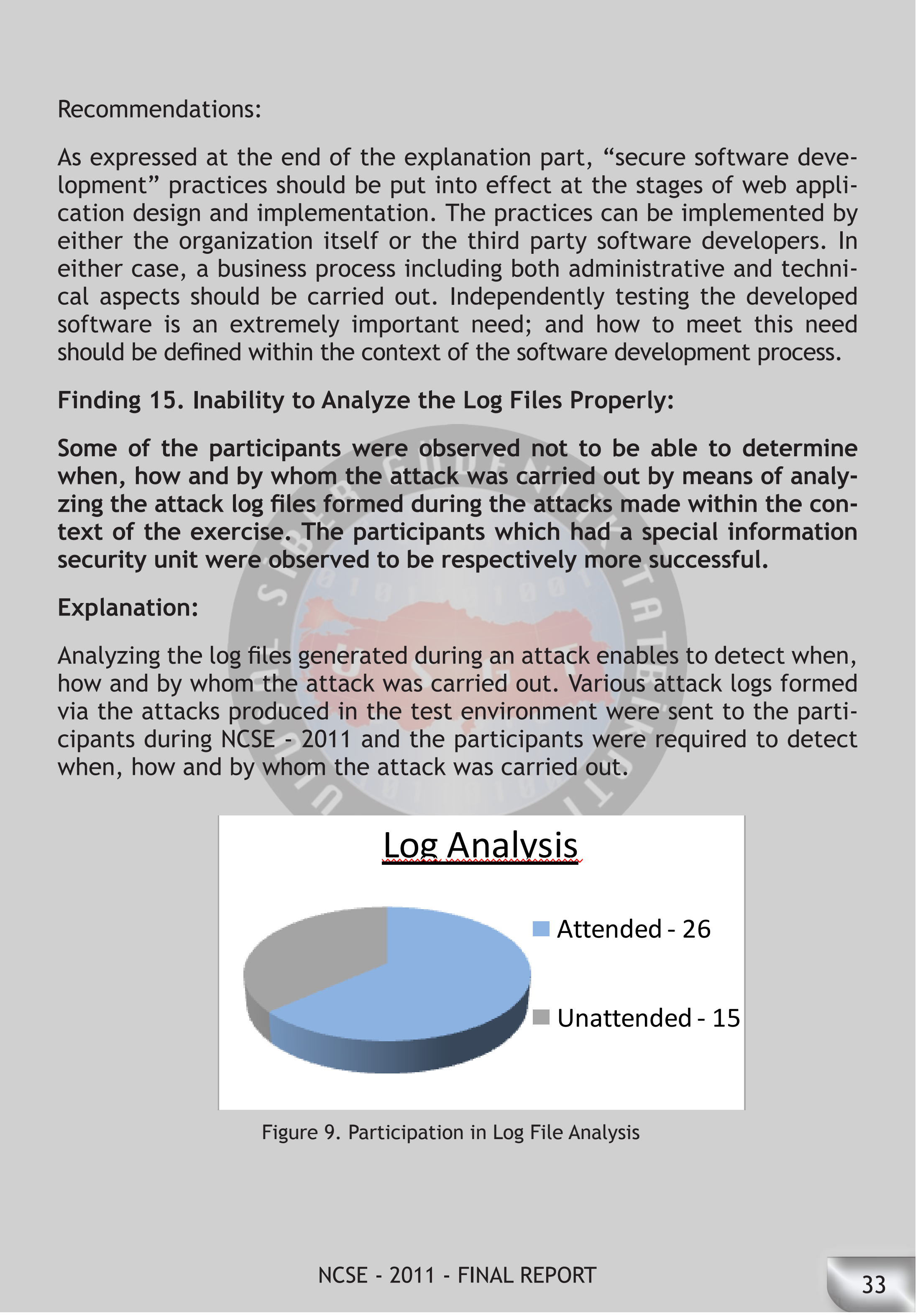


Web Application Scanning
Attended - 25
Unattended - 16

Figure 7. Participation in Web Applications Analysis Study

In NCSE - 2011, 25 participants volunteered for this attack (Figure 7). Totally 66 applications declared by those participants were checked. The graphic classifying the detected vulnerabilities as High, Medium and Low according to their levels of importance is presented in Figure 8. The names of the participants are expressed as numbers for the sake of confidentiality. A special report was prepared for each of the participants that volunteered for web application control and was submitted to the relevant organization. The participants, considering security as a basic need during application development and having their applications checked by the independent agencies, were noticed to have respectively less vulnerabilities in their web applications.

Figure 8. Numbers of the Web Vulnerabilities detected in the Participants



Recommendations:

As expressed at the end of the explanation part, "secure software development" practices should be put into effect at the stages of web application design and implementation. The practices can be implemented by either the organization itself or the third party software developers. In either case, a business process including both administrative and technical aspects should be carried out. Independently testing the developed software is an extremely important need; and how to meet this need should be defined within the context of the software development process.

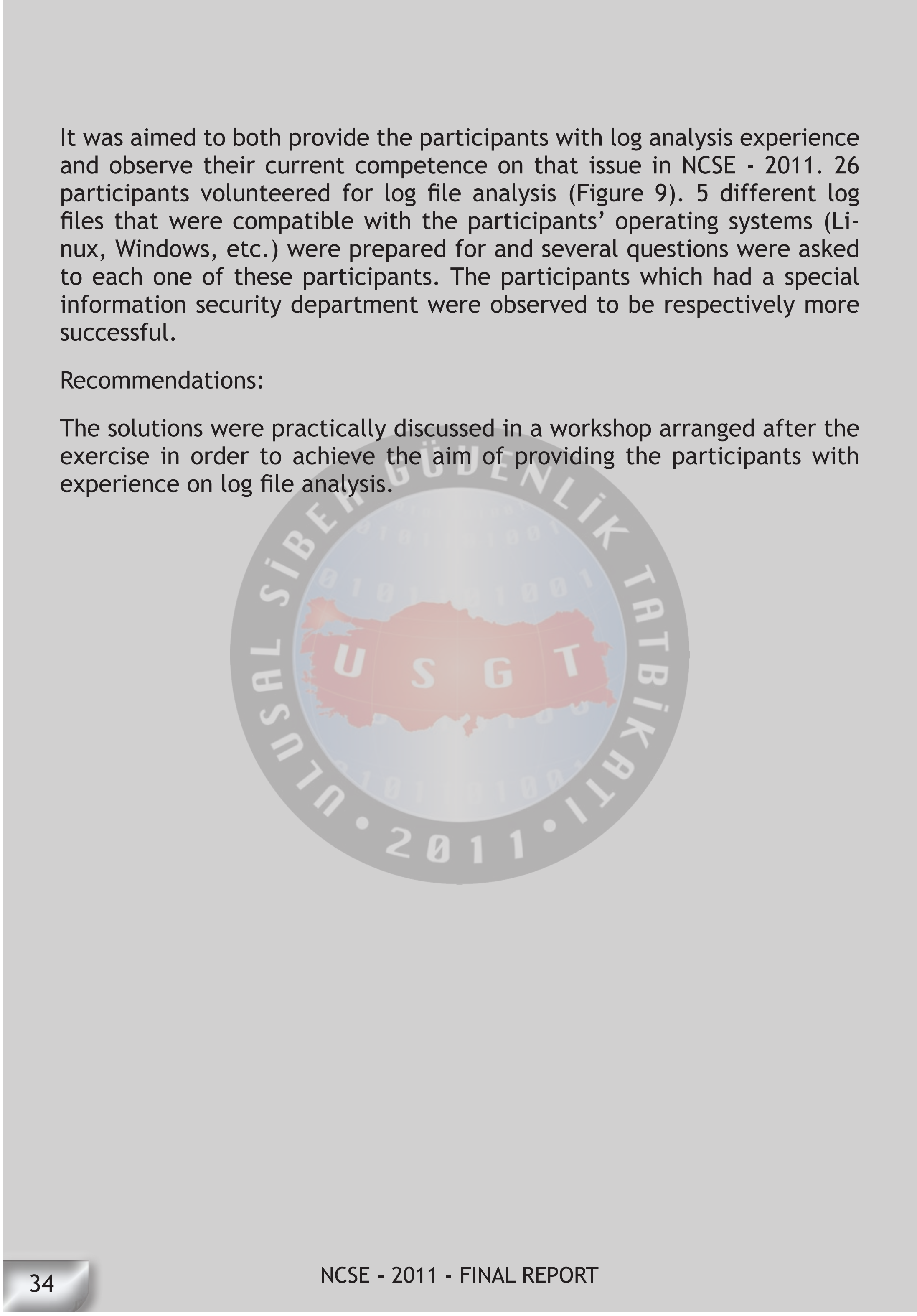
Finding 15. Inability to Analyze the Log Files Properly:

Some of the participants were observed not to be able to determine when, how and by whom the attack was carried out by means of analyzing the attack log files formed during the attacks made within the context of the exercise. The participants which had a special information security unit were observed to be respectively more successful.

Explanation:

Analyzing the log files generated during an attack enables to detect when, how and by whom the attack was carried out. Various attack logs formed via the attacks produced in the test environment were sent to the participants during NCSE - 2011 and the participants were required to detect when, how and by whom the attack was carried out.

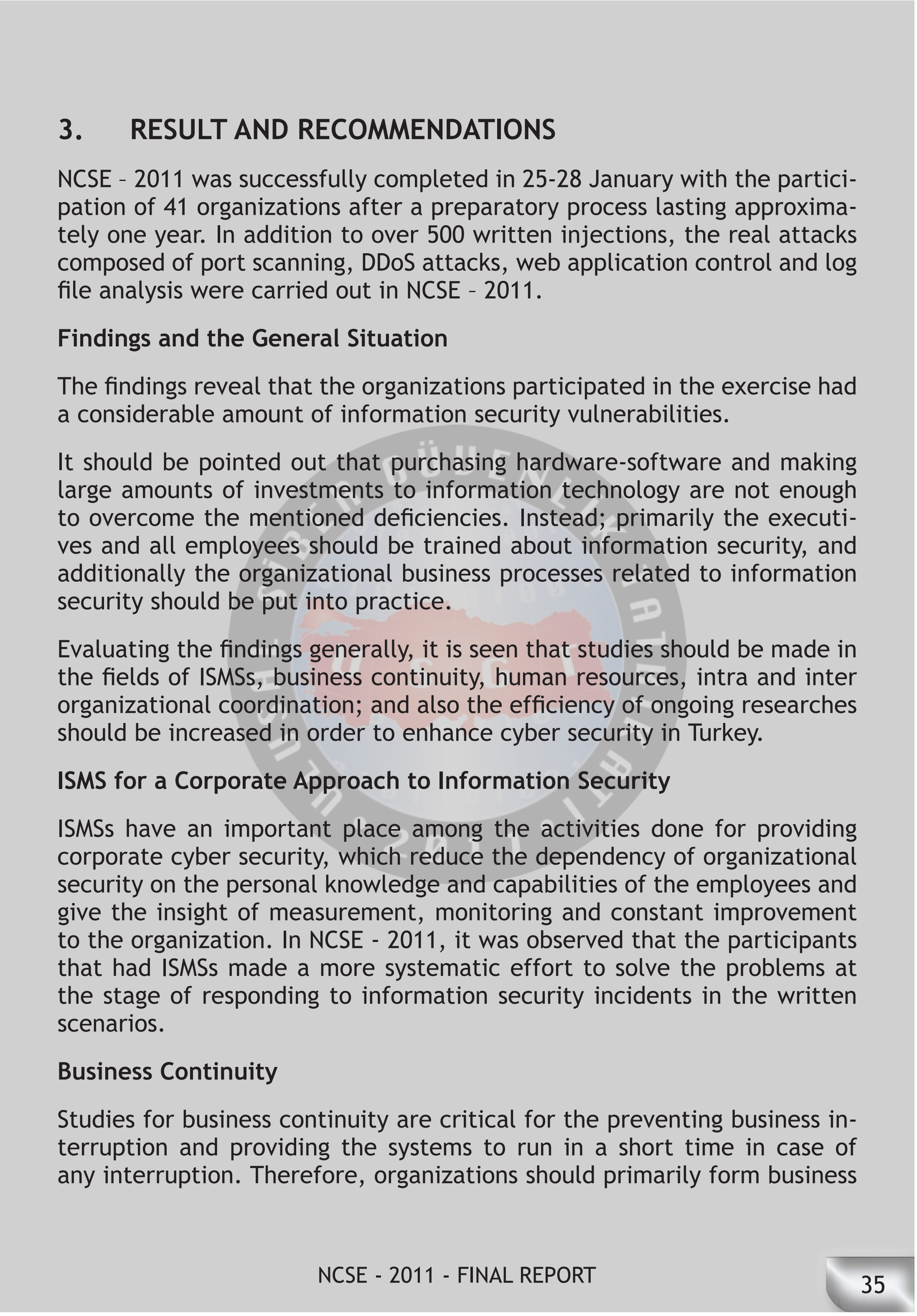
Figure 9. Participation in Log File Analysis



It was aimed to both provide the participants with log analysis experience and observe their current competence on that issue in NCSE - 2011. 26 participants volunteered for log file analysis (Figure 9). 5 different log files that were compatible with the participants' operating systems (Linux, Windows, etc.) were prepared for and several questions were asked to each one of these participants. The participants which had a special information security department were observed to be respectively more successful.

Recommendations:

The solutions were practically discussed in a workshop arranged after the exercise in order to achieve the aim of providing the participants with experience on log file analysis.



3. RESULT AND RECOMMENDATIONS

NCSE – 2011 was successfully completed in 25-28 January with the participation of 41 organizations after a preparatory process lasting approximately one year. In addition to over 500 written injections, the real attacks composed of port scanning, DDoS attacks, web application control and log file analysis were carried out in NCSE – 2011.

Findings and the General Situation

The findings reveal that the organizations participated in the exercise had a considerable amount of information security vulnerabilities.

It should be pointed out that purchasing hardware-software and making large amounts of investments to information technology are not enough to overcome the mentioned deficiencies. Instead; primarily the executives and all employees should be trained about information security, and additionally the organizational business processes related to information security should be put into practice.

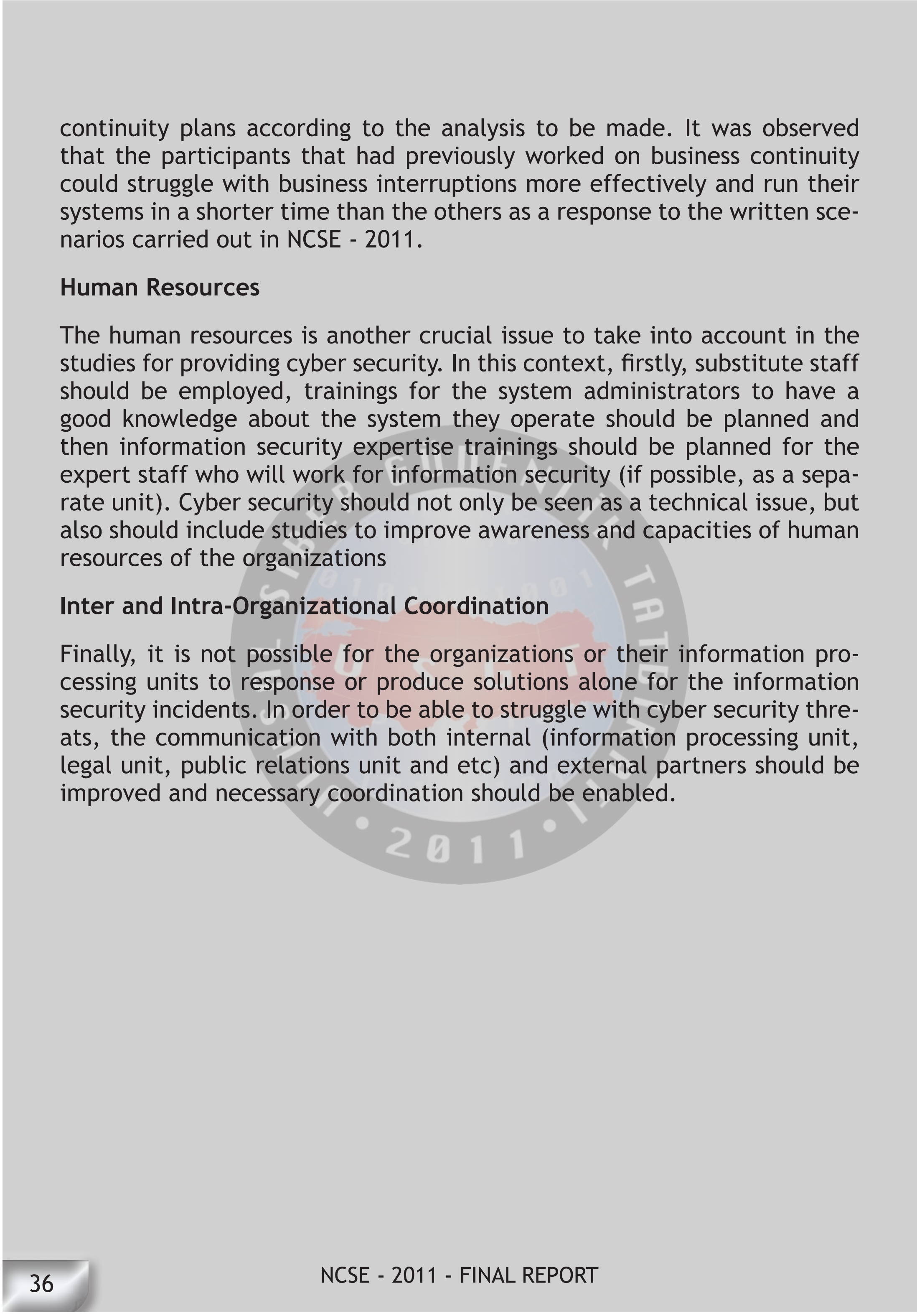
Evaluating the findings generally, it is seen that studies should be made in the fields of ISMSs, business continuity, human resources, intra and inter organizational coordination; and also the efficiency of ongoing researches should be increased in order to enhance cyber security in Turkey.

ISMS for a Corporate Approach to Information Security

ISMSs have an important place among the activities done for providing corporate cyber security, which reduce the dependency of organizational security on the personal knowledge and capabilities of the employees and give the insight of measurement, monitoring and constant improvement to the organization. In NCSE - 2011, it was observed that the participants that had ISMSs made a more systematic effort to solve the problems at the stage of responding to information security incidents in the written scenarios.

Business Continuity

Studies for business continuity are critical for the preventing business interruption and providing the systems to run in a short time in case of any interruption. Therefore, organizations should primarily form business



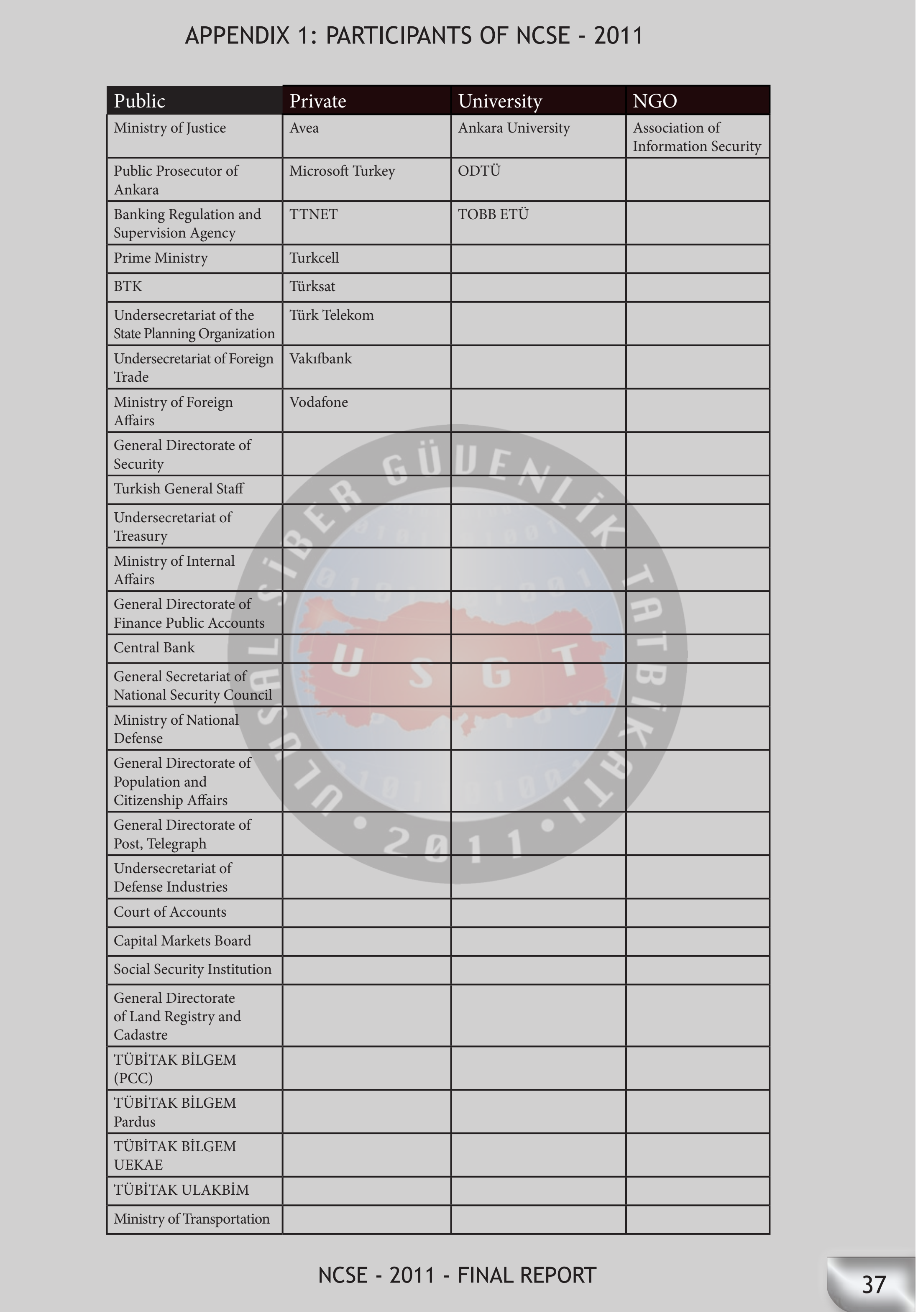
continuity plans according to the analysis to be made. It was observed that the participants that had previously worked on business continuity could struggle with business interruptions more effectively and run their systems in a shorter time than the others as a response to the written scenarios carried out in NCSE - 2011.

