2014

Strategies to Counter Cyber Attacks: Cyber Threats and Critical Infrastructure Protection

Bilge Karabacak
Franklin University, bilge.karabacak@franklin.edu

Unal Tatar

Strategies to Counter Cyber Attacks:

Cyber Threats and Critical Infrastructure Protection

Bilge KARABACAK, Chief Researcher, TÜBİTAK-BİLGEM
Ünal TATAR, Senior Researcher, TÜBİTAK-BİLGEM

Abstract. Today, cyber threats have the potential to harm critical infrastructures which may result in the interruption of life-sustaining services, catastrophic economic damages or severe degradation of national security. The diversity and complexity of cyber threats that exploit the vulnerabilities of critical infrastructures increase every day. . In order to lessen the potential harm of cyber threats, countermeasures have to be applied and the effectiveness of these countermeasures has to be monitored continuously. In this study, a brief definition and history of critical infrastructures are introduced. Cyber threats are examined in four fundamental categories. Vulnerabilities of critical infrastructures are categorized and examined. Finally, countermeasures that may play a key role in critical infrastructure protection programs are categorized.

1. Introduction

Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and the government.[1] Critical Infrastructure Protection (CIP) is an important program in which governments have to take action in order to cope with cyber threats. The first formal document that uses the term "critical infrastructure" dates back to 15 July 1996, which is an executive order signed by the U.S. president.[2] Physical threats and 'cyber threats' are stated as two major threat types in this executive order. The purpose of the executive order is to set forth the basic steps of CIP.

[1] The White House, Presidential Decision Directive/NSC-63 at http://www.fas.org/irp/offdocs/pdd/pdd-63.htm (accessed 12 June 2012)
[2] Presidential Executive Order 13010, Critical Infrastructure Protection, p. 3.

According to the Presidential Decision Directive, many of the critical infrastructures have historically been physically and logically separate systems that had little interdependence. As a result of advances in information technology and the necessity of improved efficiency, however, these infrastructures have become increasingly automated and interlinked.[3] Therefore, it is important to note that the term of "critical infrastructure protection" was proposed after the widespread use of information technologies in these infrastructures. Critical infrastructures and information technologies have strong relationships in many different ways and levels.[4]

Cyber threats are evolving with each passing day. Almost every week, a new cyber incident appears in the media. Cyber threats are asymmetric in nature.[5] They can harm critical infrastructures in great extent by making minor cyber operations. In this paper, cyber threats against critical infrastructures are tried to be categorized. The vulnerabilities of critical infrastructures are defined. The countermeasures for the resulting risks are categorized and listed.

2. Strategies to Counter Cyber Attacks

In this part of the paper, cyber assets, cyber threats, vulnerabilities of critical infrastructures and countermeasures are explained in the following four subsections respectively.

2.1 Cyber Assets: Critical Infrastructures

Today, almost all critical sectors use cyber systems. Transportation, banking and finance, health and emergency, defense sectors and vital government facilities use conventional information technologies. Telecommunications sector is also a critical infrastructure and it is entirely composed of information technologies.[6] Some of the critical sectors are controlled and monitored

---

[3] The White House, Presidential Decision Directive/NSC-63 at http://www.fas.org/irp/offdocs/pdd/pdd-63.htm (accessed 12 June 2012)

[4] Jayawickrama, "Managing Critical Information Infrastructure Security Compliance: A Standard Based Approach Using ISO/IEC 17799 and 27001" p. 563.

[5] Kshetri, "Information and communications technologies, strategic asymmetry and national security" p. 564.

[6] Beltran, "Internet as a critical infrastructure: lessons from the backbone experience in South America", p. 1.

by SCADA systems, which are specially crafted software and equipment. SCADA stands for Supervisory Control and Data Acquisition. Energy, water and critical manufacturing are key sectors that use SCADA systems.

In the 70s, 80s and even in the 90s, SCADA systems were legacy systems. They composed of exotic, proprietary and even obscure hardware and software. The SCADA systems were almost unique to the specific infrastructure. SCADA systems were isolated as well. There were no access to corporate networks and the Internet. In those days, there was no Internet in fact.