Human Resources

The human resources is another crucial issue to take into account in the studies for providing cyber security. In this context, firstly, substitute staff should be employed, trainings for the system administrators to have a good knowledge about the system they operate should be planned and then information security expertise trainings should be planned for the expert staff who will work for information security (if possible, as a separate unit). Cyber security should not only be seen as a technical issue, but also should include studies to improve awareness and capacities of human resources of the organizations

Inter and Intra-Organizational Coordination

Finally, it is not possible for the organizations or their information processing units to response or produce solutions alone for the information security incidents. In order to be able to struggle with cyber security threats, the communication with both internal (information processing unit, legal unit, public relations unit and etc) and external partners should be improved and necessary coordination should be enabled.



APPENDIX 1: PARTICIPANTS OF NCSE - 2011

Public	Private	University	NGO
Ministry of Justice	Avea	Ankara University	Association of Information Security
Public Prosecutor of Ankara	Microsoft Turkey	ODTÜ	
Banking Regulation and Supervision Agency	TTNET	TOBB ETÜ	
Prime Ministry	Turkcell		
BTK	Türksat		
Undersecretariat of the State Planning Organization	Türk Telekom		
Undersecretariat of Foreign Trade	Vakıfbank		
Ministry of Foreign Affairs	Vodafone		
General Directorate of Security			
Turkish General Staff			
Undersecretariat of Treasury			
Ministry of Internal Affairs			
General Directorate of Finance Public Accounts			
Central Bank			
General Secretariat of National Security Council			
Ministry of National Defense			
General Directorate of Population and Citizenship Affairs			
General Directorate of Post, Telegraph			
Undersecretariat of Defense Industries			
Court of Accounts			
Capital Markets Board			
Social Security Institution			
General Directorate of Land Registry and Cadastre			
TÜBİTAK BİLGEM (PCC)			
TÜBİTAK BİLGEM Pardus			
TÜBİTAK BİLGEM UEKAE			
TÜBİTAK ULAKBİM			
Ministry of Transportation			

APPENDIX 2: PHOTOS FROM NCSE – 2011

NCSE - 2011 - FINAL REPORT

38

NCSE - 2011 - FINAL REPORT

39

USGT
DEVLET PLANLAMA TEŞKİLATI

NCSE - 2011 - FINAL REPORT

41

42

NCSE - 2011 - FINAL REPORT

ULUSAL SİBER GÜVENLİK TATBİKATI
• 2011 •
USGT
BTK
BİLGİ TEKNOLOJİLERİ
VE İLETİŞİM KURUMU
TÜBİTAK

2 System Security Research in Europe: A Research Roadmap

Authors SysSec consortium

Dissemination SysSec website exclusive

This whitepaper is an extended version of the research roadmap produced by the SysSec consortium, detailing the key research directions in Systems Security in Europe.

SEVENTH FRAMEWORK PROGRAMME

Information & Communication Technologies
Trustworthy ICT

NETWORK OF EXCELLENCE

syssec

A European Network of Excellence in Managing Threats and Vulnerabilities in the Future Internet: *Europe for the World* [†]

System Security Research in Europe: A Research Roadmap

Abstract: During its first year of operation, the SysSec network of excellence has created a roadmap for System Security Research. This white paper presents a summary of this Roadmap along with its expected impact on the European industry, the European Citizen, and Society in general. In addition, this document describes the procedure we propose to maintain the roadmap and update its content at the end of each project year.

The *SysSec* consortium consists of:

FORTH-ICS	Coordinator	Greece
Politecnico Di Milano	Principal Contractor	Italy
Vrije Universiteit Amsterdam	Principal Contractor	The Netherlands
Institut Eurécom	Principal Contractor	France
IICT-BAS	Principal Contractor	Bulgaria
Technical University of Vienna	Principal Contractor	Austria
Chalmers University	Principal Contractor	Sweden
TUBITAK-BILGEM	Principal Contractor	Turkey

[†] The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 257007.

1 Introduction

One of the main activities of the SysSec Network of Excellence consists of defining and updating a yearly *roadmap* of research areas that need to be addressed in order to mitigate the threats identified by each Working Group. The roadmap will serve the twofold objective of driving the research conducted by the SysSec's partners, and of serving as a guideline for other researchers in the field of system security.

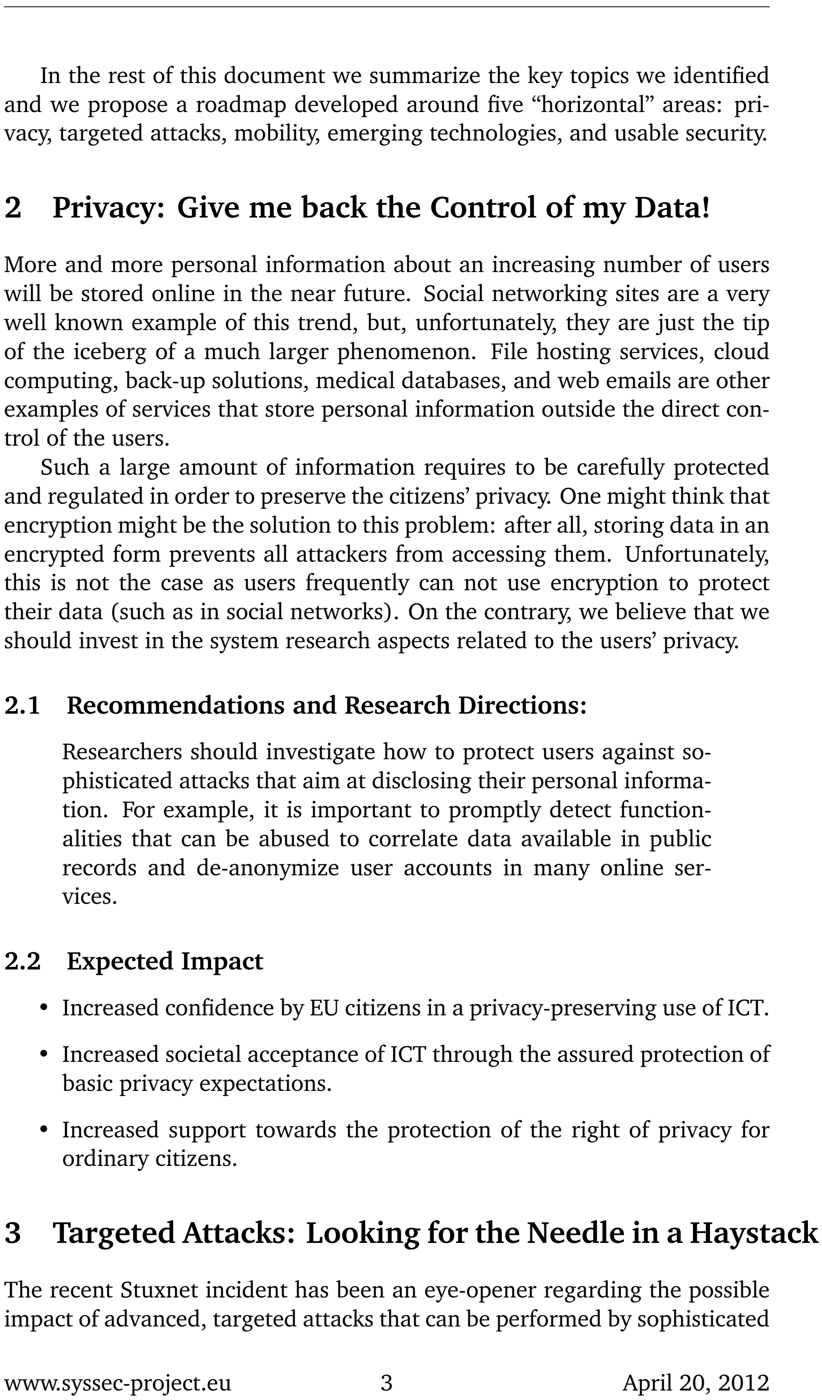
This document is a summary of the Roadmap defined by SysSec [2]. The role of this document, and therefore of the research roadmap, is (i) to analyze the current status of each threat, (ii) to outline the research that needs to be done to mitigate it, and (iii) to list the impact this research is expected to have on the European industry, the European citizen, and the European Society in general.

1.1 Roadmap Definition Process

The collaboration with external experts, both through the project's mailing list and the participation to the face-to-face meetings, helped us to achieve a more general and precise view of which areas of system security need to be better investigated in the near future. One of the outcomes of our brainstorming activity is a list of driving factors that are responsible for changing the IT world, and that can give us a possible direction toward which we need to focus our effort. The result of the brainstorming can be summarized by the following few, important keywords: *mobility*, *increasing lack of privacy*, *24/7 connectivity*, and *cloud computing*. The starting point for the meeting discussion was the *White Book* [1] published at the end of the FORWARD Project. The document contained a number of recommendations for future research based on the likelihood and severity of a number of identified upcoming threats. The main difference between the result of the white book and the content of this document is in the scope of the document.

The White Book was written to be a comprehensive overview of all possible upcoming threats, grouped in eight categories and ranked based on four different aspects: impact, likelihood, obliviousness, and R&D needs. The *SysSec* yearly roadmap aims instead at being a more focused document, in which we review the current state of the threats identified in the past to update the research workplan for the upcoming years.

In addition to the White Book, we refined our roadmap by taking into account the content of similar roadmaps and strategic documents recently published in Europe and in the United States (for a more comprehensive overview of such previous work please refer to the complete project Deliverable [2]).



In the rest of this document we summarize the key topics we identified and we propose a roadmap developed around five “horizontal” areas: privacy, targeted attacks, mobility, emerging technologies, and usable security.

2 Privacy: Give me back the Control of my Data!

More and more personal information about an increasing number of users will be stored online in the near future. Social networking sites are a very well known example of this trend, but, unfortunately, they are just the tip of the iceberg of a much larger phenomenon. File hosting services, cloud computing, back-up solutions, medical databases, and web emails are other examples of services that store personal information outside the direct control of the users.

Such a large amount of information requires to be carefully protected and regulated in order to preserve the citizens’ privacy. One might think that encryption might be the solution to this problem: after all, storing data in an encrypted form prevents all attackers from accessing them. Unfortunately, this is not the case as users frequently can not use encryption to protect their data (such as in social networks). On the contrary, we believe that we should invest in the system research aspects related to the users’ privacy.

2.1 Recommendations and Research Directions:

> Researchers should investigate how to protect users against sophisticated attacks that aim at disclosing their personal information. For example, it is important to promptly detect functionalities that can be abused to correlate data available in public records and de-anonymize user accounts in many online services.

2.2 Expected Impact

- Increased confidence by EU citizens in a privacy-preserving use of ICT.
- Increased societal acceptance of ICT through the assured protection of basic privacy expectations.
- Increased support towards the protection of the right of privacy for ordinary citizens.

3 Targeted Attacks: Looking for the Needle in a Haystack

The recent Stuxnet incident has been an eye-opener regarding the possible impact of advanced, targeted attacks that can be performed by sophisticated actors with significant resources at their disposal [3]. The attack clearly showed how our current defense tools, policies, and infrastructures failed in front of a threat that was designed to focus against a specific target instead of blindly targeting the entire community.

Malicious hardware can also be used as a very subtle vector to perform extremely hard to detect attacks against critical infrastructures, large corporations, and government organizations. However, targeted attacks do not necessarily need to be extremely sophisticated and, even in their simplest forms, can pose a very serious threat against normal users. Targeted SPAM, for example, is extremely effective in phishing users credentials. We envision ad-hoc banking trojans could be developed in the near future to avoid detection by targeting only a restricted group of individuals.

In addition, we believe there is a serious risk that attackers will soon start developing automated techniques to customize attacks based on private user information and aggregated data collected from multiple online sources.

3.1 Recommendations and Research Directions:

> We believe it is very important for researchers to develop new techniques to collect and analyze data associated with targeted attacks. The lack of available datasets, in addition to the limitation of the traditional analysis and protection techniques, is one of the weak points in the everlasting war against malware. In this area, the problem is often to find the needle of the targeted attack in the haystack of the traditional attacks perpetuating every day on the Internet.
>
> In addition, researchers should also focus on new defense approaches that take into account alternative factors (such as monetization), and large scale prevention and mitigation (e.g. at the Internet Service Provider's (ISP) level).

3.2 Expected Impact

- Significant improvement towards the protection of Critical Infrastructures.
- Winning significant ground against sophisticated cyber attackers.
- Design of new detection and protection techniques to mitigate cyber-espionage attacks against governments and large organizations.
- Improved collaboration with international research and operational stakeholders.

4 Security of New and Emerging Technologies: Hey You! Get out of my Cloud!

Analyzing and securing emerging technologies has always been a core objective in the area of system security. Unfortunately, it is often the case that new services and new devices are released before the research community has had a chance of studying their security implications.

In the near future, we can identify four topics, in the area of new and emerging technologies, that need to be studied from a security point of view:

Cloud Computing - The Cloud is quickly changing the way companies run their business. Servers can be quickly launched and shut down via application programming interfaces, offering the user a greater flexibility compared to traditional server rooms.

From a system security perspective, there are a number of aspects that are specific to cloud computing. For instance, the impact of "insider threats", the issues related to privacy and "data management", and the attacks against the "virtualization" infrastructure.

Online Social Networks - As these online communities, such as Facebook, MySpace, Orkut, Twitter, LinkedIn, and others, have been adopted by millions of Internet users, miscreants have started abusing them for a variety of purposes, including stalking, identity theft, spamming, direct advertising, spreading of malware, etc. Monitoring and securing social networks is therefore very important to protect the users from a large spectrum of attacks.

Smart Meters - This new class of devices is a clear example of a new technology that has been rapidly deployed without the required security protection mechanisms. Studying and fixing these devices in particular, but also extending previous work done in more general sensor networks should therefore be one of the goals of system security researchers.

SCADA Networks - Even though SCADA is not exactly a new technology, these devices were initially designed to be isolated and thus built with certain underlying security assumptions. Since many industrial process control systems became reachable from the outside (even when, as shown by Stuxnet, the attacker has to cross an "airgap"), the security of these networks has become an important priority.

4.1 Recommendations and Research Directions:

Securing new and emerging technologies before it is too late is one of the main priorities of the system security area. In this direction, it is important to sponsor activities and collaboration between academia and the industrial vendors to maximize the impact of the research and reduce the time required for the analysis and the experiments.

4.2 Expected Impact

- Increased adoption of, and placing trust in, emerging technologies by ordinary citizens.
- Reduced costs associated with security incidents.
- Lower barriers for mobile operators and application developers to provide accessible and affordable mobile services to their customers.

5 Mobility

We are currently witnessing the penetration of mobile devices in every facet of our society. These devices have varying characteristics but their underlying common features are: ever-increasing computational capabilities and continuous connectivity, be it Ethernet, WiFi, GSM, 3G, 4G LTE, Bluetooth, or even infrared.

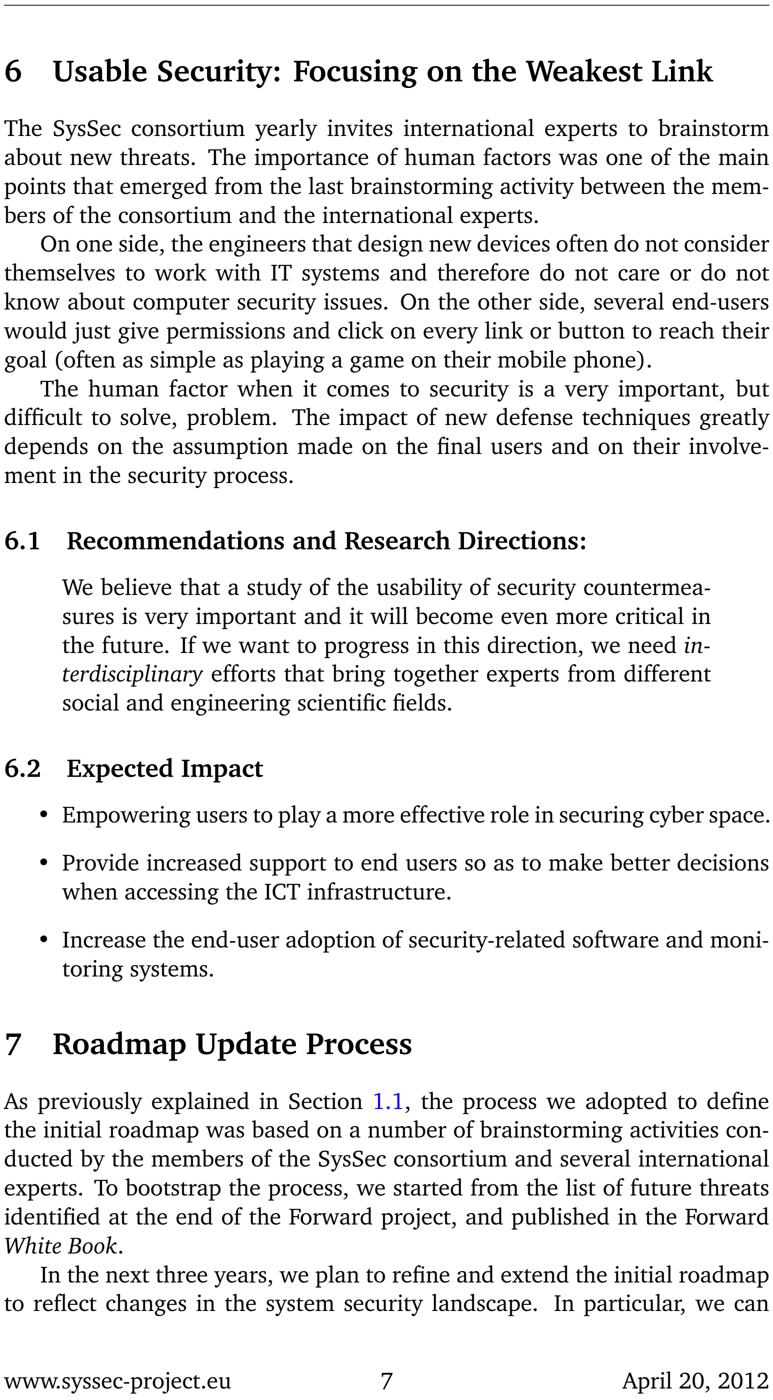
Exploiting such devices is often easy due to a number of factors, not all applicable in all cases: limited computational power to run full-fledged security software like antivirus, firewalls, or intrusion detection systems, dependency on battery power, so even if security software exists it may not be practical to run, lacking security design, ease-of-use trumping security requirements, easy physical access by attackers, etc.

5.1 Recommendations and Research Directions:

We believe it is very important to focus our research toward the security of mobile phones. In particular, we need new tools and techniques that can be deployed to the current smartphone systems to detect and prevent attacks against the device and its applications.

5.2 Expected Impact

- Increased adoption of mobile devices for commercial use by ordinary citizens.
- Improved European industrial competitiveness in mobile phone applications in all realms of life.



6 Usable Security: Focusing on the Weakest Link

The SysSec consortium yearly invites international experts to brainstorm about new threats. The importance of human factors was one of the main points that emerged from the last brainstorming activity between the members of the consortium and the international experts.

On one side, the engineers that design new devices often do not consider themselves to work with IT systems and therefore do not care or do not know about computer security issues. On the other side, several end-users would just give permissions and click on every link or button to reach their goal (often as simple as playing a game on their mobile phone).

The human factor when it comes to security is a very important, but difficult to solve, problem. The impact of new defense techniques greatly depends on the assumption made on the final users and on their involvement in the security process.

6.1 Recommendations and Research Directions:

> We believe that a study of the usability of security countermeasures is very important and it will become even more critical in the future. If we want to progress in this direction, we need *interdisciplinary* efforts that bring together experts from different social and engineering scientific fields.

6.2 Expected Impact

- Empowering users to play a more effective role in securing cyber space.
- Provide increased support to end users so as to make better decisions when accessing the ICT infrastructure.
- Increase the end-user adoption of security-related software and monitoring systems.

7 Roadmap Update Process

As previously explained in Section 1.1, the process we adopted to define the initial roadmap was based on a number of brainstorming activities conducted by the members of the SysSec consortium and several international experts. To bootstrap the process, we started from the list of future threats identified at the end of the Forward project, and published in the Forward *White Book*.

In the next three years, we plan to refine and extend the initial roadmap to reflect changes in the system security landscape. In particular, we can

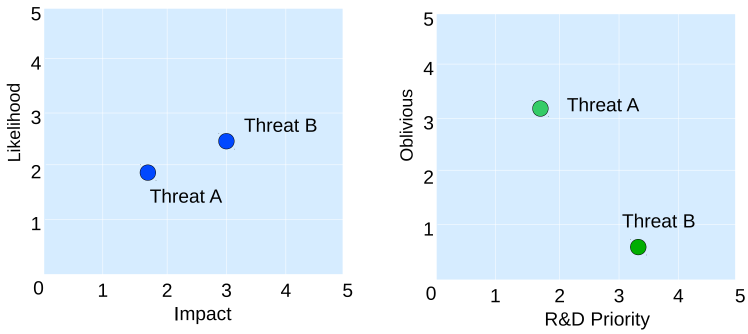
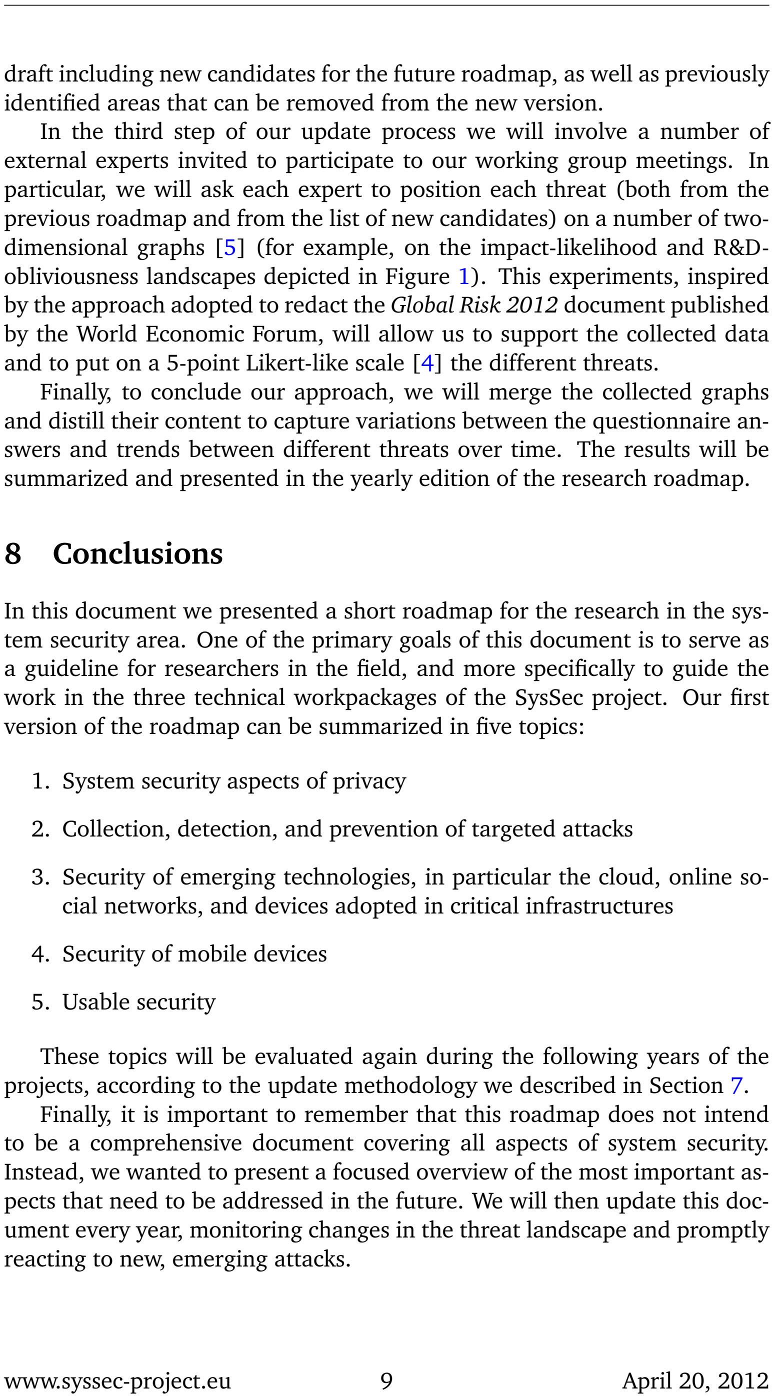


Figure 1: Example of Landscape Graphs used to estimate the potential characteristics of each threats

identify four main reasons that can lead to modification of the roadmap's direction:

- New threats and attacks are discovered that need to be addressed by the research community (e.g., the security of Smart Meter devices)
- Existing threats are mitigated by deployed products, changes in the underlying technology, or new defense mechanisms (e.g., the use of random tokens has been successfully adopted as countermeasure against cross-site request forgery attacks)
- Existing threats, even if unsolved and still potentially harmful, lose interest because of changes in the underground ecosystem or in the criminal motivations (e.g., flash worms were replaced by more lucrative botnets).
- Changes in the existing technology or in the available services suddenly increase the likelihood and severity of some previously unlikely attacks (e.g., spear phishing boosted by the spread of Social Networking sites, or mobile malware by the new widely available smarthphones)

In order to make our approach more systematic, we propose a simple yet effective procedure to update the roadmap. First of all, at the beginning of each year we collect information from several sources: scientific papers published in top venues in system security, statistics about current and future threats reported by antivirus and security companies in their public reports, and opinions of international experts discussed in blogs, talks, whitepapers, or public panels. We then use the collected information to redact an internal



draft including new candidates for the future roadmap, as well as previously identified areas that can be removed from the new version.