Today, SCADA systems use open international standards for most of the operations. They use standard hardware, software, operating systems, and protocols. SCADA systems make use of COTS (Commercial off the shelf) products in most cases. Today, SCADA systems are well documented as well. Finally, SCADA systems are connected to corporate networks and even to the Internet by wired or wireless means.[7] Therefore, energy and water industries may be exposed to cyber threats directly.

In general, almost all of the critical sectors are connected to the Internet. Although Internet is a physically distributed infrastructure, it is logically unified. In this unique logical infrastructure, we live with cyber threats like cyber attacks, cyber criminals and cyber spies. In the next subsection, cyber threats are elucidated in four categories.

2.2 Cyber Threats

Cyber threats can be categorized in four main groups.[8] These groups are hacktivism, cyber crime, cyber espionage and cyber war. However there is no clear-cut distinction among these groups as shown in Figure-1. These categorized cyber threats can intersect with each other in many different ways. A member of a hacktivist group may get into a cyber crime activity. The

[7] Igure, "Security Issues in SCADA Networks" p. 500.
[8] Prichard, "Cyber Terrorism: A Study of the Extent of Coverage in Computer Security Textbooks" p. 280.

same guy may take part in coordinated cyber war or cyber espionage.

A cyber act can be categorized or perceived as both cyber war and hacktivism. As an example, a country can consider a cyber incident as cyber war. On the contrary, another country can consider the same act as hacktivism.

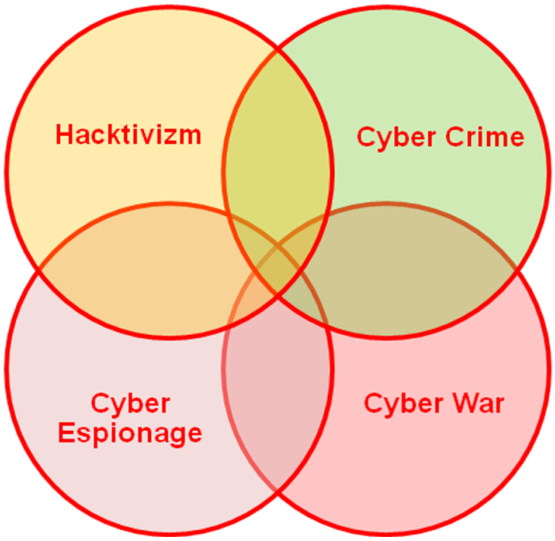

Figure 1: Four types of cyber threats

When critical infrastructures are taken into consideration, cyber espionage and cyber war are much more harmful than hacktivism and cyber crime.

2.2.1 Hacktivism

Hacktivists create opportunistic attacks against weak targets. The power of hacktivists comes from their number. Hacktivism is the activity of a group of hackers. The hacker group 'Anonymous' is a hacktivist group. The main purpose of hacktivists is not to make money. Rather, they protest something. For example, they protest the governmental restrictions to the Internet and they take aim at the websites of public organizations.

Hacktivists usually perform Denial of Service (DoS) attacks. A DoS attack can be defined as purposefully flooding the bandwidth or resources of a targeted system with a huge number of

legitimate service requests. Hacktivists usually target the availability of networks and systems by performing DoS attacks. In addition to DoS attacks, hacktivists try to deface websites, especially websites of public organizations. They do not usually try to deface a specific website for a long time. Rather, they search for a specific vulnerability on a number of websites and deface all of the websites in their search scope that contain the specific vulnerability. Hacktivist use botnets or get contact with the owner of botnets in order to perform Distributed DoS (DDoS) attacks to guarantee the unavailability of networks and systems.

2.2.2 Cyber Crime

By contrast with hacktivists, the main purpose of cyber criminals is to make money. Cyber criminals are individuals. Usually, they do not act in groups like hacktivists. They steal credit card information, bank account credentials and passwords. The target critical sector for cyber criminals is banking and finance. Compared to the other threat types, cyber crime does not have a prominent effect on critical infrastructures.

2.2.3 Cyber Espionage

Cyber espionage is basically the act of stealing documents from networks of foreign countries [9]. The loss of confidentiality is the major consequence of cyber espionage. The term Advanced Persistent Threat (APT) is used under the context of cyber espionage. According to the Mandiant, which is a famous information security company, APT is a group of sophisticated, determined and coordinated attackers that have been systematically compromising (U.S.) government and commercial computer networks for years. The vast majority of APT activity observed by Mandiant has been linked to China.[10]

According to the Department of Defense Strategy for Operating in Cyberspace, every year, an

[9] Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats", p. 9.
[10] Mandiant, M Trends, The Advanced Persistent Threat, p. 1.

amount of intellectual property larger than that contained in the Library of Congress is stolen from networks maintained by U.S. businesses, universities, and government departments and agencies. [11]

US - China Economic and Security Review Commission of USA prepared a report to Congress in 2008. According to this report, China has an active cyber espionage program. This report says that China's cyber warfare is so sophisticated that the United States may be unable to counteract or even detect the efforts.[12]

2.2.4 Cyber War

Cyber war is the coordinated attacks to specific critical sectors of a country. Every critical sector is a potential target of cyber war. Most of the cyber security experts think that Stuxnet virus is the beginning of real cyber war. Stuxnet was discovered in June 2010. The target of the Stuxnet virus was the availability of Iranian nuclear energy infrastructure. According to a New York Times report, which was released on 1 January 2012, President Obama secretly ordered increasingly sophisticated attacks on the computer systems that run Iran's main nuclear enrichment facilities, significantly expanding America's first sustained use of cyber weapons, according to participants in the program.[13] The cyber attacks against the availability of Estonian and Georgian websites and network infrastructures are another example of cyber war. Although Russia did not undertake those attacks as a government, the coordinated attacks were performed by Russian people. The target of cyber war is not only the availability of systems and networks. A virus called 'duqu' affected the confidentiality of Iranian energy infrastructure. Duqu was discovered after Stuxnet. It is considered that the source of duqu and Stuxnet was the same

[11] Department of Defense, Strategy for Operating in Cyberspace, p. 4.
[12] US - China Economic and Security Review Commission, 2008 Report to Congress, p. 164.
[13] New York Times, "Middle East Page" at http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all (accessed 13 June 2012)

because of their similarities. Duqu provided services to the attackers; currently this includes information stealing capabilities.[14] The last discovered malware is called Flame, Flamer or Skywiper. According to the New York Times, Flame appears to be part of the state-sponsored campaign that spied on and eventually set back Iran's nuclear program in 2010.[15]

2.2.5 Cyber Threats - Final Remarks

The number of cyber espionage and cyber war activities is low compared to the number of cyber crime and hacktivist attacks. When the economic damage and national security is the main concern, the impact level of cyber espionage is very high compared to the impact level of other threats types.[16] Although cyber espionage attacks are low in number, they cause intellectual property losses. This has a great value for a country. Although cyber crime activities are large in number, the loss is limited to credentials and money. When the public safety is the main concern, the impact level of cyber war is high compared to the impact level of other threat types. Cyber war can affect the availability of SCADA systems and corporate networks.

According to the draft Cyber Security Act of 2012, an industry can be defined as "critical" if damage or unauthorized access to that system could reasonably

a) Result in the interruption of life-sustaining services,
b) Cause catastrophic economic damages or
c) Cause severe degradation of national security. [17]

By using this damage classification, the prominent effects of the four threat categories on critical infrastructures are shown in Table-1. Although there is no crystal-clear classification and

[14] Wikipedia, "Duqu article" at http://en.wikipedia.org/wiki/Duqu (accessed 13 June 2012)
[15] New York Times, "Technology Page" at http://www.nytimes.com/2012/05/31/technology/researchers-link-flame-virus-to-stuxnet-and-duqu.html (accessed 13 June 2012)
[16] Kshetri, "Patterns of Global Cyber War and Crime: A Conceptual Framework" p. 552.
[17] The Senate of United States, The Draft Cyber Security Act of 2012, http://www.hsgac.senate.gov/download/the-cybersecurity-act-of-2012-s-2105 (accessed 13 June 2012)

correlation between threat types and impact types, Table-1 shares the notion that cyber espionage and cyber war are much more harmful than cyber crime and hacktivism.