In the third step of our update process we will involve a number of external experts invited to participate to our working group meetings. In particular, we will ask each expert to position each threat (both from the previous roadmap and from the list of new candidates) on a number of two-dimensional graphs [5] (for example, on the impact-likelihood and R&D-obliviousness landscapes depicted in Figure 1). This experiments, inspired by the approach adopted to redact the *Global Risk 2012* document published by the World Economic Forum, will allow us to support the collected data and to put on a 5-point Likert-like scale [4] the different threats.

Finally, to conclude our approach, we will merge the collected graphs and distill their content to capture variations between the questionnaire answers and trends between different threats over time. The results will be summarized and presented in the yearly edition of the research roadmap.

8 Conclusions

In this document we presented a short roadmap for the research in the system security area. One of the primary goals of this document is to serve as a guideline for researchers in the field, and more specifically to guide the work in the three technical workpackages of the SysSec project. Our first version of the roadmap can be summarized in five topics:

1. System security aspects of privacy
2. Collection, detection, and prevention of targeted attacks
3. Security of emerging technologies, in particular the cloud, online social networks, and devices adopted in critical infrastructures
4. Security of mobile devices
5. Usable security

These topics will be evaluated again during the following years of the projects, according to the update methodology we described in Section 7.

Finally, it is important to remember that this roadmap does not intend to be a comprehensive document covering all aspects of system security. Instead, we wanted to present a focused overview of the most important aspects that need to be addressed in the future. We will then update this document every year, monitoring changes in the threat landscape and promptly reacting to new, emerging attacks.

References

[1] The Forward Consortium. White book: Emerging ict threats, January 2010. http://www.ict-forward.eu/media/publications/forward-whitebook.pdf.

[2] The SysSec Consortium. Deliverable d4.1: First report on threats on the future internet and research roadmap, September 2011. http://www.syssec-project.eu/media/page-media/3/syssec-d4.1-future-threats-roadmap.pdf.

[3] N. Falliere, L.O. Murchu, and E. Chien. W32. stuxnet dossier. *Symantec Security Response*.

[4] R. Likert. A technique for the measurement of attitudes. *Archives of psychology*, 1932.

[5] Z. Minchev and V. Shalamanov. Scenario generation and assessment framework solution in support of the comprehensive approach. In *Proceedings of SAS-081 Symposium on Analytical Support to Defence Transformation, RTO-MP-SAS-081, Sofia, Boyana, April 26*, 2010.

3
Social network security

Authors SysSec consortium

Dissemination SysSec website exclusive

This whitepaper deals with the risks associated with the use of social networks. It is a high-level abstract of the consortium's research in the area, aimed at general public and decision-maker consumption.

Social network security

A SysSec Whitepaper*

September 4, 2012

1 Introduction

In recent years, social networks have become more than a technology. They directly influence the lives of millions of people around the world. Friendships, social interaction and shared media are just a small subset of the offered functionality. However, the growing popularity also comes with a downside. With over 800 million users [5] in December 2011, Facebook is the largest, most widely accepted social network so far. Recently, it was repeatedly referred to as being the Microsoft Windows of the smartphones. The large amount of information published, and often publicly shared, by users on their online social network profiles is additionally attracting the attention of attackers. If just a single successful attack is launched against a network such as Facebook, the impact is tremendous with over 800 million people being potential victims. To make sure that such an attack does not happen on a large scale, security researchers focus on various properties of these virtual communities and try to find solutions for arising problems.

Naturally, *pure* social networks like Facebook and its predecessors are very good examples and can be used as a reference for most case studies. There are, however, various other platforms to consider. A good example are gaming platforms like Steam [12], Origin [13] or BattleNet [11] where users interact, share their latest achievements or simply chat with each other. Other networks such as LinkedIn or Xing focus on more professional participants to help them establish business relationships and maintain them. In fact, a lot of communities reaching from the aforementioned gaming to research communities, already established their own social network to help likeminded individuals to keep in touch.

What all of these platforms have in common is the fact that they rely on their user's social interactions to function. They only differ in the validity of the presented persona and, from an attacker's point of view, the asset connected with the person behind that persona. That can be a real name and personal

*The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement no 257007.

information on Facebook, credit card information on gaming platforms or in-game currency in an MMOG. Security researchers aim to protect those assets by devising new protection mechanisms or identifying previously unseen threats. This task is not always simple and, due to the unpredictable nature of humans and their actions, often challenging.

2 Traditional attacks

Attacks on social networks are usually variants of traditional security threats (such as malware, worms, spam [15], and phishing [14]). These "common" threats are thoroughly discussed in existing research papers. The one thing these attacks have in common when used in junction with social networks is their possibility to leverage personal data for a higher impact. Spam, for example, can be directly sent to an interested person, probably with the name of a friend as the sender [15]. Worms and other malware have a higher infection rate because links within a social network are more likely to be clicked [10]. Phishing attacks can be aimed at a narrow category of individuals with a higher success rate as traditional spam [4]. These attacks are carried out in a different context by leveraging the social networks as a new medium to reach the victims. Moreover, adversaries can take advantage of the trust relationships between "friends" in social networks to craft more convincing attacks by exploiting personal information gleaned from victims' pages. Therefore, most of the attack requires, as a first step, to become friend of the victim. As already mentioned in the introduction, that applies to almost any form of social networks as long as they support some form of "friendship".

As web applications served to the user via standardized, well-known protocols, social networks can also be attacked in equally well-known ways. OWASP lists the top ten of the web vulnerabilities which of course also apply to social networks. Placed on the very top are injection vulnerabilities. One might think that textbook-like SQL-injection attacks are a thing of the past, but in May 2011, they were the reason for roughly 56.000 user credentials of the dating-social-network findfriendz.com being disclosed. Facebook itself has been shown to be vulnerable to XSS (Cross-Site-Scripting) and CSRF (Cross-Site-Request-Forgery) attacks in the past [2].

While traditional attacks undoubtedly have a severe impact on the customer base provided by today's social networks, new attack vectors, which are specifically tailored to operate on the unique structure of social networks, are emerging.

3 New attack vectors

As the name already suggests, social human interaction is an integral part of social networks. Hence the user itself, rather than the technical infrastructure, is predominantly targeted by social engineering attacks. A typical example is to spike a user's interest on a certain topic that in turn provokes an inconsiderate user action (scamming). A good example for this behavior are various "viral videos" that spread through Facebook over the last year. The new aspect in social engineering attacks in social networks are the trust relationships built upon the aforementioned "friendships". In fact, past research has shown that users of online social networks tend to exhibit a higher degree of trust in friend requests and messages sent by other users (e.g., [7, 9]).

In a *reverse social engineering* attack, this heightened amount of trust is exploited by an attacker that does not initiate contact with the victim. Rather, the victim is tricked into contacting the attacker herself. As a result, a high degree of trust is established between the victim and the attacker as the victim is the entity that first wanted to establish a relationship. Once a reverse social engineering attack is successful (i.e., the attacker has established a friend relationship with the victim), she can then launch a wide range of attacks such as persuading victims to click on malicious links, blackmailing, identity theft, and phishing. Some of the features provided by online social networks can be abused by attackers with the aim of launching automated reverse social engineering attacks. This form of attack can be categorized into three sub-groups, namely, recommendation-based, visitor tracking-based, and demographics-based reverse social engineering.

In the recommendation attack, the aim is to exploit the friend recommendations made by the social network to promote the fake profile of a fictitious user to the victim. The hope, from the attacker's point of view, is that the victim will be intrigued by the recommendation, and will attempt to contact the bogus profile that is under the attacker's control. In the visitor tracking attack, the aim is to trigger the target's curiosity by simply browsing her profile page. The notification that the page has been visited may be enough to attract the target to visit the attacker profile. Finally, in the demographic-based attack scenario, the attacker attempts to reach his victims by forging fake demographic or personal information with the aim of attracting the attention of users with similar preferences (e.g., similar musical tastes, similar interests, etc.).

These attacks highlight just a single facette of social networks. Other than friendship status and the involved level of trust, platform-based applications (Apps) represent another widely-used functionality with the potential to cause mischief. Probably everyone who has a Facebook profile has as least once been confronted with Farmville, Mafia Wars, birthday calendars or other apps through either news items on friends' walls or even direct requests by friends to use them. Although the times when third-party apps had unlimited access to a user's data are over by now, people still tend to willingly accept even boldest permission requests. One explanation for that behavior is that users often propagate their trust relationship to a friend directly to apps used by this friend [16]. Efforts to make users more aware of the privacy they are giving away might be a step into the right direction.

Another form of data exposure is presented by the possibility for third-party websites to interact with the social network by utilizing so-called plugins. Social plugins enable third-party websites to offer personalized content by leveraging the social graph, and allow their visitors to seamlessly share, comment, and interact with their social circles [3]. For example, Facebook's Like button, probably the most widely deployed social plugin [1], enables users to leave positive feedback for the web page in which it has been embedded, share the page with their friends, and view their friends that have "liked" the page, along with the total number of "likes" from all visitors. Google's "+1" button [6] offers almost identical features to the Like button, while similar widgets are also available from other popular social networking sites such as Twitter and LinkedIn.

Social plugins have also been used for a wide variety of other applications including authentication. For example, instead of a web site implementing its own authentication system with user names and passwords, it may use a *social login* plugin offered by a social networking platform such as Facebook. In theory, this approach to authentication not only saves visitors from the burden of remembering one more password, but also gives them the opportunity to experience a personalized service from the web site based on their preferences and social circle.

Unfortunately, both technologies also bear an enormous risk to badly influence a user's privacy. In most cases, a visit to the target site is enough to identify the visitor, regardless of the actual interaction done with the plugin. Social login, on the other hand, enables third-party websites to access private information in a user's profile. A privacy leak not always anticipated by the user.

4 Outlook

In general, the evolution from traditional attacks to more specific forms that leverage social network information was logical. Where technological quirks, weaknesses and vulnerabilities acted as an enabler for traditional attack scenarios, relationships, trust and private information play an equally important role in social networks. Still, large-scale attacks with severe impact to the majority of participants of a social network have not been reported yet. In our opinion, the reason for this is twofold.

First of all, a social network is a strongly supervised and encapsulated structure where permissions are needed to carry out most actions (e.g. sending messages or posting comments). Misbehavior is promptly reported and the corresponding account blocked. Secondly, an attack, once implemented, does not necessarily yield the same results over time. In contrast to a deterministic, technological tool like a botnet or malware in general, the target in social networks are humans. And that bears the advantage of a certain capability to adapt to the circumstances. In the long run, even the most gullible user will be able to tell the difference between a legitimate friend request and a bogus one.

The greatest danger the users and participants of social networks have to face today, are privacy leaks. When the platforms have been introduced at first, they were designed as relatively closed environments which undoubtedly came with their own set of problems. In recent years, however, the progressive integration of social networks into other branches made it increasingly difficult to track where personal information is used or where it can be accessed [8]. Even the tiny like-button discussed before, comes with its privacy issues, not to mention more advanced technologies like social authentication and other plugins.

For targeted attacks like spear phishing or social engineering, a social network is the perfect background. Even though the user is ultimately responsible for the amount of detail offered by her own presentation, researchers are prompted to raise the bar an attacker has to cross before successfully launching an attack. Previous research has proven the feasibility of keeping up or even staying ahead in the arms race. With ongoing effort it can be assured that it also holds true in the future.

References

[1] BuiltWith - Widgets Distribution. http://trends.builtwith.com/widgets.

[2] Facebook CSRF and XSS vulnerabilities. http://www.john-jean.com/blog/advisories/facebook-csrf-and-xss-vulnerabilities-destructive-worms-on-a-social-network-350.

[3] Facebook Plugins. http://developers.facebook.com/docs/plugins/.

[4] Facebook Security Phishing Attack In The Wild. http://www.securelist.com/en/blog/208193325/Facebook_Security_Phishing_Attack_In_The_Wild.

[5] Facebook Stats. http://www.facebook.com/press/info.php?statistics.

[6] Google +1 button. http://www.google.com/+1/button/.

[7] Sophos Facebook ID Probe. http://www.sophos.com/pressoffice/news/articles/2007/08/facebook.html, 2008.

[8] M. Balduzzi, C. Platzer, T. Holz, E. Kirda, D. Balzarotti, and C. Kruegel. Abusing Social Networks for Automated User Profiling. In *Recent Advances in Intrusion Detection*, pages 422–441. Springer, 2010.

[9] L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda. All Your Contacts Are Belong to Us: Automated Identity Theft Attacks on Social Networks. In *18th International Conference on World Wide Web (WWW)*, 2009.

[10] R. Dhamija, J. D. Tygar, and M. Hearst. Why phishing works. In *Proceedings of the SIGCHI conference on Human Factors in computing systems*, CHI '06, pages 581–590, New York, NY, USA, 2006. ACM.

[11] http://eu.battle.net/. Battle.net. 2 2012.

[12] https://steamcommunity.com/. The steam gaming community. 2 2012.

[13] http://www.origin.com/. Origin. 2 2012.

[14] T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer. Social phishing. *Commun. ACM*, 50(10):94–100, 2007.

[15] G. Stringhini, C. Kruegel, and G. Vigna. Detecting spammers on social networks. In *ACSAC*, 2010.

[16] N. Wang, H. Xu, and J. Grossklags. Third-party apps on facebook: privacy and the illusion of control. In *Proceedings of the 5th ACM Symposium on Computer Human Interaction for Management of Information Technology*, page 4. ACM, 2011.

4 Future Research in Systems Security

Authors SysSec Consortium

Dissemination SysSec website, and FIA Research Roadmap

This whitepaper was also published in the FIA Research Roadmap, which basically adopted the SysSec-developed research roadmap on systems security as part of their broader effort.

Future Research in Systems Security

Evangelos Markatos and Davide Balzarotti* , eds

The SysSec Project
contact@syssec-project.eu

Abstract. During its first year of operation, the SysSec network of excellence has created a roadmap for System Security Research. This short paper presents a summary of this Roadmap along with its expected impact on the European industry, the European Citizen, and Society in general.

1 Privacy: Give me back the Control of my Data!

More and more personal information about an increasing number of users will be stored online in the near future. Social networking sites are a very well known example of this trend, but, unfortunately, they are just the tip of the iceberg of a much larger phenomenon. File hosting services, cloud computing, back-up solutions, medical databases, and web emails are other examples of services that store personal information outside the direct control of the users.

Such a large amount of information requires to be carefully protected and regulated in order to preserve the citizens' privacy. One might think that encryption might be the solution to this problem: after all, storing data in an encrypted form prevents all attackers from accessing them. Unfortunately, this is not the case as users frequently can not use encryption to protect their data (such as in social networks). On the contrary, we believe that we should invest in the system research aspects related to the users' privacy.

2 Targeted Attacks: Looking for the Needle in a Haystack

The recent Stuxnet incident has been an eye-opener regarding the possible impact of advanced, targeted attacks that can be performed by sophisticated actors with significant resources at their disposal. The attack clearly showed how our current defense tools, policies, and infrastructures failed in front of a threat that was designed to focus against a specific target instead of blindly targeting the entire community.

Malicious hardware can also be used as a very subtle vector to perform extremely hard to detect attacks against critical infrastructures, large corporations, and government organizations. However, targeted attacks do not necessarily need

* The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement no 257007.

to be extremely sophisticated and, even in their simplest forms, can pose a very serious threat against normal users. Targeted SPAM, for example, is extremely effective in phishing users credentials. We envision ad-hoc banking trojans could be developed in the near future to avoid detection by targeting only a restricted group of individuals.

In addition, we believe there is a serious risk that attackers will soon start developing automated techniques to customize attacks based on private user information and aggregated data collected from multiple online sources.

3 Security of New and Emerging Technologies: Hey You! Get out of my Cloud!

Analyzing and securing emerging technologies has always been a core objective in the area of system security. Unfortunately, it is often the case that new services and new devices are released before the research community has had a chance of studying their security implications.

In the near future, we can identify four topics, in the area of new and emerging technologies, that need to be studied from a security point of view:

Cloud Computing - The Cloud is quickly changing the way companies run their business. Servers can be quickly launched and shut down via application programming interfaces, offering the user a greater flexibility compared to traditional server rooms.

From a system security perspective, there are a number of aspects that are specific to cloud computing. For instance, the impact of “insider threats”, the issues related to privacy and “data management”, and the attacks against the “virtualization” infrastructure.

Online Social Networks - As these online communities, such as Facebook, MySpace, Orkut, Twitter, LinkedIn, and others, have been adopted by millions of Internet users, miscreants have started abusing them for a variety of purposes, including stalking, identity theft, spamming, direct advertising, spreading of malware, etc. Monitoring and securing social networks is therefore very important to protect the users from a large spectrum of attacks.

Smart Meters - This new class of devices is a clear example of a new technology that has been rapidly deployed without the required security protection mechanisms. Studying and fixing these devices in particular, but also extending previous work done in more general sensor networks should therefore be one of the goals of system security researchers.

SCADA Networks - Even though SCADA is not exactly a new technology, these devices were initially designed to be isolated and thus built with certain underlying security assumptions. Since many industrial process control systems became reachable from the outside (even when, as shown by Stuxnet, the attacker has to cross an “airgap”), the security of these networks has become an important priority.

4 Mobility

We are currently witnessing the penetration of mobile devices in every facet of our society. These devices have varying characteristics but their underlying common features are: ever-increasing computational capabilities and continuous connectivity, be it Ethernet, WiFi, GSM, 3G, 4G LTE, Bluetooth, or even infrared.

Exploiting such devices is often easy due to a number of factors, not all applicable in all cases: limited computational power to run full-fledged security software like antivirus, firewalls, or intrusion detection systems, dependency on battery power, so even if security software exists it may not be practical to run, lacking security design, ease-of-use trumping security requirements, easy physical access by attackers, etc.

5 Usable Security: Focusing on the Weakest Link

The SysSec consortium yearly invites international experts to brainstorm about new threats. The importance of human factors was one of the main points that emerged from the last brainstorming activity between the members of the consortium and the international experts.

On one side, the engineers that design new devices often do not consider themselves to work with IT systems and therefore do not care or do not know about computer security issues. On the other side, several end-users would just give permissions and click on every link or button to reach their goal (often as simple as playing a game on their mobile phone).

The human factor when it comes to security is a very important, but difficult to solve, problem. The impact of new defense techniques greatly depends on the assumption made on the final users and on their involvement in the security process.

6 Conclusions

In this document we presented a short roadmap for the research in the system security area. One of the primary goals of this document is to serve as a guideline for researchers in the field, and more specifically to guide the work in the three technical workpackages of the SysSec project. Our first version of the roadmap can be summarized in five topics:

1. System security aspects of privacy
2. Collection, detection, and prevention of targeted attacks
3. Security of emerging technologies, in particular the cloud, online social networks, and devices adopted in critical infrastructures
4. Security of mobile devices
5. Usable security

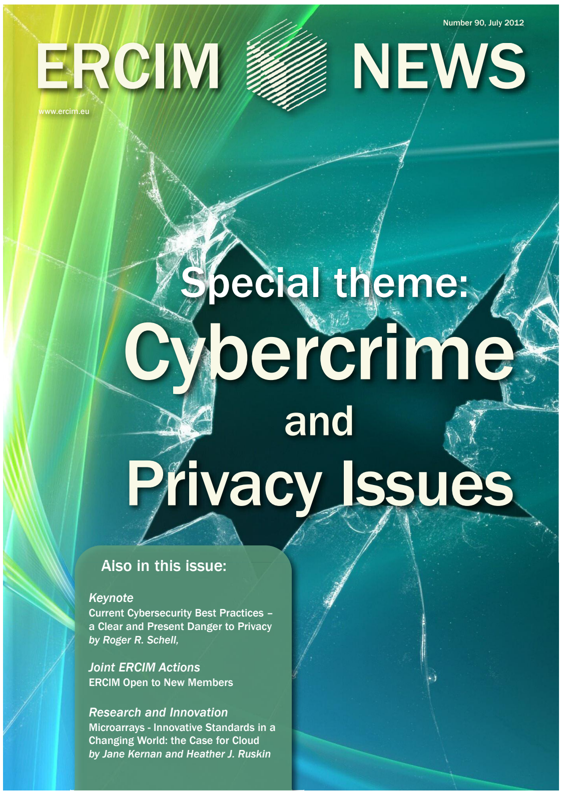
5

SysSec: Managing Threats and Vulnerabilities in the Future Internet

Authors Evangelos Markatos, Herbert Bos

Dissemination SysSec website, and ERCIM news

This whitepaper appeared as an article in ERCIM news, detailing some of the key research directions in SysSec project.


Number 90, July 2012
ERCIM NEWS
www.ercim.eu
Special theme:
Cybercrime
and
Privacy Issues
Also in this issue:
Keynote
Current Cybersecurity Best Practices – a Clear and Present Danger to Privacy
by Roger R. Schell,
Joint ERCIM Actions
ERCIM Open to New Members
Research and Innovation
Microarrays - Innovative Standards in a Changing World: the Case for Cloud
by Jane Kernan and Heather J. Ruskin

SysSec: Managing Threats and Vulnerabilities in the Future Internet

by Evangelos Markatos and Herbert Bos

For many years, cyber attackers have been one step ahead of the defenders. The asymmetric nature of the threat has led to a vicious cycle where attackers end up winning. SysSec, a new Network of Excellence in the area of Systems Security, attempts to break this vicious cycle and encourages researchers to work not on yesterday's attacks but on tomorrow's threats, to anticipate the attackers' next move and to make sure they are prepared.

Over the past decade we have seen a large number of cyber attacks on the Internet. Motivated by financial profits or political purposes, cyber attackers usually launch attacks that stay below the radar, are difficult to detect, and exploit the weakest link: the user. We believe that the core of the problem lies in the nature of cyber security itself: in the current practice of cyber security, most defenses are reactive while attackers are by definition proactive. Cyber security researchers usually chase the attackers trying to find one more defense mechanism for every newly created attack. Thus, we are facing an asymmetrical threat: while attackers have all the time in the world to choose when and where to strike minimizing their cost, defenders must respond fast, within narrow time constraints, and at a very high cost. Each new round of attack-and-defense drains energy from the defenders, leading them down a vicious cycle which will eventually wear them out. It seems that the only way to build effective defenses is to break this cycle, by changing the rules of the game, by anticipating the moves of the attackers, and by being one step ahead of them, through (i) identifying emerging vulnerabilities, and (ii) working towards responding to possible attacks before they appear in the wild. In this aspect, the recently created SysSec Network of Excellence takes a game-changing approach to cyber security: instead of chasing the attackers after an attack has taken place, SysSec studies emerging

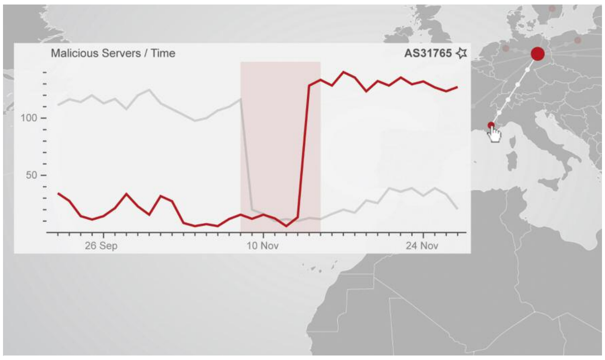


Figure 1: SysSec's BURN interface visualises malicious activities in autonomous systems---in this case, the number of malicious servers as a function of time for a network in Germany exhibits a sudden drop, whereas we find a specular sudden step in a network in France. BURN makes it easy to correlate this type of events visually.

threats and vulnerabilities ahead of time. The network's main thrusts are to identify a roadmap to work on threats and to build infrastructure to boost education in system security—to provide the expertise needed to deal with these emerging threats.

Roadmap

With the collaboration of the research community, SysSec has already produced a research roadmap (http://syssec-project.eu/roadmap1) which outlines some of the important areas the community feels we should focus on. In the first year, the project selected five categories:

1. Privacy. SysSec urges researchers to investigate how to protect users against sophisticated attacks that aim to disclose their personal information. For example, it is important to promptly detect functionalities that can be abused to correlate data available in public records and de-anonymize user accounts in many online services.
2. Targeted attacks. It is important for researchers to develop new techniques to collect and analyze data associated with targeted attacks. The lack of available datasets, in addition to the limitation of the traditional analysis and protection techniques, is one of the current weak points of the war against malware. The problem is often to find the needle of the targeted attack in the haystack of the traditional attacks perpetuated every day on the Internet. In addition, researchers should focus on new defense approaches that take into account alternative factors (such as monetization), and large scale prevention and mitigation (e.g., at the Internet Service Providers (ISP) level).
3. Security of emerging technologies, in particular the cloud, online social networks, and devices adopted in critical infrastructures (like smart meters). Security in new and emerging technologies before it is too late is one of the main priorities of the system security area. In this direction, it is important to sponsor activities and collaboration between academia and the industrial vendors to maximize the impact of the research and reduce the time required for the analysis and the experiments.
4. Mobility: develop new tools and techniques that can be deployed in current smartphone systems to detect and prevent attacks against the device and its applications.
5. Usable security: We believe that a study of the usability of security measures is important and it will become even more critical in the future. If we want to progress in this direction, we need interdisciplinary efforts that bring together experts from different fields (including engineering, system security, psychology, etc.).

With the help of experts organized in working groups, SysSec updates its roadmap yearly to reflect new threats and priorities.

Education

Having realized the lack of educational material in the area, SysSec further aims to establish a center for academic excellence in the area and has started designing a common curriculum on cyber security, focusing mostly on the production of slides and lab exercises, which are particularly hard to design and set up. A first version of the curriculum along with course material is expected to be ready by September 2012. It will be open to universities throughout Europe and will help to set up a state of the art cyber security curriculum to train the next generation of experts.

We underline that besides SysSec several other projects aim to map the research landscape in cyber security. However, with a clear focus on system security and the development of usable course material, we believe SysSec occupies a unique and valuable niche. SysSec may be contacted at contact@syssec-project.eu, may be followed in twitter (twitter: syssecproject) and may be found in Facebook (http://www.facebook.com/SysSec).

References:

Privacy-Preserving Social Plugins

[1] G. Kontaxis, M. Polychronakis, A. D. Keromytis and E; P. Markatos. “Privacy-Preserving Social Plugins”, In the Proceedings of the 21st USENIX Security Symposium, 2012.

[2] F. Maggi, A.Volpatto, S. Gasparini, G. Boracchi, S. Zanero. “POSTER: Fast, Automatic iPhone Shoulder Surfing”. In the Proceedings of the 18th ACM/SIGSAC Conference on Computer and Communications Security (CCS), 2012.

[3] C. Rossow, C. J. Dietrich, C. Kreibich, C. Grier, V. Paxson, N. Pohlmann, H. Bos and M. van Steen. “Prudent Practices for Designing Malware Experiments: Status Quo and Outlook”. In the Proceedings of the 33rd IEEE Symposium on Security & Privacy (Oakland), 2012.

Please contact:

Herbert Bos, VU University
Amsterdam, The Netherlands
Tel: +31-20 598 7746
E-mail: HerbertB@cs.vu.nl

Evangelos Markatos
FORTH-ICS, Greece
Tel: +30 2810391655
E-mail: contact@syssec-project.eu

6 Cybersecurity in the Smart Grid

Authors Magnus Almgren, Davide Balzarotti, Marina Papatriantafilou and Valentin Tudor

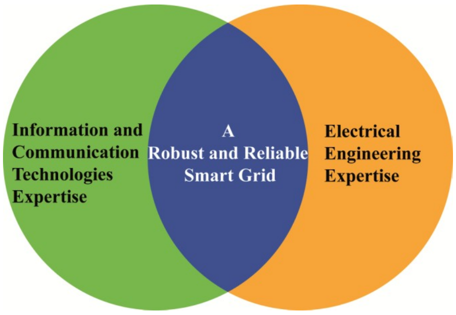
Dissemination SysSec website, and ERCIM news

This whitepaper appeared as an article in ERCIM news, with a high-level report on security issues in the context of smart grids. It ias important because it shows also the effects of the cooperation between SysSec and the EU-funded project CRISALIS.

Cybersecurity in the Smart Grid

by Magnus Almgren, Davide Balzarotti, Marina Papatriantafilou and Valentin Tudor[1]

In the past, the easiest way to attack the electrical grid would have been to physically access and destroy components. However, with the introduction of the smart grid and its increased dependence on information and communication technologies (ICT), the future grid may be vulnerable to pernicious cyber attacks performed remotely. In CRISALIS and SysSec, we are studying the properties of the envisioned smart grid to be able to anticipate and mitigate future attacks against this critical infrastructure.


Information and Communication Technologies Expertise
A Robust and Reliable Smart Grid
Electrical Engineering Expertise

In Europe and elsewhere, the electrical grid is being transitioned into the "smart grid" in order to increase flexibility and accommodate large scale energy production from renewable sources. This transition involves, among other steps, the installation of new, advanced equipment – for example, the replacement of traditional domestic electrical meters with smart meters - and remote communication with devices – for example, allowing remote access to an unsupervised energy production site. Together with the new functionalities, this transition introduces concerns about how the technology can be misused by adversaries [1].

The security issues associated with the smart grid include the following. Many of the new security issues in the smart grid are well-known problems in the information and communication technology (ICT) domain, such as buffer overflows in devices and sloppy implementations of cryptographic protocols. However, the solutions from the more mature ICT domain may not be directly applicable to the smart grid due to resource-constrained devices (smart meters), the life cycle of components (there will always be legacy systems) or the impossibility of immediately shutting down and patching a machine that needs to run 24/7. Other issues originate from the electrical and power engineering domain (device tampering). There are also challenging new problems originating from the intersection between the electrical engineering and ICT domains, for example where a cyber attack (buffer overflow) in turn affects properties of the electrical grid (power quality), which in turn may propagate back to the ICT domain (vulnerability of control loop) [2]. An interdisciplinary approach is required to identify possible solutions to these problems.

In SysSec, a network of excellence in Europe, and CRISALIS, a European research project, we are working on improving the security in critical systems, in particular the smart grid, through two orthogonal approaches. One major problem is the lack of cross-domain expertise in both ICT security

[1] Published in ERCIM News #92, http://ercim-news.ercim.eu/images/stories/EN92/EN92-web.pdf

and power engineering. Being a network of excellence, SysSec organizes several activities to bring together researchers and practitioners from different domains. For example, we organized a summer school for students across Europe for a hands-on approach to learn more about reverse engineering of malware targeting critical infrastructure. To our surprise, we hit the ceiling on the number of students we could accept within less than a week of the announcement, forcing us to create a waiting list. This points to the need of better education in this area and we will also include modules for hardware security and critical infrastructure protection as part of the effort in SysSec to provide a common curriculum on cyber security.

Another major problem hampering the analysis of security properties of the smart grid is the proprietary nature of the technologies and protocols involved: there are few open source tools available to perform an in-depth analysis of a system. For this reason, we are developing a toolset in CRISALIS that can be used by researchers to validate security claims made by vendors and increase the overall security of the deployed components. One of the first deliverables will be an open-source fuzzer to test the protocols used in this domain. By working closely with industrial partners, the goal is to provide new tools to detect intrusions and effective techniques to analyse infected systems.

Even though the smart grid is a necessity, it is important to understand the security risks before complete systems are deployed and interconnected across Europe. Learning from and avoiding simple problems that have already been encountered in the ICT domain, we may focus on the new types of threats that arise as a consequence of the interdisciplinary nature of this complex environment. For this reason, projects such as SysSec and CRISALIS, which bring together experts from different domains, are crucial at this stage.

CRISALIS (http://www.crisalis-project.eu/) may be contacted at contact@crisalis-project.eu. SysSec (http://www.syssec-project.eu/) may be contacted at the corresponding contact@syssec-project.eu, followed in twitter (twitter:syssecproject) and Facebook (http://www.facebook.com/SysSec).

References:

[1] National Institute of Standards and Technology Interagency, "Guidelines for Smart Grid Cyber Security (NISTIR 7628)," vol. 1-3, http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628, 2010.

[2] Costache, Tudor, Almgren, Papatriantafilou, Saunders, "Remote control of smart meters: friend or foe?," EC2ND-2011, Gothenburg, Sweden.

Please contact:
Magnus Almgren
Chalmers University of Technology, Sweden
+46 31 772 1702
magnus.almgren@chalmers.se

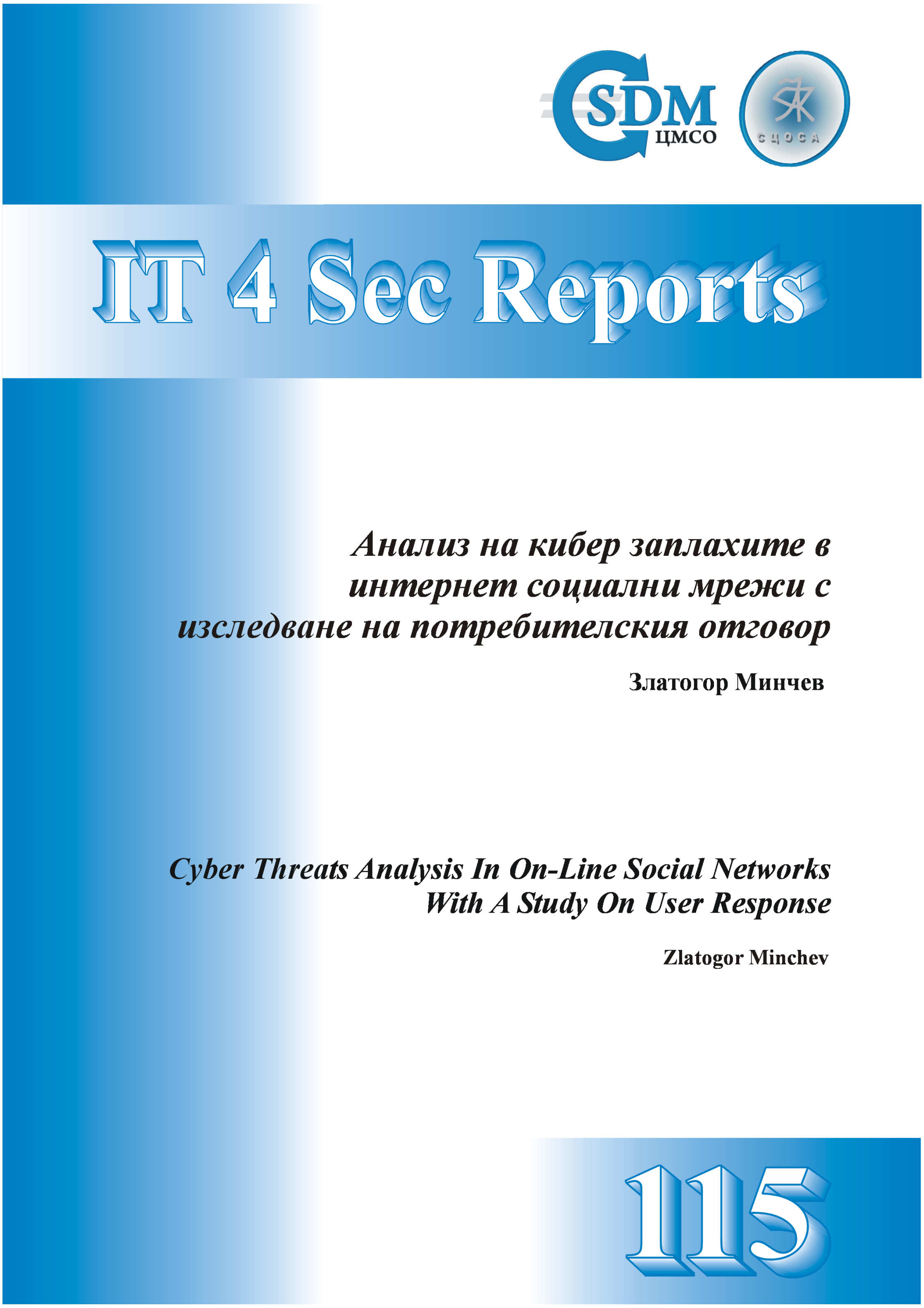
7

Cyber Threats Analysis In On-Line Social Networks With A Study On User Response

Authors IICT-BAS on behalf of the SysSec consortium

Dissemination SysSec website, and through IICT-BAS's channels in Bulgaria

This whitepaper, aimed at a national audience (in Bulgaria) is aimed to extend and deepens the impact of the project, by translating some of the consortium's resarch results in a more consumable form for decision makers and the general public who may not find them accessible in English. We decided to include this whitepaper as an example of an exercise all partners have done in disseminating high-level information about our research to our national audiences.



IT 4 Sec Reports

Анализ на кибер заплахите в интернет социални мрежи с изследване на потребителския отговор

Златогор Минчев

Cyber Threats Analysis In On-Line Social Networks With A Study On User Response

Zlatogor Minchev

115

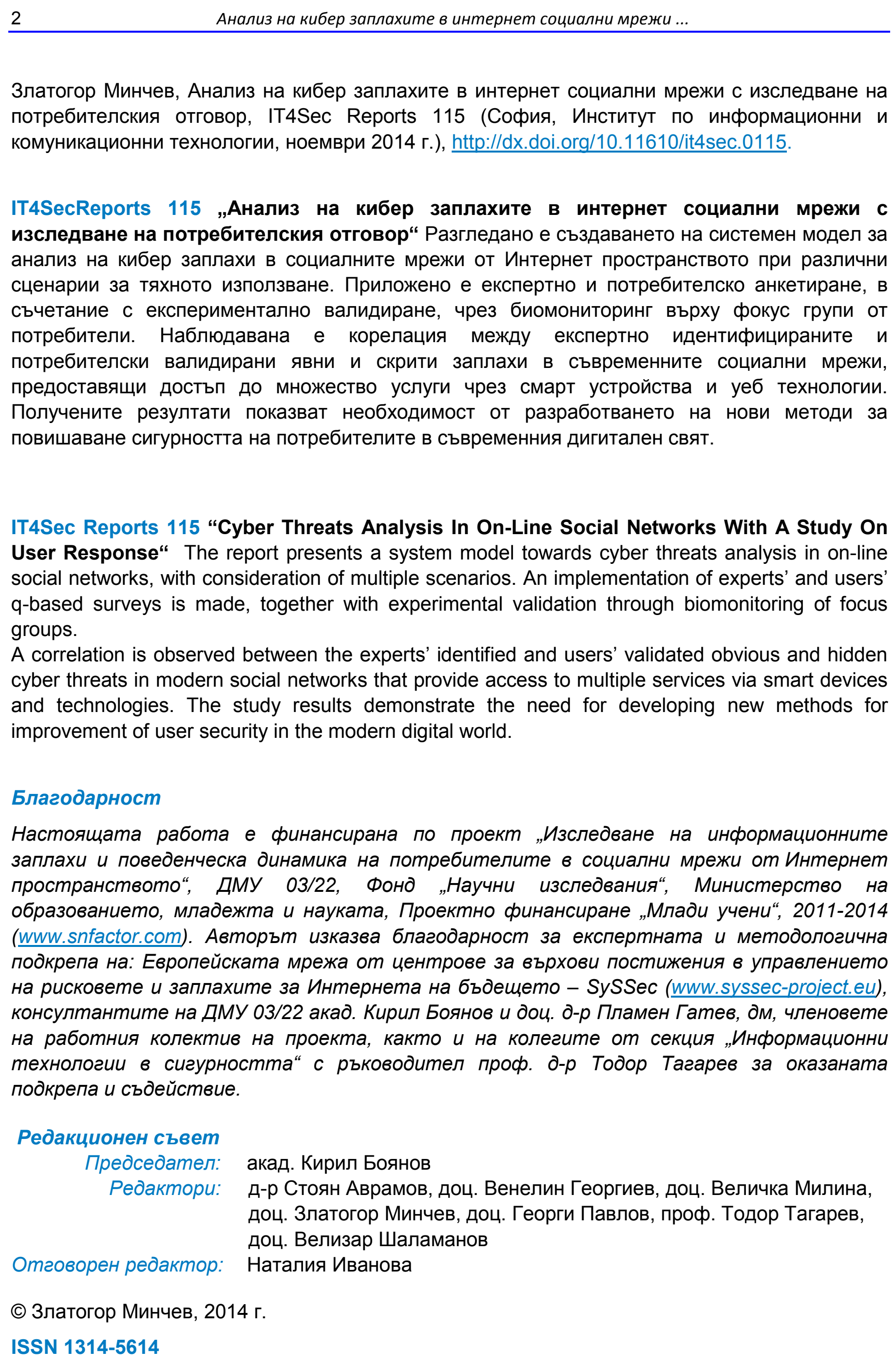
IT4Sec Reports 115
http://dx.doi.org/10.11610/it4sec.0115

Анализ на кибер заплахите в интернет социални мрежи с изследване на потребителския отговор

Златогор Минчев

Институт по информационни и комуникационни технологии – БАН
секция “Информационни технологии в сигурността”
www.IT4Sec.org

София, ноември 2014 г.



Златогор Минчев, Анализ на кибер заплахите в интернет социални мрежи с изследване на потребителския отговор, IT4Sec Reports 115 (София, Институт по информационни и комуникационни технологии, ноември 2014 г.), http://dx.doi.org/10.11610/it4sec.0115.

IT4SecReports 115 „Анализ на кибер заплахите в интернет социални мрежи с изследване на потребителския отговор“ Разгледано е създаването на системен модел за анализ на кибер заплахи в социалните мрежи от Интернет пространството при различни сценарии за тяхното използване. Приложено е експертно и потребителско анкетиране, в съчетание с експериментално валидиране, чрез биомониторинг върху фокус групи от потребители. Наблюдавана е корелация между експертно идентифицираните и потребителски валидирани явни и скрити заплахи в съвременните социални мрежи, предоставящи достъп до множество услуги чрез смарт устройства и уеб технологии. Получените резултати показват необходимост от разработването на нови методи за повишаване сигурността на потребителите в съвременния дигитален свят.

IT4Sec Reports 115 “Cyber Threats Analysis In On-Line Social Networks With A Study On User Response“ The report presents a system model towards cyber threats analysis in on-line social networks, with consideration of multiple scenarios. An implementation of experts' and users' q-based surveys is made, together with experimental validation through biomonitoring of focus groups.

A correlation is observed between the experts' identified and users' validated obvious and hidden cyber threats in modern social networks that provide access to multiple services via smart devices and technologies. The study results demonstrate the need for developing new methods for improvement of user security in the modern digital world.