THREAT TYPE	IMPACT TYPE
Hacktivism	The interruption of life-sustaining services (Minor)
Cyber Crime	Economic damages (Minor)
Cyber Espionage	Economic damages (Major) Severe degradation of national security
Cyber War	The interruption of life-sustaining services (Major) Economic damages (Intermediate)

Table 1: Threat categories versus impacts

2.3 Vulnerabilities

Vulnerabilities of critical infrastructures can be classified into two major groups, which are technical vulnerabilities and non-technical vulnerabilities.

2.3.1 Technical Vulnerabilities

Technical vulnerabilities are divided into two subgroups; which are basic protocol vulnerabilities and application vulnerabilities. Basic protocol vulnerabilities are the vulnerabilities of common Internet protocols.[18] The core protocols of the Internet such as Internet Protocol (IP), Transmission Control Protocol (TCP), Domain Name System (DNS), Hypertext Transfer Protocol (HTTP) and routing protocols were designed and implemented without focusing on security features since the Internet was initially used in academic and governmental environments. At these environments, humans were trusted entities. Security countermeasures are included in Internet protocols as add-ons after the proliferation and widespread use of the

[18] Alcaraz-Tello, "Secure Management of SCADA Networks" p. 23.

Internet. Therefore, the Internet is vulnerable to basic and competent attacks like denial of service, eavesdropping, spoofing and sniffing. Apart from basic protocols, there are a number of applications including operating systems that logically run on top of basic protocols. According to the IBM X-force report, there is exponential increase in cumulative vulnerability disclosures from 1996 to 2010.[19] These application vulnerabilities are exploited by attackers to gain access privileges to remote systems, to steal information and to stop services.

2.3.2 Non-technical Vulnerabilities

In spite of the state-of-the-art security systems, such as digital signatures, cryptography, biometric security, stateful firewalls, intrusion prevention systems, access control systems, the number of security breaches increases. Even closed networks are infected with targeted worms and viruses as in the case of Stuxnet. It is argued by security experts that Stuxnet infected the closed energy network of Iran by means of USB thumb drives of the workers of the nuclear enrichment facilities. The reason for security breaches is non-technical vulnerabilities. Non-technical vulnerabilities are related with the people and the processes.[20] Unfortunately, the weakest link for security is the human being. As an example, in November 2008, US-CERT issued a warning that malicious code was increasingly propagating via USB flash drive devices. The fact that USB thumb drives are being used by so many people makes them an attractive target for malware writers.[21] In those days, US Department of Defense has temporarily banned the use of thumb drives, CDs and other removable storage.[22] Although, technical countermeasures are vital for the security of critical infrastructures, it will not be as effective as expected without improvements in the behavior of people and security processes.

---

[19] IBM X-force, 2010 Trend and Risk Report, p. 75.
[20] Stouffer, "Guide to Industrial Control Systems (ICS) Security", p. 3-7.
[21] CNET, News Site at http://news.cnet.com/8301-1009_3-10104496-83.html (accessed 13 June 2012)
[22] Wired, website at http://www.wired.com/dangerroom/2008/11/army-bans-usb-d (accessed 13 June 2012)

2.3.3 Vulnerabilities - Final Remarks

Certain threat types exploit certain vulnerabilities as shown in Table-2. Although it is not a golden rule, hacktivists generally exploit basic protocols at first, and then application vulnerabilities. Cyber criminals usually exploit application vulnerabilities. Cyber warriors use application and infrastructure vulnerabilities like hacktivists. Finally, cyber spies exploit people and process vulnerabilities.

THREAT TYPE	EXPLOITED VULNERABILITY TYPE
Hacktivism	Basic Protocol Vulnerabilities Application Vulnerabilities
Cyber Crime	Application Vulnerabilities
Cyber Espionage	Non-technical Vulnerabilities Application Vulnerabilities
Cyber War	Application Vulnerabilities Basic Protocol Vulnerabilities

Table 2: Threat categories versus vulnerabilities

2.4 Countermeasures

Most of the vulnerabilities can be patched by using simple technical preventive countermeasures. There will still be a considerable amount of risk after applying preventive countermeasures. Corrective countermeasures should be used in order to minimize the risk amount. Even if all of the preventive and corrective countermeasures are applied, there will be some minor residual risk. Hundred percent security is not possible in the real world. There is no technology and budget that eliminates the risk totally. The residual risks generally originate from the vulnerabilities of people and processes. The cyber espionage teams and spies usually use these vulnerabilities in order to steal information.