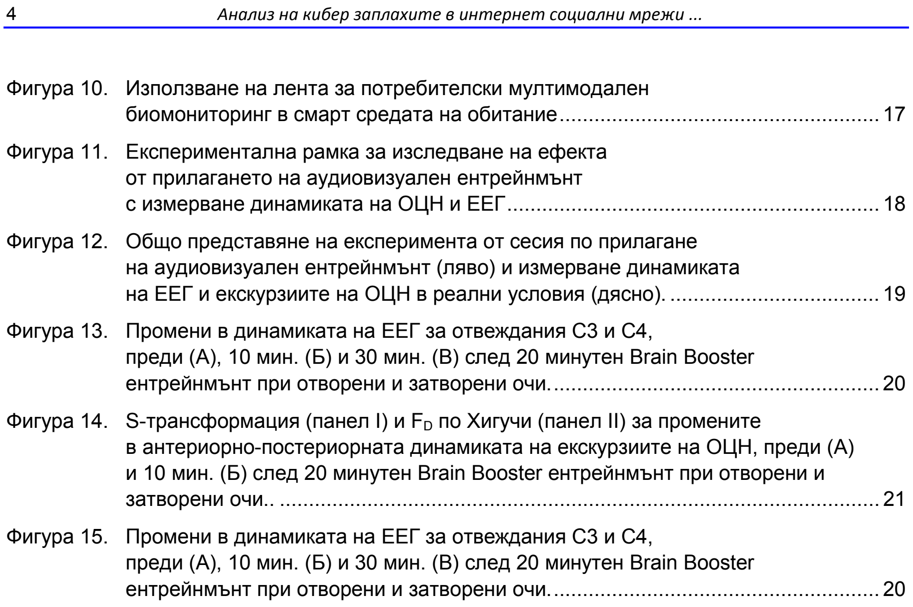
Благодарност

Настоящата работа е финансирана по проект „Изследване на информационните заплахи и поведенческа динамика на потребителите в социални мрежи от Интернет пространството“, ДМУ 03/22, Фонд „Научни изследвания“, Министерство на образованието, младежта и науката, Проектно финансиране „Млади учени“, 2011-2014 (www.snfactor.com). Авторът изказва благодарност за експертната и методологична подкрепа на: Европейската мрежа от центрове за върхови постижения в управлението на рисковете и заплахите за Интернета на бъдещето – SySSec (www.syssec-project.eu), консултантите на ДМУ 03/22 акад. Кирил Боянов и доц. д-р Пламен Гатев, дм, членовете на работния колектив на проекта, както и на колегите от секция „Информационни технологии в сигурността“ с ръководител проф. д-р Тодор Тагарев за оказаната подкрепа и съдействие.

ISSN 1314-5614

СЪДЪРЖАНИЕ

Списък на фигурите



4 *Анализ на кибер заплахите в интернет социални мрежи ...*

1. МОДЕЛНО ИЗСЛЕДВАНЕ НА ПОТРЕБИТЕЛСКИТЕ АКТИВНОСТИ В СОЦИАЛНИТЕ МРЕЖИ

Реализирането на настоящото изследване е съчетание от експертни мнения с моделно представяне в подходяща среда за анализ. Използвани бяха три анкетни проучвания, на основата, на които бе създаден системен модел в средата I-SCIP-SA (Minchev & Petkova, 2010), детайлизирани по-долу.

Най-общо, потребителските активности (дейности) в социалните мрежи могат да се групирани около сценарии за: регулярно сърфиране, забавления и социален инженеринг (Минчев, 2012).

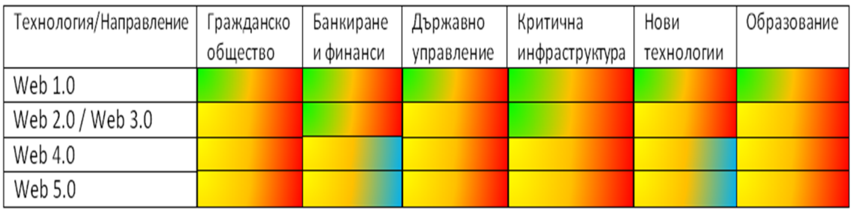
В тази връзка ще отбележим и устойчиви тенденции в прогнозите за важността в дигиталното общество на социалните мрежи, социалния инженеринг и личното пространство за потребителите, които се потвърждават в редица публикации по темата (Balzarotti, Markatos, Minchev, et al, 2013, Minchev & Boyanov, 2014, Balzarotti, 2014).

Предвид факта, че за съвкупното изследване на трите дейности е необходим обединяващ системен модел, за негов управляващ фактор бе избрано „мултимедийното съдържание“ (Боянов, Минчев, Боянов, 2013). То е богат източник на информация в съвременните социални мрежи, използващи Web 3.0 технологии и ще запази тази тенденция с въвеждането на 4G решения в мобилните смарт устройства (Боянов, 2014). От друга страна неговото влияние се оценява от някои автори и като „дигитална дрога“ влияеща на подрастващите (Singel, 2010), което го прави значим, потенциален източник на кибер заплахи за потребителите.

Допълнително, през 2013 г. и 2014 г., Съвместният център за обучение симулации и анализ, организира две анкетни проучвания свързани с темата.

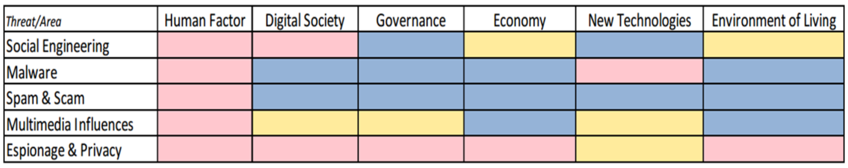
Първото изследване (изготвено в подкрепа на проекта за Национална стратегия по кибернетична сигурност на Р България, 2013), се отнасяше до тенденциите във влиянието на уеб технологиите върху различни социални направления на дигиталното общество и обхващаше 150 национални и международни експерти. Второто изследване от 2014 г. бе за мултикритериална оценка на кибер заплахите в социалните мрежи и обхващаше 75 експерти. Обобщения от изследванията, публикувани накратко в (Минчев, 2013, Minchev, 2013, Minchev & Kelevedjiev, 2014) са показани на Фиг. 1.

Резултатите, показани на Фиг. 1 (а), използват цветова скала от зелено към червено, през жълто, показваща засилване на дадено направление в посока към червения цвят и съответно – отслабване, в посока към зеления цвят. Използването на син цвят, отразява наличието на неопределеност. Времевият хоризонт на изследването е пет години - до 2018 г.



Технология/Направление	Гражданско общество	Банкиране и финанси	Държавно управление	Критична инфраструктура	Нови технологии	Образование
Web 1.0	🟩🟥	🟩🟥	🟩🟥	🟩🟥	🟩🟥	🟩🟥
Web 2.0 / Web 3.0	🟨🟥	🟩🟥	🟨🟥	🟩🟥	🟨🟥	🟨🟥
Web 4.0	🟨🟥	🟨🟦	🟨🟥	🟨🟥	🟨🟦	🟨🟥
Web 5.0	🟨🟥	🟨🟦	🟨🟥	🟨🟥	🟨🟦	🟨🟥

(а)



Threat/Area	Human Factor	Digital Society	Governance	Economy	New Technologies	Environment of Living
Social Engineering	🟥	🟥	🟦	🟨	🟦	🟨
Malware	🟥	🟦	🟦	🟦	🟥	🟦
Spam & Scam	🟥	🟦	🟦	🟦	🟦	🟦
Multimedia Influences	🟥	🟨	🟨	🟦	🟨	🟦
Espionage & Privacy	🟥	🟥	🟥	🟥	🟨	🟥

(б)

Фиг.1. Обобщения на мултикритериални анкетни проучвания на тенденциите във влиянието на уеб технологиите върху различни социални направления от развитието на дигиталното общество за 2013 г. (а) и кибер заплахите в социалните мрежи за 2014 г. (б).

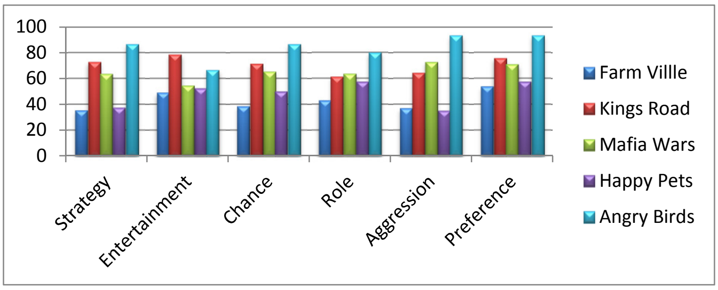
За Web 2.0/Web 3.0 технологиите, използвани в съвременните социални мрежи, прогнозите са критични по отношение и на шестте изследвани направления („Гражданско общество", „Банкиране и финанси", "Държавно управление", „Критична инфраструктура", „Нови технологии", „Образование"). Очакваните бъдещи заплахи от Web 4.0/Web 5.0, фокусират в неопределеност: „Банкиране и финанси" и „Нови технологии". Тези прогнози отчитат факта, че се очаква новите уеб технологии да навлязат в дигиталното общество на 21 век, след не по-малко от десет години (A Digital Agenda for Europe, 2010).

Тук е важно да акцентираме върху „Критичната инфраструктура", като елемент от комуникационната и информационната инфраструктура, която запазва своята оценка за целия прогнозен период. В тази връзка ще споменем и моделното изследване на проблема в средата I-SCIP-SA (Minchev & Petkova, 2010), по отношение на използването на новите ИКТ за подобряване на съвременната среда за гранична кибер сигурност, което потвърждава направената класификация за „Критичната инфраструктура" от системна гледна точка и нейното значение като източник на скрити кибер заплахи (Minchev, 2013).

Оценяването на кибер заплахите в социалните мрежи (вж. Фиг. 1 (б)) бе извършено в шест направления ("Human Factor" – „Човешки фактор", "Digital Society" – „Дигитално общество", "Governance" – „Държавно управление", "Economy" – „Икономика", "New Technologies" – „Нови технологии" и "Environment of Living" – „Среда на обитание"), като са идентифицирани пет области като източник на заплахи ("Social Engineering" – „Социален инженеринг", "Malware" – „Зловреден софтуер", "Spam & Scam" – „Спам/Скам", "Multimedia Influence" – „Влияние на мултимедията", "Espionage & Privacy" – „Шпионаж и лично пространство"). Използвана е тристепенна цветна скала (*жълто* – „високо", *червено* – „много високо", *синьо* – „неопределено").

Като обобщение от двете изследвания за „Влияние на мултимедията“, „Социалния инженеринг“ и „Шпионаж и лично пространство“, можем да отчетем, че се запазва тенденция за „висока“ и „много висока“ значимост за всичките шест направления на оценка за следващите пет години до 2018 г. за всички изследвани области на развитие в дигиталното общество. За някои от направленията, оценяваните кибер заплахите са класифицирани като неопределени от участващите експерти.

Друго изследване, включващо фокус-група от общо 37 анкетирани лица (28 момчета и 9 момичета на средна възраст 15,6 години, ученици - геймъри от гимназиалната форма на обучение), допълва изложеното по отношение на значението на мултимедията. То се фокусира върху мултикритериална оценка на избрани популярни игри, като елемент на мултимедията, в социалната мрежа Facebook (Фиг. 2). Тя бе избрана, предвид изключителната си популярност (Top 15 Most Popular Social Networking Sites, 2014), в т.ч. и сред 250 българските потребители (Minchev & Feimova, 2014).



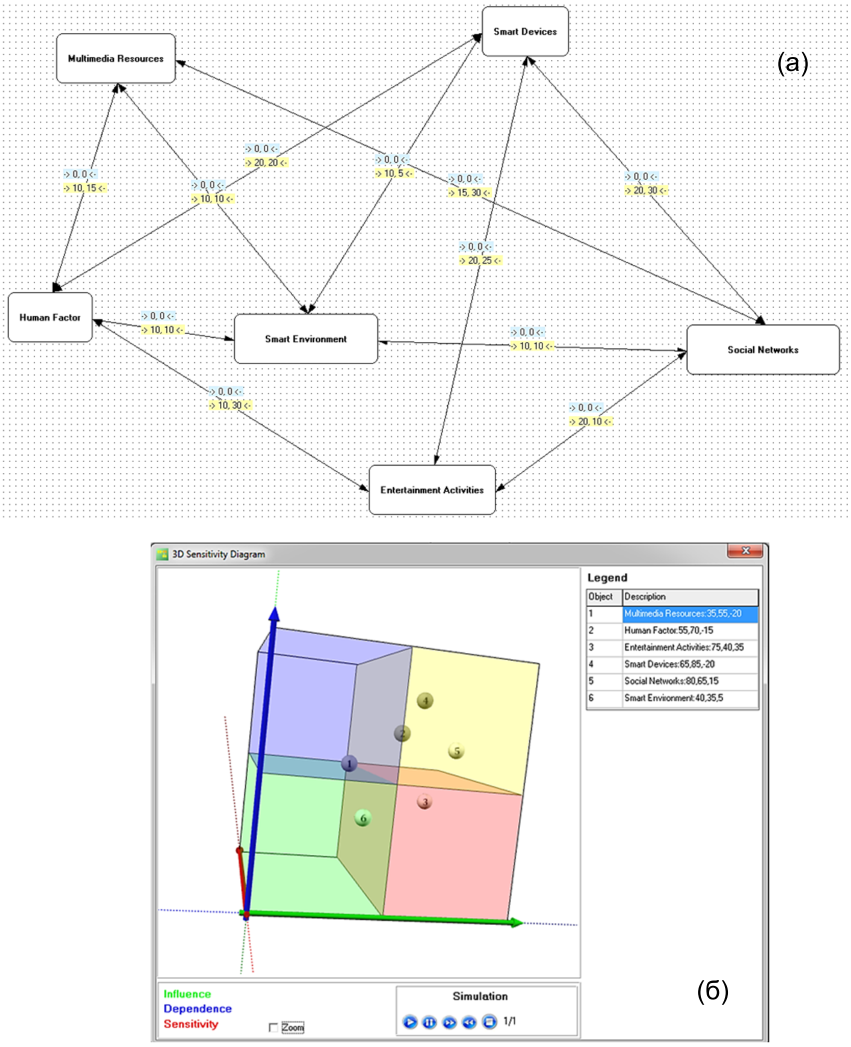
Фиг.2. Обобщени резултати, в проценти, от анкетно проучване за типа и предпочитанията на потребителска фокус-група и избрани популярни игри в социалната мрежа Facebook.

От представените резултати става видна засилената популярност на игрите за забавление свързани с насилие. Безспорно, отличени са Angry Birds, Mafia Wars и Kings Road. Избраните оценъчни направления са свързани с типовете на играта („Стратегия“ – “Strategy”, „Забавление – “Entertainment”, „Късмет“ – “Chance”, „Ролева“ – “Role”) и оценките за „Предпочитания“ (“Preference”) и „Агресивност“ (“Aggression”). Тази тревожна тенденция по отношение на агресията, като предпочитан тип игри при подрастващите, се потвърждава и от други изследвания в областта (Bavelier et al, 2011).

Предвид изложеното дотук, с използване на данните от тези изследвания бе създаден системен модел (Фиг. 3) в средата I-SCIP-SA (Minchev & Petkova, 2010) за оценка на въздействието на мултимедийното съдържание в социалните мрежи (Minchev & Feimova, 2014, Minchev et al, 2014).

Всички обекти в системата са свързани претеглено (обектите са означени със заоблени, именувани правоъгълници, връзките с едно- и дву- посочни стрелки, а техните атрибути – с етикет в жълто, за теглото на връзката и в синьо за времетраенето на разглеждането на връзката, за настоящия случай; в предложения модел, то е „0“, защото е разгледан статично, за оценка, като този въпрос ще бъде дискутиран по-долу). Избрани бяха шест агрегирани обекта: „Мултимедийни ресурси“ – “Multimedia Resources”, „Смарт устройства“ – “Smart Devices”, „Социални мрежи“ - “Social Networks”, „Човешки фактор“ –

“Human Factor”, „Смарт среда“ – “Smart Environment”, потребителски „Активности свързани със забавления“ – “Entertainment Activities”.



Legend

Object	Description
1	Multimedia Resources:35,55,-20
2	Human Factor:55,70,-15
3	Entertainment Activities:75,40,35
4	Smart Devices:65,85,-20
5	Social Networks:80,65,15
6	Smart Environment:40,35,5

Фиг.3. Системен модел (а) за оценка на въздействието на мултимедийното съдържание в социалните мрежи и диаграма на чувствителността (б) в средата I-SICIP-SA (Minchev & Feimova, 2014, Minchev et al, 2014).

Разпределението на обектите в модела е представено графично, в 3D Декартова координатна система, наречена диаграма на чувствителността (отчасти основана на тази, публикувана в (Vester, 2002, вж. Фиг. 3б), на базата на нормализираните стойности за интервала [0,1], изразени в проценти на правата („Влияние” (Influence) – *x*) и обратната връзка („Зависимост” (Dependence) – *y*) между обектите.

Абсолютната разлика между тези две стойности се дефинира като „Чувствителност” и е представена, като z-координата оцветена в червено. Тя също подразделя обектите на активни (оцветени в светло сиво, >50% от интервала [0,1]) и пасивни (< 50 % от интервала [0,1], оцветени в тъмно сиво), по зададен граничен праг за всеки от секторите на диаграмата.

Според оцветяването на секторите в Диаграмата на чувствителност и съотношението „влияние/зависимост” са определени следните класове обекти: зелен – буферни; жълт – критични; син – пасивни; червен – активни. Като под „активни” и „пасивни” обекти се има предвид тяхното класифициране от гл. т. на управлението, т.е. активните са директно управляеми, докато при пасивните - управлението е косвено.

Както става видно от Фиг. 3б, като активни и пряко управляеми са класифицирани обектите „Активности, свързани със забавления“ (Entertainment Activities, z=35) – 3; пасивни и косвено управляеми, т.е. криещи скрити опасности са: „Мултимедийни ресурси” (Multimedia Resources, z=-20) – 1.

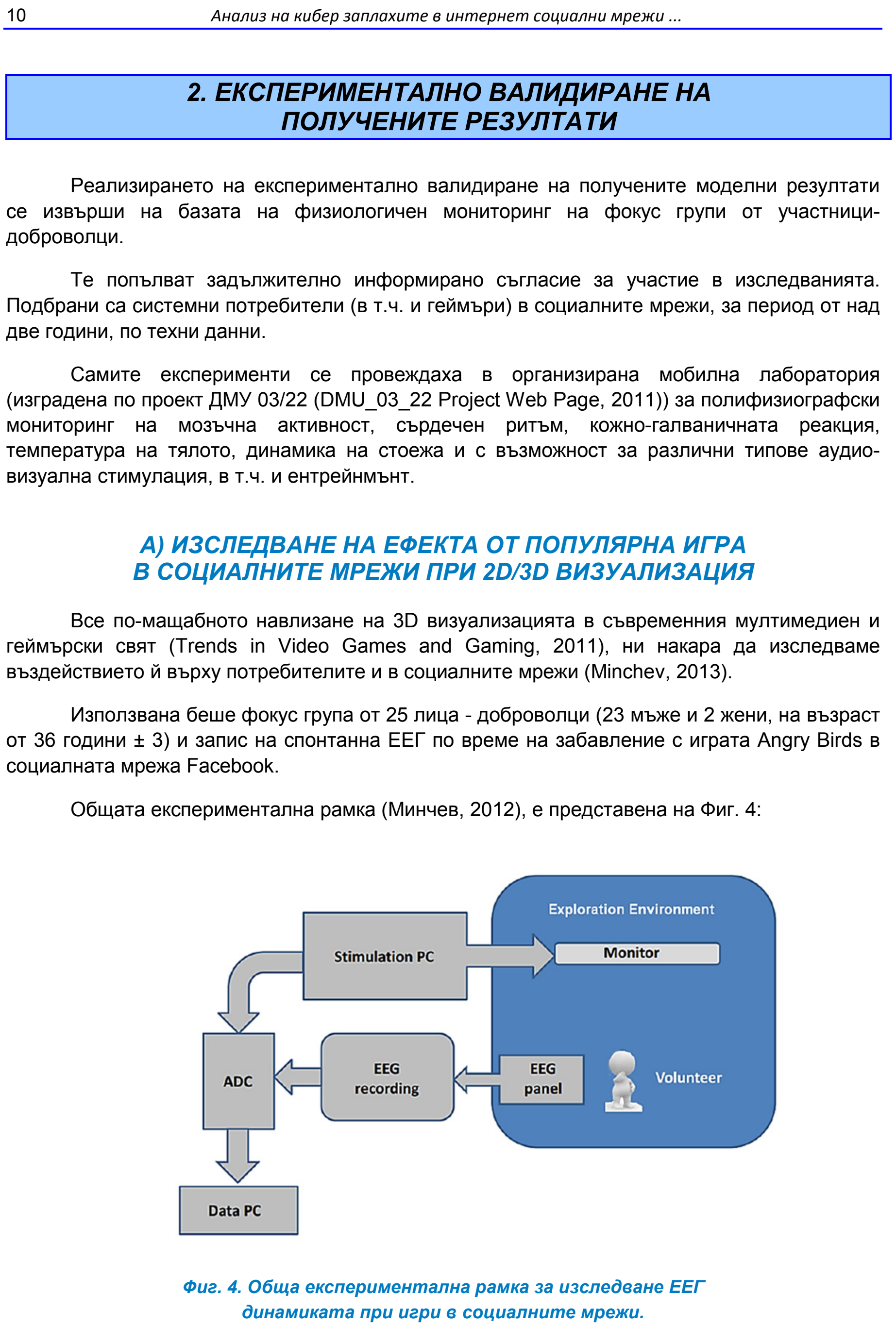
Обектите „Човешки фактор“ (Human Factor, z=-15) – 2 и „Смарт устройства“ (Smart Devices, z=-20) – 4 са критични и косвено управляеми, а „Социални мрежи“ (Social Networks, z=15) – 15 – критични и пряко управляеми.

Обектът „Смарт среда“ (Smart Environment, z=5) – 6 в модела е определен като буферен.

Предвид експертния характер на полученото разпределение на обектите в модела за оценка на въздействието на мултимедийното съдържание в социалните мрежи, ще отбележим, че средата I-SCIP-SA позволява и задаване на стойностите за „Влияние” и „Зависимост” и като масив от данни и неговото динамично симулиране. Преходите между отделните стойности, елементи на масива могат да бъдат апроксимирани с различни функции (например: линейна, експоненциална, s-образна и т.н.) и представени дискретно (Naim & Towill, 1994).

Тъй като подобно симулиране дава доста субективна оценка за значимостта на идентифицираните кибер заплахи в социалните мрежи, използвахме само неговата базова класификация за значимостта на мултимедията, като източник на скрити кибер заплахи. Потребителско валидиране, по отношение на реално влияние на мултимедията върху човешкия фактор, бе извършено чрез серия физиологични експерименти за мониторинг на централната и периферната нервна система, вкл. и с допълнителна стимулация.

В следващия параграф тази част от изследването ще бъде по-детайлно представена.



2. ЕКСПЕРИМЕНТАЛНО ВАЛИДИРАНЕ НА ПОЛУЧЕНИТЕ РЕЗУЛТАТИ

Реализирането на експериментално валидиране на получените моделни резултати се извърши на базата на физиологичен мониторинг на фокус групи от участници-доброволци.

Те попълват задължително информирано съгласие за участие в изследванията. Подбрани са системни потребители (в т.ч. и геймъри) в социалните мрежи, за период от над две години, по техни данни.

Самите експерименти се провеждаха в организирана мобилна лаборатория (изградена по проект ДМУ 03/22 (DMU_03_22 Project Web Page, 2011)) за полифизиографски мониторинг на мозъчна активност, сърдечен ритъм, кожно-галваничната реакция, температура на тялото, динамика на стоежа и с възможност за различни типове аудио-визуална стимулация, в т.ч. и ентрейнмънт.

А) ИЗСЛЕДВАНЕ НА ЕФЕКТА ОТ ПОПУЛЯРНА ИГРА В СОЦИАЛНИТЕ МРЕЖИ ПРИ 2D/3D ВИЗУАЛИЗАЦИЯ

Все по-мащабното навлизане на 3D визуализацията в съвременния мултимедиен и геймърски свят (Trends in Video Games and Gaming, 2011), ни накара да изследваме въздействието ѝ върху потребителите и в социалните мрежи (Minchev, 2013).

Използвана беше фокус група от 25 лица - доброволци (23 мъже и 2 жени, на възраст от 36 години ± 3) и запис на спонтанна ЕЕГ по време на забавление с играта Angry Birds в социалната мрежа Facebook.

Общата експериментална рамка (Минчев, 2012), е представена на Фиг. 4:

Фиг. 4. Обща експериментална рамка за изследване ЕЕГ динамиката при игри в социалните мрежи.

Както е показано на Фиг. 4, експерименталната рамка включва:

(i) Монитор - Monitor (използван бе IPS LG D2343P с 3D функция, оборудван с пасивни очила);
(ii) Симулационен компютър - Simulation PC (използвана е работна станция Intel® Core i5, 6 GB 1600 Mhz RAM с NVIDIA 2 GB DDR3 карта, свързана с LG монитора, посредством HDMI интерфейс за максимално качество на изображението);
(iii) ЕЕГ записваща система – EEG recording (Nation 7128W – C20, Китай, която позволява безжична работа, т.е. предоставя относителна свобода на движенията на изследваните лица). Записите от изследването бяха мониторирани в реално време и съхранени в лаптоп HP8220 с Windows XP (изискван от специализирания софтуер на производителя Nation). Използвано бе 16 битово АЦП (ADC) с честота на семплиране – f_s = 512 Hz.

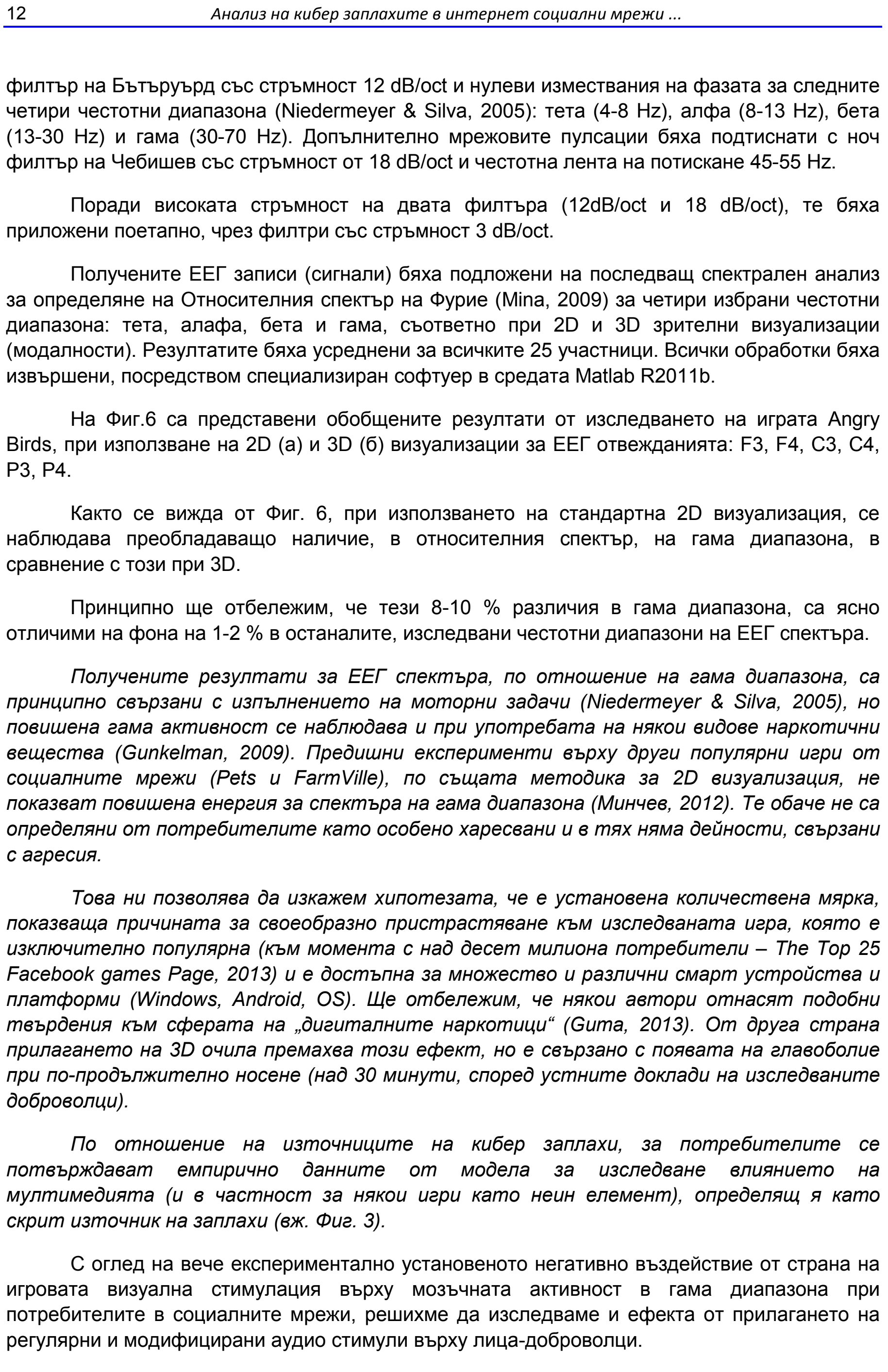
За провеждане на експериментите използвахме работна маса, удобен ергономичен офис-стол (за поставяне на подопитните лица в седяща позиция), към които беше добавено оборудването от мобилната лаборатория.

Мониторирани и записвани бяха шест отвеждания (F3, F4, C3, C4, P3, P4 по системата на Джаспер (Niedermeyer & Silva, 2005)) посредством електроди Ag/AgCl, пластична монтажна каска и специализирана електропроводима паста Ten20 Conductive. Референтните електроди A1, A2 бяха поставени стандартно – на „processi mastoidei“ на лицата, на които се извършват експериментите, а заземяващия електрод - на техните чела (вж. Фиг. 5).

Фиг. 5. Общо представяне на експеримента за изследване ЕЕГ динамиката при игра в социалните мрежи в реални условия.

Експерименталните серии бяха с времетраене от по три минутни за 2D и 3D модалностите на визуализация. По време на тези серии, доброволците играят on-line три нива на популярната Angry Birds Star Wars на Rovio® (Angry Birds Web Page, 2013) през своя Facebook потребителски профил. Всички записи бяха направени при изключен аудио сигнал в нормални работни условия и седяща позиция. Интерфейсът за управление бе ограничен до двубутонна оптична мишка Creative® със скролер.

ЕЕГ записите бяха селектирани, и само тези, без значими артефакти, бяха избрани за по-нататъшна обработка, посредством цифрова филтрация. Използван беше лентов



филтър на Бътъруърд със стръмност 12 dB/oct и нулеви изместванния на фазата за следните четири честотни диапазона (Niedermeyer & Silva, 2005): тета (4-8 Hz), алфа (8-13 Hz), бета (13-30 Hz) и гама (30-70 Hz). Допълнително мрежовите пулсации бяха подтиснати с ноч филтър на Чебишев със стръмност от 18 dB/oct и честотна лента на потискане 45-55 Hz.

Поради високата стръмност на двата филтъра (12dB/oct и 18 dB/oct), те бяха приложени поетапно, чрез филтри със стръмност 3 dB/oct.

Получените ЕЕГ записи (сигнали) бяха подложени на последващ спектрален анализ за определяне на Относителния спектър на Фурие (Mina, 2009) за четири избрани честотни диапазона: тета, алафа, бета и гама, съответно при 2D и 3D зрителни визуализации (модалности). Резултатите бяха усреднени за всичките 25 участници. Всички обработки бяха извършени, посредством специализиран софтуер в средата Matlab R2011b.

На Фиг.6 са представени обобщените резултати от изследването на играта Angry Birds, при използване на 2D (а) и 3D (б) визуализации за ЕЕГ отвежданията: F3, F4, C3, C4, P3, P4.

Както се вижда от Фиг. 6, при използването на стандартна 2D визуализация, се наблюдава преобладаващо наличие, в относителния спектър, на гама диапазона, в сравнение с този при 3D.

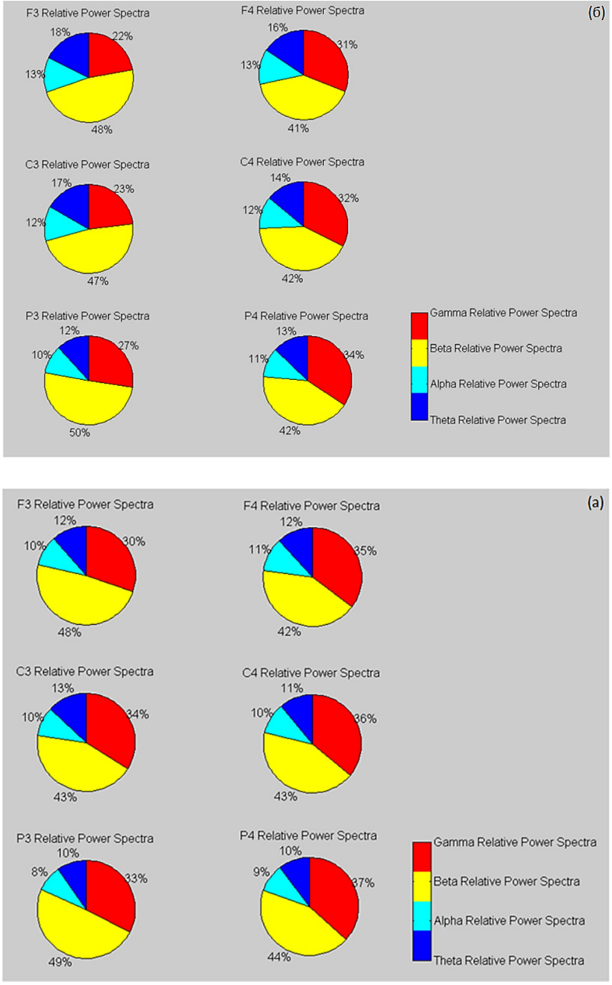
Принципно ще отбележим, че тези 8-10 % различия в гама диапазона, са ясно отличими на фона на 1-2 % в останалите, изследвани честотни диапазони на ЕЕГ спектъра.

Получените резултати за ЕЕГ спектъра, по отношение на гама диапазона, са принципно свързани с изпълнението на моторни задачи (Niedermeyer & Silva, 2005), но повишена гама активност се наблюдава и при употребата на някои видове наркотични вещества (Gunkelman, 2009). Предишни експерименти върху други популярни игри от социалните мрежи (Pets и FarmVille), по същата методика за 2D визуализация, не показват повишена енергия за спектъра на гама диапазона (Минчев, 2012). Те обаче не са определяни от потребителите като особено харесвани и в тях няма дейности, свързани с агресия.

Това ни позволява да изкажем хипотезата, че е установена количествена мярка, показваща причината за своеобразно пристрастяване към изследваната игра, която е изключително популярна (към момента с над десет милиона потребители – The Top 25 Facebook games Page, 2013) и е достъпна за множество и различни смарт устройства и платформи (Windows, Android, OS). Ще отбележим, че някои автори отнасят подобни твърдения към сферата на „дигиталните наркотици“ (Guma, 2013). От друга страна прилагането на 3D очила премахва този ефект, но е свързано с появата на главоболие при по-продължително носене (над 30 минути, според устните доклади на изследваните доброволци).

По отношение на източниците на кибер заплахи, за потребителите се потвърждават емпирично данните от модела за изследване влиянието на мултимедията (и в частност за някои игри като неин елемент), определящ я като скрит източник на заплахи (вж. Фиг. 3).

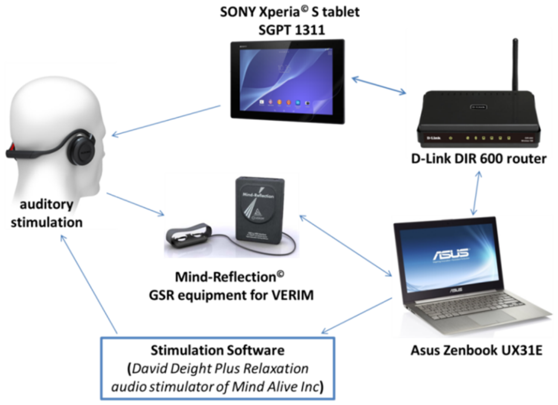
С оглед на вече експериментално установеното негативно въздействие от страна на игровата визуална стимулация върху мозъчната активност в гама диапазона при потребителите в социалните мрежи, решихме да изследваме и ефекта от прилагането на регулярни и модифицирани аудио стимули върху лица-доброволци.



Фиг. 6. Резултати от изследването на играта Angry Birds при 2D (а) и 3D (б) визуализации за ЕЕГ спектъра и отвеждания: F3, F4, C3, C4, P3, P4.

Б) ИЗСЛЕДВАНЕ НА ЕФЕКТА ОТ АУДИО СТИМУЛАЦИЯ ЧРЕЗ ПОПУЛЯРНИ МЕЛОДИИ

Изследвани бяха 15 здрави лица-доброволци (средна възраст 30 години ± 3; 10 мъже и 5 жени). Приложен бе мониторинг на кожно-галваничната реакция (КГР) чрез стандартно двуелектродно решение на Mind-Reflection©, позволяващо еластично закрепване в областта на проксималните фаланги на ръката. Общата идея на експерименталната рамка и обобщени резултати е представена в (Minchev et al, 2014) и е показана на Фиг.7.


SONY Xperia© S tablet SGPT 1311
D-Link DIR 600 router
auditory stimulation
Mind-Reflection© GSR equipment for VERIM
Asus Zenbook UX31E
Stimulation Software (*David Deight Plus Relaxation audio stimulator of Mind Alive Inc*)

Фиг. 7. Експерименталната рамка за изследване на музикални стимули чрез потребителски мониторинг на кожно-галваничната реакция.

Както е видно от Фиг. 7 експерименталната рамка, включва:

- Специализирана апаратура за измерване, мониторинг и запис на кожно-галваничната реакция, производство на Mind-Reflection© GSR, EC;
- Ултрабук Asus Zenbook© UX31E за връзка с апаратурата през USB и софтуер VERIM© Lab Light;
- Таблет SONY Xperia© SGPT 1311 за потребителски достъп до музикалните стимули;
- Стимулационен софтуер, инсталиран в David Delight Plus© аудио-визуален биофийдбек сесиен стимулатор;
- Рутер D-Link DIR 600 за осигуряване на защитен безжичен достъп до Интернет пространството и синхронизация за начало и край на експеримента по време.

Експериментът обхващаше звукова стимулация в удобна седяща позиция с подпрени, почиващи ръце върху работната маса (вж. Фиг. 8). Подобно на (Liu et al, 2011) бяха подбрани две популярни мелодии със средна продължителност от 180 секунди. Изследваните емоционални отговори, ограничихме до „страх“ със стимул *Ghost in the Machine* от албума Dark Water на Анджело Бадаламенти и „радост“ – *Увертюрата от операта Вилхем Тел* на Джоакино Росини.

Фиг. 8. Общо представяне на експеримента за изследване на музикални стимули чрез потребителски мониторинг на КГР в реални условия.

Допълнително, с цел потвърждение класификацията с надеждна статистическа значимост, мелодиите за „страх“ и „радост“ бяха сравнени с аудио стимулите „жужене на пчели“ („страх, неприятно усещане“) и „чуруликащи пойни птички“ („радост, приятно усещане“, възпроизвеждани в цикъл с обща продължителност 180 секунди) от International Affective Digitized Sounds (Bradley & Lang, 2007) на Центъра за изследване на емоциите и вниманието, САЩ. Данните ни бяха предоставени, официално, за нашата научно-изследователска работа, от страна на колегите от САЩ. Получените резултати ни дадоха над 95 % съвпадение на двете класификации за изследваните лица-доброволци.

Използваните мелодии бяха възпроизвеждани в стимулационна серия от две сесии (оригинална и манипулирана), последователно с 60 секунди пауза с тишина между всяко от възпроизвежданията.

С цел постигане на реализъм в експеримента използвахме мултимедиен уеб достъп чрез вграденото приложение на YouTube от таблета и комплект стерео Hi-Fi слушалки.

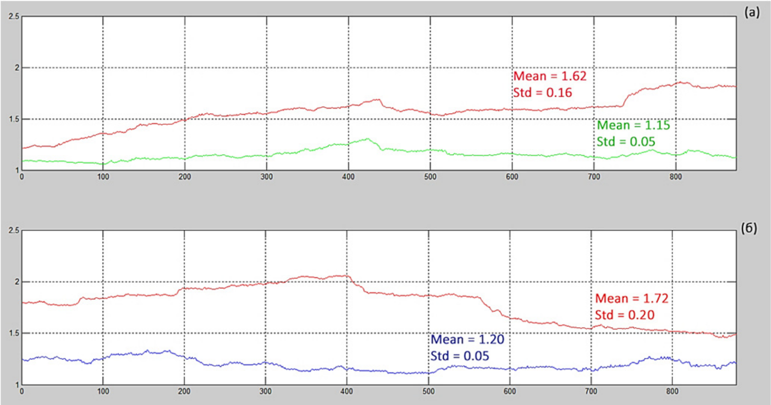
Манипулацията за всяка от мелодиите бе осъществена чрез Brain Booster бинаурална стимулация (David Delight Plus Manual, 2014), както следва: за лявото ухо - 14-10 Hz, и за дясното 19-10 Hz, насложен върху хармоничен носещ аудио сигнал чрез David Deight Plus© Relaxation аудио-визуален стимулатор на Mind Alive Inc., Канада, свързан с таблета. Използвана бе само 1/4 от изходната мощност на аудиоканала, с цел частично маскиране на стимулацията с оригиналната мелодия.

Стартирането на стимулатора и възпроизвеждането на мелодиите бе задача на потребителя, а синхронизацията по време извършвахме на база на данните от рутера D-Link DIR 600 за достъп до социалната мрежа YouTube.

Получените записи (сигнали) на КГР бяха подложени на последващ фрактален анализ за определяне на динамиката на фракталната размерност F_D по метода на Хигучи за биосигнали, използван в други подобни изследвания за ЕЕГ сигнали (Georgiev, Minchev et al, 2009).

Резултатите бяха усреднени за всичките 15 участника. Всички обработки бяха направени посредством специализиран софтуер в средата Matlab R2011b.

На Фиг. 9 са представени усреднените резултати от изследването.



Фиг. 9. Усреднени резултати за динамиката на фракталната размерност F_D по Хигучи на сигнали от КГР за „радост“ (а) и „страх“ (б) в оригинален (зелено и синьо) и стимулиран вариант (червено).

Както се вижда от Фиг. 9, при използването на допълнителна Brain Booster аудио стимулация (отбелязана в червено, (а), (б)) се наблюдава ясна разлика и при двете мелодии („радост“ – (а), зелено; „страх“ – (б), синьо) за целия експеримент с предложената мярка – динамична фрактална размерност F_D, измерена по метода на Хигучи (Georgiev, Minchev et al, 2009).

Като цяло ще отбележим, че относителните разлики в динамиката на фракталната размернот за КГР в оригиналния и стимулирания вариант на мелодиите за „радост“ и „страх“, по отношение на техните средни, са доста малки - 5 - 8 %.

Принципно използването на КГР, като биометричен показател, зависи от условията на експеримента и моментното състояние на изследваните лица-доброволци. Класическият метод за неговото прилагане при изследването на емоции, чрез поредица от въпроси и отговори и сравнение на тонична с хабитуционна кожна проводимост (Braithwaite et al, 2013) е практически трудно приложим за представената експериментална рамка и задача за идентификация на манипулации в изследваното мултимедийно съдържание.

Предложеният модифициран метод и анализ на КГР е полезен тъй като демонстрира устойчива разлика за целия период на експерименталните сесии.

*Ще отбележим, че подобни нелинейни изследвания се срещат в литературата за биометрични мултисензорни системи в различни ситуации (Prati & Batista, 2012, Kaveh-Yazdy et al, 2012), вкл. и за музикални стимули (*Makeig et al, 2011*).*

Получените резултати дават основание да приемем, че използването на динамична фрактална размерност в КГР сигнали също е полезен показател за количествена оценка на въздействието на мултимедията върху потребителите в социалните мрежи.

Предвид факта, че мултимедийното съдържание въздейства на съвременните потребители в значително по-дълги периоди и различни ситуации, в следващия параграф ще бъдат показани някои пилотни резултати и насоки за развитие на предложената идея.

В) ИЗСЛЕДВАНЕ НА ЕФЕКТА ОТ ПРИЛАГАНЕТО НА АУДИОВИЗУАЛЕН ЕНТРЕЙНМЪНТ В РАЗЛИЧНИ СИТУАЦИИ

Изследвани бяха 7 здрави лица-доброволци (средна възраст 37 години ± 8; 4 мъже и 3 жени). Приложен бе аудиовизуален ентрейнмънт (Siever, 2014, Huang & Charyton, 2008) чрез специализирана апаратура и софтуер – David Delight Plus© аудио-визуален биофийдбек сесиен стимулатор. Мониторирани и записвани бяха динамиката на ЕЕГ (чрез Nation 7128W – C20) и екскурзиите на Общия център на налягането – ОЦН (чрез нископрофилна педобарографска платформа Tekscan Evolution©, използваща резистивна технология, в сътрудничество с ТК 02/60 (TK_02_60 Project Web Page, 2010)) в изправено положение на лицата доброволци.

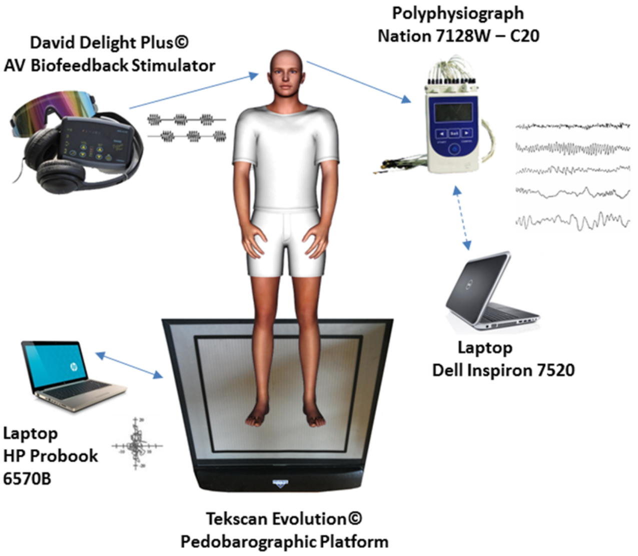
Изследването на екскурзиите на ОЦН поставя въпроса за необходимостта от разглеждане на проблема динамично в различни условия. Темата е предмет на проучване от водещи технологични компании, с акцент - нискобюджетен мониторинг на спортни поведенчески дейности (CES Fitness Tech Trends, 2014), както и въвеждане на мултимедийна интерактивност с добавена и виртуална реалност от типа Google Glasses и Oculus VR.

В рамките на сътрудничество с ДФНИ Т01/4 (DFNI_T01_4 Project Web Page, 2012), бе разработен и изпробван прототип на лента за мултимодален биомониторинг (вж. Фиг. 10) и профилиране на обитателите на смарт средата (Georgiev & Minchev, 2013, Ioannidis, Stamatogiannakis & Petsas, 2013).

Фиг.10. Използване на лента за потребителски мултимодален биомониторинг в смарт средата на обитание.

Прилагането на преносими експериментални решения изисква създаването на предварителна лабораторна методологична рамка и база данни за сравнение на получените резултати, което е посочено в последващата ни работа от настоящата точка, с използване на фабрични технологични решения.

Общата идея на експерименталната рамка за изследване на влиянието на мултимедийния (аудио-визуален) ентрейнмънт (стимулация) чрез динамиката на ЕЕГ и ОЦН е показана на Фиг.11 (Минчев и Гатев, 2014).



Фиг. 11. Експериментална рамка за изследване на ефекта от прилагането на аудиовизуален ентрейнмънт с измерване динамиката на ОЦН и ЕЕГ.

Както е видно от Фиг. 11, експерименталната рамка, включва:

- Полифизиограф Nation© 7128W – C20, Китай, който позволява безжична работа, т.е. предоставя относителна свобода на движенията на изследваните лица). Записите от изследването бяха мониторирани в реално време и съхранени в лаптоп Dell Inspiron 7520 с Windows XP (изискван от специализирания софтуер на производителя Nation). Използвано бе 16 битово АЦП с честота на семплиране – f_s = 512 Hz за ЕЕГ сигналите от шест отвеждания по системата на Джаспер 10/20 (Niedermeyer & Silva, 2005).
- Педобарографска нископрофилна резистивна платформа Tekscan© Evolution, позволяваща мониторинг, анализ и запис на екскурзиите на Общия център на налягането и наляганията на ходилата, посредством специализиран софтуер на Tekscan и лаптоп HP Probook 6570B с Windows 7, свързан през USB порта към платформата.

- David Delight Plus© аудио-визуален биофийдбек сесиен стимулатор в комплект със стимулационни LED очила, Hi-Fi слушалки и специализиран софтуер за възпроизвеждане и програмиране на стимулационни сесии за ентрейнмънт.

Експериментът обхващаше измерване, в изправен стоеж (спокоен и сетивно затруднен, чрез затваряне на очите, вж. Фиг. 12), на динамиката на ЕЕГ (от отвеждания: Fp1, Fp2, C3, C4, O1, O2 и по методиката, предложена в 2.А) и екскурзиите в ОЦН, което се извърши на три етапа: преди и след (10 и 30 минути) аудиовизулен Brain Booster ентрейнмънт, с продължителност от 20 минути (David Delight Plus, Operator's Manual, 2014).

Продължителността и на шестте измервания за ЕЕГ и ОЦН е по 60 секунди (като екскурзиите на ОЦН се измерват в 2 x 30 секунди) за всяко, а сесиите се редуват последователно за отворени и затворени очи, с цел опростяване на експеримента.

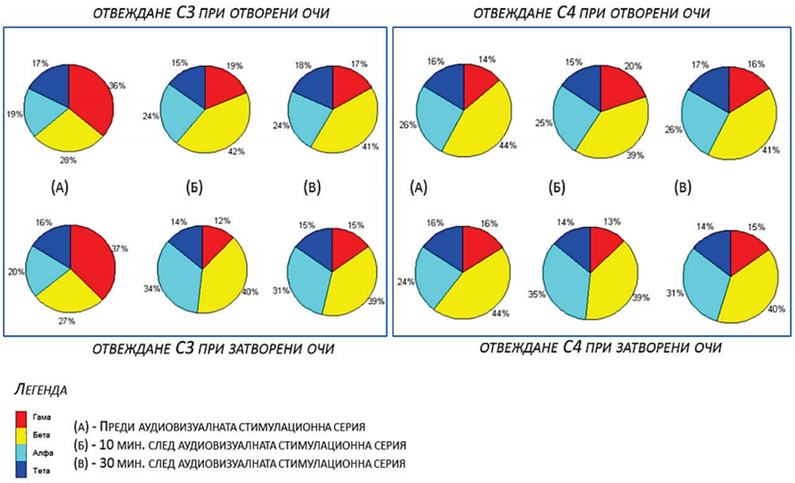
Фиг.12. Общо представяне на експеримента от сесия по прилагане на аудиовизуален ентрейнмънт (ляво) и измерване динамиката на ЕЕГ и екскурзиите на ОЦН в реални условия (дясно).

Предвид дължината на ентрейнмънт сесията (20 минути), тя се осъществява отделно в удобно седнало положение.

Получените записи (сигнали) на ЕЕГ бяха филтрирани, анализирани и оценени, подобно на 2.А с относителен спектър на мощността по Фурие за четири честотни диапазона: тета, алфа, бета и гама. Антериорно/постериорните промени в екскурзиите на ОЦН бяха подложени на анализ по метода на Хигучи за динамична, приближена оценка на фракталната размерност F_D (подобно на 2.Б и Doyle et al, 2004) и изследвани с време-честотна S-трансформация (Stockwell, 1996), използвана успешно за ЕЕГ сигнали (Minchev & Gatev, 2012).

Резултатите бяха усреднени за всичките 7 участника. Всички обработки бяха направени, посредством специализиран софтуер в средата Matlab R2011b.

На Фиг. 13 са представени усреднените резултати от изследването, преди, 10 и 30 минути след прилагането на 20 минутен Brain Booster ентрейнмънт сесията за ЕЕГ динамиката в C3 и C4 отвеждания.



Фиг.13. Промени в динамиката на ЕЕГ за отвеждания C3 и C4, преди (А), 10 мин. (Б) и 30 мин. (В) след 20 минутен Brain Booster ентрейнмънт при отворени и затворени очи.

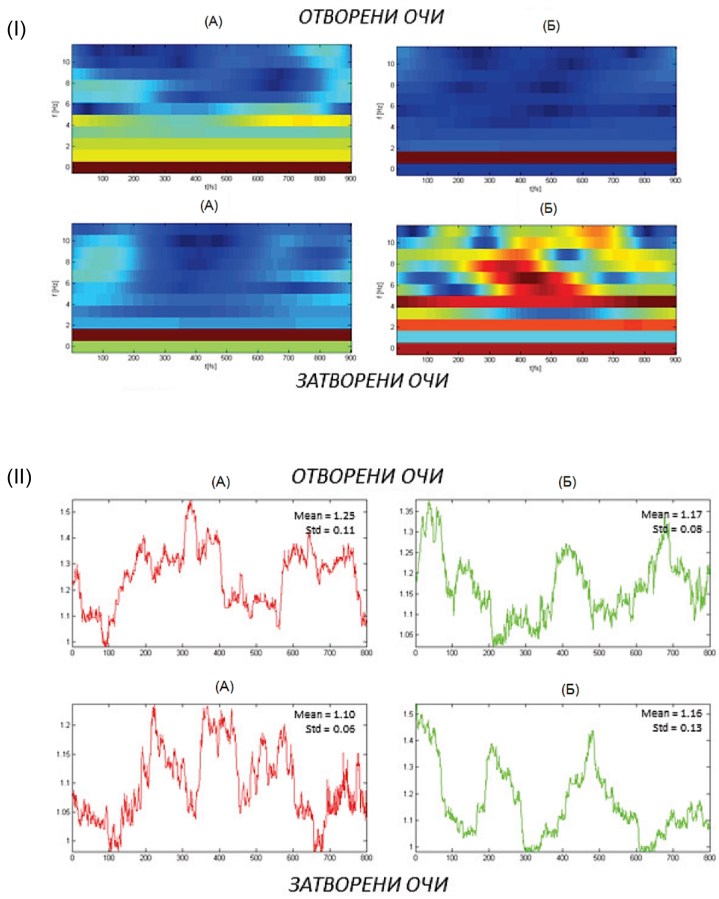
На Фиг. 14 са представени S-трансформация и F_D по Хигучи за промените в антериорно-постериорната динамика на екскурзиите на ОЦН, преди и 10 мин. след 20 минутен Brain Booster ентрейнмънт при отворени и затворени очи.

Както е видно от Фиг. 13, в избраните за представяне моменти (преди, 10 и 30 минути след Brain Boooster ентрейнмънта) и отвеждания, за ЕЕГ динамиката се наблюдава устойчиво увеличение на енергията на спектъра в бета диапазона (отбелязан в жълто) от ляво – C3 с 10-12 % при отворени очи; алфа диапазона (отбелязан в светло синьо) от дясно – C4 се увеличава с 10-15 % при затворени очи след ентрейнмънт сесията.

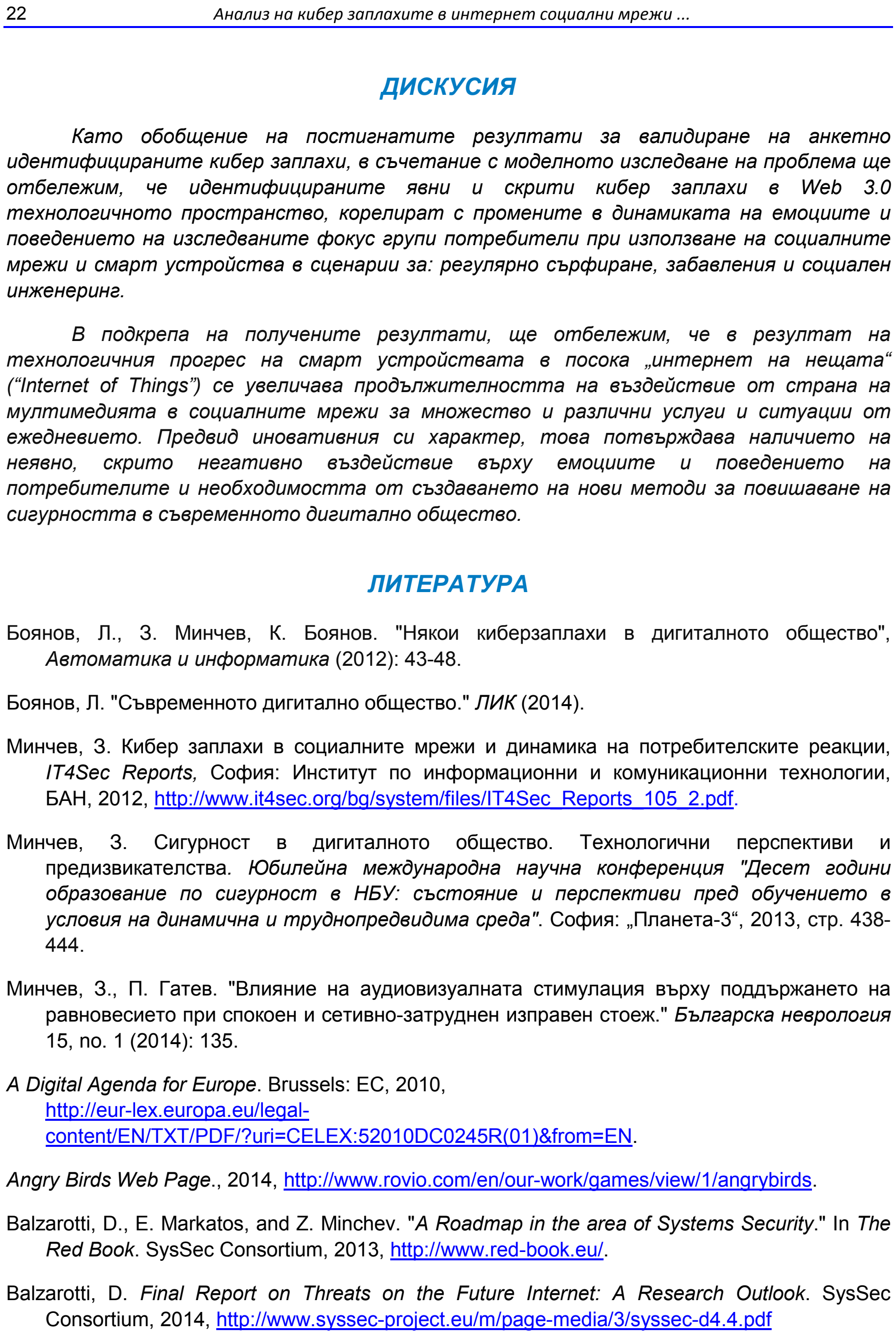
Избраните отвеждания отчитат както аудио, така и визуалните стимулационни влияния (Niedermeyer & Silva, 2005). Ще отбележим, че използваната Brain Booster стимулация бе избрана на основата на Sterman-Kaiser Imaging Lab (SKIL 3) ЕЕГ количествена база данни за невротрейнинг (SKIL 3, 2014) и като цяло се стреми към стимулирано повишаване вниманието на участниците по време на експеримента.

Антериорно-постериорните промени в динамиката на екскурзиите на ОЦН показват ясно намаляване на фракталната размерност F_D при отворени очи, 10 мин. след ентрейнмънт сесията (с около 7-8%). Това става видимо и от спектъра на S-трансформацията. Обратната тенденция се наблюдава при измервания със затворени очи, преди и след сесията.

Получените резултати за ЕЕГ спектъра показват ясно изразено стимулационно въздействие на аудиовизуалния ентрейнмънт. От друга страна, промяната в динамиката на стоежа, представена чрез екскурзиите в ОЦН след стимулацията, представлява оригинален резултат, който предоставя инструмент за идентифициране на динамични промени в позата, които не са явно откриваеми при мониторинг на обхвата на екскурзиите на ОЦН.



Фиг.14. S-трансформация (панел I) и F_D по Хигучи (панел II) за промените в антериорно-постериорната динамиката на екскурзиите на ОЦН, преди (А) и 10 мин. (Б) след 20 минутен Brain Booster ентрейнмънт при отворени и затворени очи.



ДИСКУСИЯ

Като обобщение на постигнатите резултати за валидиране на анкетно идентифицираните кибер заплахи, в съчетание с моделното изследване на проблема ще отбележим, че идентифицираните явни и скрити кибер заплахи в Web 3.0 технологичното пространство, корелират с промените в динамиката на емоциите и поведението на изследваните фокус групи потребители при използване на социалните мрежи и смарт устройства в сценарии за: регулярно сърфиране, забавления и социален инженеринг.

В подкрепа на получените резултати, ще отбележим, че в резултат на технологичния прогрес на смарт устройствата в посока „интернет на нещата" ("Internet of Things") се увеличава продължителността на въздействие от страна на мултимедията в социалните мрежи за множество и различни услуги и ситуации от ежедневието. Предвид иновативния си характер, това потвърждава наличието на неявно, скрито негативно въздействие върху емоциите и поведението на потребителите и необходимостта от създаването на нови методи за повишаване на сигурността в съвременното дигитално общество.

ЛИТЕРАТУРА

Боянов, Л., З. Минчев, К. Боянов. "Някои киберзаплахи в дигиталното общество", *Автоматика и информатика* (2012): 43-48.

Боянов, Л. "Съвременното дигитално общество." *ЛИК* (2014).

Минчев, З. Кибер заплахи в социалните мрежи и динамика на потребителските реакции, *IT4Sec Reports,* София: Институт по информационни и комуникационни технологии, БАН, 2012, http://www.it4sec.org/bg/system/files/IT4Sec_Reports_105_2.pdf.

Минчев, З. Сигурност в дигиталното общество. Технологични перспективи и предизвикателства. *Юбилейна международна научна конференция "Десет години образование по сигурност в НБУ: състояние и перспективи пред обучението в условия на динамична и труднопредвидима среда"*. София: „Планета-3", 2013, стр. 438-444.

Минчев, З., П. Гатев. "Влияние на аудиовизуалната стимулация върху поддържането на равновесието при спокоен и сетивно-затруднен изправен стоеж." *Българска неврология* 15, no. 1 (2014): 135.

A Digital Agenda for Europe. Brussels: EC, 2010, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0245R(01)&from=EN.

Angry Birds Web Page., 2014, http://www.rovio.com/en/our-work/games/view/1/angrybirds.

Balzarotti, D., E. Markatos, and Z. Minchev. "*A Roadmap in the area of Systems Security*." In *The Red Book*. SysSec Consortium, 2013, http://www.red-book.eu/.

Balzarotti, D. *Final Report on Threats on the Future Internet: A Research Outlook*. SysSec Consortium, 2014, http://www.syssec-project.eu/m/page-media/3/syssec-d4.4.pdf

Bavelier, D., C. S. Green, D. H. Han, P. F. Renshaw, M. M. Merzenich, and D. A. Gentile. "Brains on Video Games." *Nature Reviews - Neuroscience* 12 (2011): 763-768.

Bradley, M., and P. Lang. *The International Affective Digitized Sounds: Affective Ratings of Sounds and Instruction Manual* In *IADS-2*. NIMH Center for the Study of Emotion and Attention.

Braithwaite, J., D. Watson, R. Jones, and M. A. Rowe. *Guide for Analysing Electrodermal Activity & Skin Conductance Responses for Psychological Experiments* In *Technical Report*. Birmingham, UK: Selective Attention & Awareness Laboratory Behavioural Brain Sciences Centre, University of Birmingham, 2013.

CES Fitness Tech Trends. Moor Insights & Strategy, 2014, http://www.moorinsightsstrategy.com/wp-content/uploads/2014/01/CES-2014-Wearable-Sports-Fitness-Tech-Trends-FINAL.pdf.

David Delight Plus In *Operator's Manual*. Canada: Mind Alive Inc., 2014, http://www.mindalive.com/manuals/delight_plus_manual.pdf.

DFNI_T01_4 Project Web Page., 2012, www.smarthomesbg.com.

DMU_03_22 Project Web Page., 2011, www.snfactor.com.

Doyle, T., E. Dugan, B. Humphries, and R. U. Newton. "Discriminating between elderly and young using a fractal dimension analysis of centre of pressure." *Int J Med Sci* 1, no. 1 (2004): 11-20.

Georgiev, S., Z. Minchev, Ch. Christova, and D. Philipova. "EEG Fractal Dimension Measurement before and after Human Auditory Stimulation." *BIO AUTOMATION* (2009): 70-81.

Georgiev, S., and Z. Minchev. *An Evolutionary Prototyping for Smart Home Inhabitants Wearable Biomonitoring* In *Conjoint Scientific Seminar 'Modelling & Control of Information Processes'*. Vol. 12. Sofia: Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, 2013, pp. 21-30.

Guma, G. "Messing with Our Minds: Psychiatric Drugs, Cyberspace and "Digital Indoctrination"." *Global Research* (2013), http://www.globalresearch.ca/messing-with-our-minds-psychiatric-drugs-cyberspace-and-digital-indoctrination/5357710.

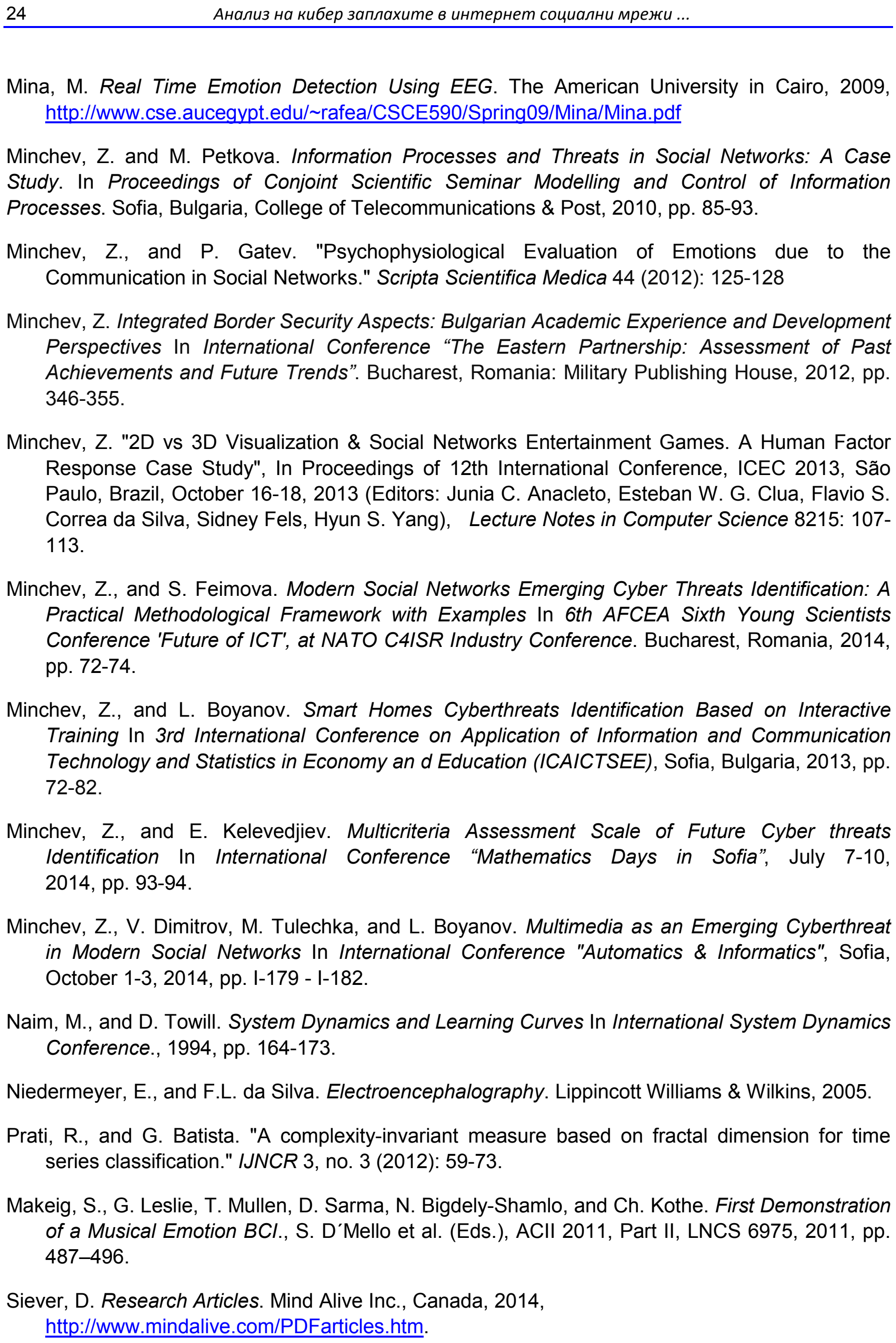
Gunkelman, J. *Drug exposure and EEG/qEEG findings*. Quantitative Electroencephalography (qEEG): Information & Discussion, 2009, http://qeegsupport.com/drug-exposure-and-eegqeeg-findings/.

Huang, T., and Ch. A. Charyton. "Comprehensive Review of the Psychological Effects of Brinwave Entrainment." *Alternative Therapies* 14, no. 5 (2008): 38-49.

Ioannidis, S., M. Stamatogiannakis, and Th. Petsas. *Deliverable D7.3: Advanced Report on Cyberattacks on Lightweight Devices*. SysSec, 2013, http://www.syssec-project.eu/m/page-media/3/syssec-d7.3-CyberattacksLightweightDevices.pdf.

Kaveh-Yazdy, F., M. Zare-Mirakabad, and F. Xia. *A novel neighbor selection approach for KNN: a physiological status prediction case study* In *1st International Workshop on Context Discovery and Data Mining (ContextDD '12)*. New York, NY, USA: ACM, 2012.

Liu, Y., O. Sourina, and M. K. Nguyen. *Real-time EEG-based Emotion Recognition and its Applications* In *Transactions on Computational Science XII, Lecture Notes in Computer Science*., 2011, pp. 256-277



Mina, M. *Real Time Emotion Detection Using EEG*. The American University in Cairo, 2009, http://www.cse.aucegypt.edu/~rafea/CSCE590/Spring09/Mina/Mina.pdf

Minchev, Z. and M. Petkova. *Information Processes and Threats in Social Networks: A Case Study*. In *Proceedings of Conjoint Scientific Seminar Modelling and Control of Information Processes*. Sofia, Bulgaria, College of Telecommunications & Post, 2010, pp. 85-93.

Minchev, Z., and P. Gatev. "Psychophysiological Evaluation of Emotions due to the Communication in Social Networks." *Scripta Scientifica Medica* 44 (2012): 125-128

Minchev, Z. *Integrated Border Security Aspects: Bulgarian Academic Experience and Development Perspectives* In *International Conference "The Eastern Partnership: Assessment of Past Achievements and Future Trends"*. Bucharest, Romania: Military Publishing House, 2012, pp. 346-355.

Minchev, Z. "2D vs 3D Visualization & Social Networks Entertainment Games. A Human Factor Response Case Study", In Proceedings of 12th International Conference, ICEC 2013, São Paulo, Brazil, October 16-18, 2013 (Editors: Junia C. Anacleto, Esteban W. G. Clua, Flavio S. Correa da Silva, Sidney Fels, Hyun S. Yang), *Lecture Notes in Computer Science* 8215: 107-113.

Minchev, Z., and S. Feimova. *Modern Social Networks Emerging Cyber Threats Identification: A Practical Methodological Framework with Examples* In *6th AFCEA Sixth Young Scientists Conference 'Future of ICT', at NATO C4ISR Industry Conference*. Bucharest, Romania, 2014, pp. 72-74.

Minchev, Z., and L. Boyanov. *Smart Homes Cyberthreats Identification Based on Interactive Training* In *3rd International Conference on Application of Information and Communication Technology and Statistics in Economy an d Education (ICAICTSEE)*, Sofia, Bulgaria, 2013, pp. 72-82.

Minchev, Z., and E. Kelevedjiev. *Multicriteria Assessment Scale of Future Cyber threats Identification* In *International Conference "Mathematics Days in Sofia"*, July 7-10, 2014, pp. 93-94.

Minchev, Z., V. Dimitrov, M. Tulechka, and L. Boyanov. *Multimedia as an Emerging Cyberthreat in Modern Social Networks* In *International Conference "Automatics & Informatics"*, Sofia, October 1-3, 2014, pp. I-179 - I-182.

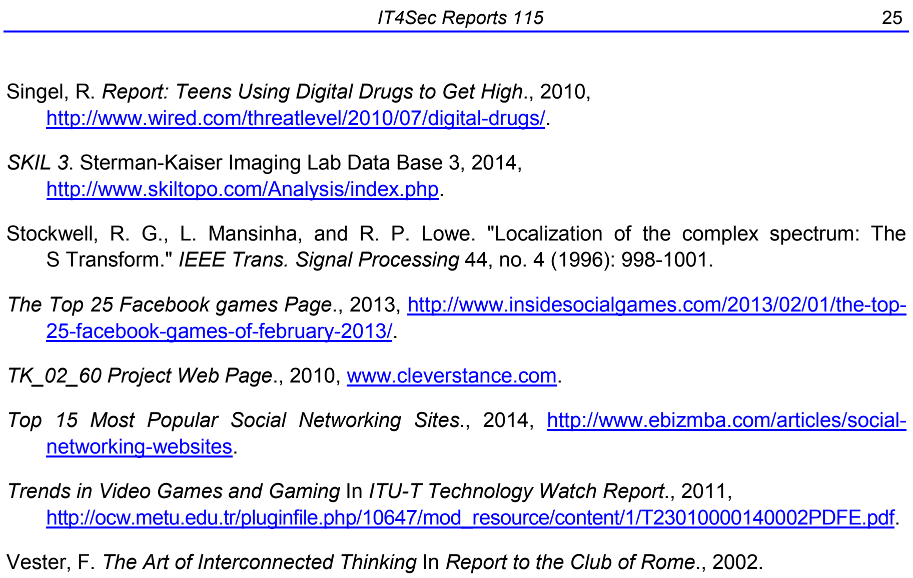
Naim, M., and D. Towill. *System Dynamics and Learning Curves* In *International System Dynamics Conference*., 1994, pp. 164-173.

Niedermeyer, E., and F.L. da Silva. *Electroencephalography*. Lippincott Williams & Wilkins, 2005.

Prati, R., and G. Batista. "A complexity-invariant measure based on fractal dimension for time series classification." *IJNCR* 3, no. 3 (2012): 59-73.

Makeig, S., G. Leslie, T. Mullen, D. Sarma, N. Bigdely-Shamlo, and Ch. Kothe. *First Demonstration of a Musical Emotion BCI*., S. D´Mello et al. (Eds.), ACII 2011, Part II, LNCS 6975, 2011, pp. 487–496.

Siever, D. *Research Articles*. Mind Alive Inc., Canada, 2014, http://www.mindalive.com/PDFarticles.htm.



Singel, R. *Report: Teens Using Digital Drugs to Get High*., 2010, http://www.wired.com/threatlevel/2010/07/digital-drugs/.

SKIL 3. Sterman-Kaiser Imaging Lab Data Base 3, 2014, http://www.skiltopo.com/Analysis/index.php.

Stockwell, R. G., L. Mansinha, and R. P. Lowe. "Localization of the complex spectrum: The S Transform." *IEEE Trans. Signal Processing* 44, no. 4 (1996): 998-1001.

The Top 25 Facebook games Page., 2013, http://www.insidesocialgames.com/2013/02/01/the-top-25-facebook-games-of-february-2013/.

TK_02_60 Project Web Page., 2010, www.cleverstance.com.

Top 15 Most Popular Social Networking Sites., 2014, http://www.ebizmba.com/articles/social-networking-websites.

Trends in Video Games and Gaming In *ITU-T Technology Watch Report*., 2011, http://ocw.metu.edu.tr/pluginfile.php/10647/mod_resource/content/1/T23010000140002PDFE.pdf.

Vester, F. *The Art of Interconnected Thinking* In *Report to the Club of Rome*., 2002.

8

When Smart Cities meet Big Data

Authors Vincenzo Gulisano, Magnus Almgren and Marina Papatriantafilou

Dissemination SysSec website, and ERCIM news

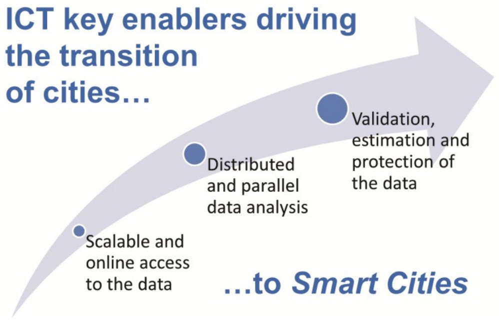
This whitepaper appeared as an article in ERCIM news, with a high-level report on security issues in information sharing, in the context of smart cities. It ias important because it shows the continuing cooperation with the EU-funded project CRISALIS.

When Smart Cities meet Big Data

by Vincenzo Gulisano, Magnus Almgren and Marina Papatriantafilou[1]

Sharing information is a key enabler in the transition of a city becoming *smart*. Information, generated by the ICT backbone of a city, and maintained by distinct public and private entities, comes with processing challenges that must be addressed in order to increase citizens' quality of life and make their cities sustainable. In CRISALIS and SysSec, we investigate such challenges from a security perspective in order to protect and enhance smart cities' sensitive infrastructures.

The possibilities enabled by Information and Communication Technologies (ICTs) are driving the evolution and transition of cities to Smart Cities. The ultimate goal is to increase the awareness of citizens', companies' and authorities' and improve their quality of life while also making it sustainable. A considerable number of research directions embrace Smart Cities: users' privacy protection [1], detection of malicious actions and misuses and users' awareness through social media. More research efforts are dedicated to specific features of a Smart City. As an example, the energy forecast techniques used to predict consumption and allow the usage of alternative energy resources (e.g., solar or wind power) to be scheduled. What all these research fields have in common is their dependency on the (possibly sensitive) data produced by the devices forming the Internet of Things (IoT) of a city. The possibilities enabled by Smart Cities demand for novel data processing paradigms to form the expertise of public and private companies. Based on our experience with both academic and industrial partners, in this article we discuss some of the challenges associated with data processing in Smart Cities.


ICT key enablers driving the transition of cities…
Scalable and online access to the data
Distributed and parallel data analysis
Validation, estimation and protection of the data
…to Smart Cities

Scalable and online access to the data
In a Smart City, millions of messages will be exchanged on a daily basis by hundreds of thousands of devices (e.g., mobile phones, electrical meters, weather stations, etc.). For example, more than 1.2 million messages are exchanged on a daily basis within an AMI infrastructure (owned by one of our industrial partners) that covers a metropolitan area with roughly 600,000 inhabitants [2]. The information generated by such devices could be matched and joined to enhance the management of Smart Cities. For example, energy or water losses caused by faulty devices could be reduced by matching the consumption measured by users' meters with the one measured by other utilities' systems. To this end, on-the-fly processing of data becomes all the more important while traditional

[1] Published in ERCIM News #98, http://ercim-news.ercim.eu/en98/special/when-smart-cities-meet-big-data

store-then-process approaches in which each company retrieves its data and stores it in order to access it sometime in the future might be no longer appropriate.

Think in a distributed and parallel fashion.
Smart Cities will be composed of several independent networks (even within the same stakeholder). Hence, no centralized application will embrace the information carried by the messages exchanged by the devices. At the same time, the huge volume of information shared by ICT devices will make parallel processing a necessity [3]. To this end, pushing the analysis closer to the sources of information would be a natural way of analyzing the messages exchanged by them and leverage the information they carry. Challenging aspects in this context will be imposed by the constrained resources of such devices.

Validate, estimate and protect the data.
Cheap, resource-constrained devices are largely employed to build the networks that will form the IoT of a Smart City. Unfortunately, the data measured and reported by such devices (e.g., energy consumption readings) is usually noisy and lossy. Reasons of this are not limited uniquely to the devices themselves (e.g., faulty or badly calibrated devices, lossy or overloaded communication channels) but can also be caused by (possibly malicious) citizens. As an example, incorrect consumption readings could be manipulated by malicious users aiming to lower their bills. To this end, validation schemes, estimation schemes and security countermeasures must be adopted in order to ensure that who leverages the information is not mislead by incorrect, partial or malicious data.

The shift from cities to Smart Cities depends on the efficiency with which information is shared among citizens and private and public companies. This information brings challenges, and, following the big data revolution, novel processing schemes must be adopted to enable the possibilities that exist of this domain. All the possibilities enabled by smart cities, like improved quality of life or energy efficiency, shall build on top of efficient data processing and users' privacy protection schemes.

CRISALIS may be contacted at contact@crisalis-project.eu. SysSec may be contacted at the corresponding contact@syssec-project.eu, followed in twitter (twitter:syssecproject) and Facebook (http://www.facebook.com/SysSec).

References:

[1] V. Tudor, M. Almgre y M. Papatriantafilou, «Analysis of the Impact of Data Granularity on Privacy for the Smart Grid,» de *WPES '13 Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society*, 2013.

[2] Z. Fu, O. Landsiedel, M. Almgren and M. Papatriantafilou, "Managing your Trees: Insights from a Metropolitan-Scale Low-Power Wireless Network," in *CCSES'14: Proceedings of the 3rd Workshop on Communications and Control for Smart Energy Systems held in conjunction with the 33rd IEEE International Conference on Computer Communications (INFOCOM)*, 2014.

[3] V. Gulisano, M. Almgren and M. Papatriantafilou, "METIS: a Two-Tier Intrusion Detection System for Advanced Metering Infrastructures," in *The fifth International Conference on Future Energy Systems (ACM e-Energy)*, 2014.

Please contact:
Vincenzo Gulisano
vinmas@chalmers.se

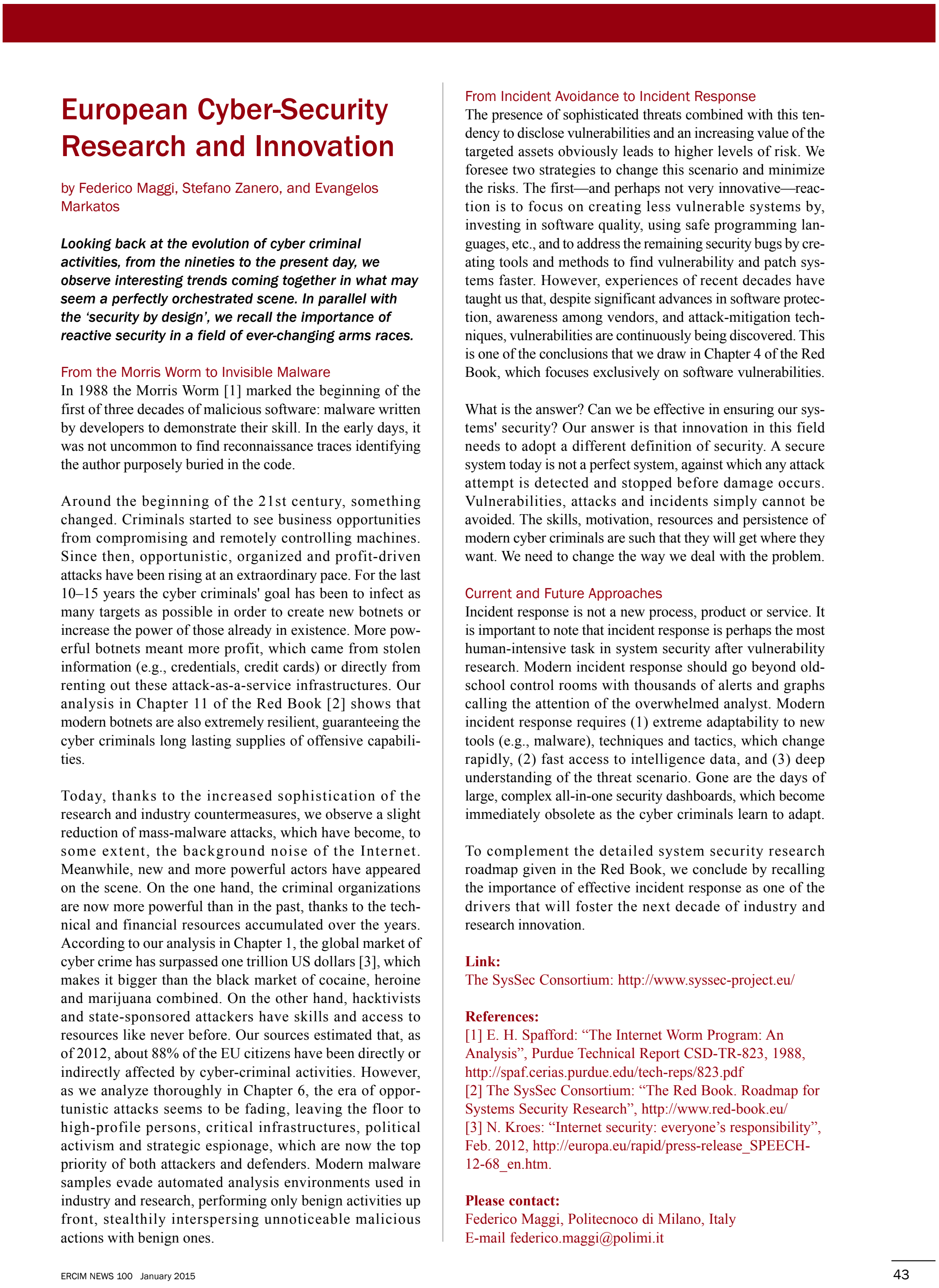
9

European Cyber-Security Research and Innovation

Authors Federico Maggi, Evangelos Markatos, Stefano Zanero

Dissemination SysSec website, and ERCIM news

This whitepaper appeared as an article in ERCIM news, with a high-level description of some of the key insights in the SysSec Red Book, in order to disseminate those results to a wider readership and entice further downloads and reading of the Red Book deliverable.



European Cyber-Security Research and Innovation

by Federico Maggi, Stefano Zanero, and Evangelos Markatos

Looking back at the evolution of cyber criminal activities, from the nineties to the present day, we observe interesting trends coming together in what may seem a perfectly orchestrated scene. In parallel with the 'security by design', we recall the importance of reactive security in a field of ever-changing arms races.

From the Morris Worm to Invisible Malware

In 1988 the Morris Worm [1] marked the beginning of the first of three decades of malicious software: malware written by developers to demonstrate their skill. In the early days, it was not uncommon to find reconnaissance traces identifying the author purposely buried in the code.

Around the beginning of the 21st century, something changed. Criminals started to see business opportunities from compromising and remotely controlling machines. Since then, opportunistic, organized and profit-driven attacks have been rising at an extraordinary pace. For the last 10–15 years the cyber criminals' goal has been to infect as many targets as possible in order to create new botnets or increase the power of those already in existence. More powerful botnets meant more profit, which came from stolen information (e.g., credentials, credit cards) or directly from renting out these attack-as-a-service infrastructures. Our analysis in Chapter 11 of the Red Book [2] shows that modern botnets are also extremely resilient, guaranteeing the cyber criminals long lasting supplies of offensive capabilities.

Today, thanks to the increased sophistication of the research and industry countermeasures, we observe a slight reduction of mass-malware attacks, which have become, to some extent, the background noise of the Internet. Meanwhile, new and more powerful actors have appeared on the scene. On the one hand, the criminal organizations are now more powerful than in the past, thanks to the technical and financial resources accumulated over the years. According to our analysis in Chapter 1, the global market of cyber crime has surpassed one trillion US dollars [3], which makes it bigger than the black market of cocaine, heroine and marijuana combined. On the other hand, hacktivists and state-sponsored attackers have skills and access to resources like never before. Our sources estimated that, as of 2012, about 88% of the EU citizens have been directly or indirectly affected by cyber-criminal activities. However, as we analyze thoroughly in Chapter 6, the era of opportunistic attacks seems to be fading, leaving the floor to high-profile persons, critical infrastructures, political activism and strategic espionage, which are now the top priority of both attackers and defenders. Modern malware samples evade automated analysis environments used in industry and research, performing only benign activities up front, stealthily interspersing unnoticeable malicious actions with benign ones.

From Incident Avoidance to Incident Response

The presence of sophisticated threats combined with this tendency to disclose vulnerabilities and an increasing value of the targeted assets obviously leads to higher levels of risk. We foresee two strategies to change this scenario and minimize the risks. The first—and perhaps not very innovative—reaction is to focus on creating less vulnerable systems by, investing in software quality, using safe programming languages, etc., and to address the remaining security bugs by creating tools and methods to find vulnerability and patch systems faster. However, experiences of recent decades have taught us that, despite significant advances in software protection, awareness among vendors, and attack-mitigation techniques, vulnerabilities are continuously being discovered. This is one of the conclusions that we draw in Chapter 4 of the Red Book, which focuses exclusively on software vulnerabilities.

What is the answer? Can we be effective in ensuring our systems' security? Our answer is that innovation in this field needs to adopt a different definition of security. A secure system today is not a perfect system, against which any attack attempt is detected and stopped before damage occurs. Vulnerabilities, attacks and incidents simply cannot be avoided. The skills, motivation, resources and persistence of modern cyber criminals are such that they will get where they want. We need to change the way we deal with the problem.

Current and Future Approaches

Incident response is not a new process, product or service. It is important to note that incident response is perhaps the most human-intensive task in system security after vulnerability research. Modern incident response should go beyond old-school control rooms with thousands of alerts and graphs calling the attention of the overwhelmed analyst. Modern incident response requires (1) extreme adaptability to new tools (e.g., malware), techniques and tactics, which change rapidly, (2) fast access to intelligence data, and (3) deep understanding of the threat scenario. Gone are the days of large, complex all-in-one security dashboards, which become immediately obsolete as the cyber criminals learn to adapt.

To complement the detailed system security research roadmap given in the Red Book, we conclude by recalling the importance of effective incident response as one of the drivers that will foster the next decade of industry and research innovation.

Link:
The SysSec Consortium: http://www.syssec-project.eu/

References:

[1] E. H. Spafford: "The Internet Worm Program: An Analysis", Purdue Technical Report CSD-TR-823, 1988, http://spaf.cerias.purdue.edu/tech-reps/823.pdf
[2] The SysSec Consortium: "The Red Book. Roadmap for Systems Security Research", http://www.red-book.eu/
[3] N. Kroes: "Internet security: everyone's responsibility", Feb. 2012, http://europa.eu/rapid/press-release_SPEECH-12-68_en.htm.

Please contact:

Federico Maggi, Politecnoco di Milano, Italy
E-mail federico.maggi@polimi.it