Countermeasures can also be divided into two main categories, which are technical countermeasures and non-technical countermeasures.

2.4.1 Technical Countermeasures

Patching the systems against vulnerabilities and implementing the latest technical security measures are the most prominent technical countermeasures. Security test and audits should be performed periodically. Active cyber security teams that are working for governments should gather cyber intelligence. Based on this cyber intelligence, predictions should be made and preventive actions should be taken. Also, research and development facilities should be supported by governments. The security for SCADA networks is a new and extremely important subject. Security must be a design issue for SCADA systems; it should not be an add-on. Certified software and hardware usage should be prioritized.[23] Both technical and policy based access control mechanisms should be used.[24]

2.4.2 Non-technical Countermeasures

There are two important non-technical countermeasures, which are awareness and cooperation. The most effective countermeasure for people vulnerabilities is security awareness. Security awareness is a vital countermeasure for not only computer users. Everyone whether computer user or not in an organization should be the target of security awareness programs.

Security is a matter of coordination, cooperation, collaboration and communication. In 2009, a Department of Homeland Security official said that hackers are better organized than governments.[25]

For all the types of threats that are stated in this paper, cooperation is a vital countermeasure. For

---

[23] Miller, "Trends in Process Control Systems Security", p. 58.
[24] Kilman, "Framework for SCADA Security Policy", p. 4.
[25] Packetstormsecurity, website at http://packetstormsecurity.org/news/view/16185/Testimony-Hackers-Better-Organized-Than-Government.html (accessed 13 June 2012)

all four threat categories, the possible cooperation instances are shown in Table-3. For a government, cooperation with critical infrastructure operators and owners is an essential and imperative countermeasure. Cooperation with Internet Service Providers (ISPs) and Computer Emergency Response Teams (CERTs) is a significant countermeasure against hacktivist attacks. Cooperation with police and law enforcement agencies is essential in order to combat cyber crime. Cooperation with CERTs and other countries are crucial in order to deal with cyber war. Cooperation with employees and cutting-edge technology makers is an indispensable countermeasure against cyber espionage.

THREAT TYPE	COOPERATION WITH ...
Hacktivism	Cooperation with ISPs Cooperation with CERTs Cooperation with infrastructure operators and owners
Cyber Crime	Cooperation with police Cooperation with law enforcement agencies Cooperation with infrastructure operators and owners
Cyber Espionage	Cooperation with employees Cooperation with technology developers Cooperation with infrastructure operators and owners
Cyber War	Cooperation with CERTs, ISPs International cooperation Cooperation with infrastructure operators and owners

Table 3: Threat categories versus sides of cooperation

2.4.3 Countermeasures - Final Remarks

Countermeasures are imperative in order to deal with cyber risks and to ensure an acceptable level of critical infrastructure protection. The application of all types of countermeasures should be considered as a life-cycle process. Once a countermeasure is applied, the effectiveness of the countermeasure should be measured continuously. The application and effectiveness of countermeasures should be monitored and improved as necessary. In Table-4, prominent countermeasures are listed for each threat category. Cooperation and technical countermeasures should be applied for all types of threats. Although security awareness is also applicable in order to deal with all threat types, it is especially important to counteract cyber espionage.

THREAT TYPE	COUNTERMEASURE
Hacktivism	Cooperation Technical Countermeasures
Cyber Crime	Cooperation Technical Countermeasures
Cyber Espionage	Cooperation Security Awareness Technical Countermeasures
Cyber War	Cooperation Technical Countermeasures

Table 4: Threat categories versus countermeasure types

3. Conclusion

Today, cyber systems serve as key infrastructures for critical sectors. Almost all sectors use information technologies for automating their core business processes. Automated business processes are connected to the Internet and corporate networks for optimization and decreasing

costs. Cyber systems of critical infrastructures are among the attractive targets of cyber threats. There are different types of threats with different motivations, qualifications and capacities. All of these threats exploit certain vulnerabilities of cyber systems of critical infrastructures. Therefore vulnerabilities have to be mitigated in order to cope with threats. There are different types of countermeasures in order to mitigate the vulnerabilities. The impact level and diversity of cyber threats will increase steadily in parallel with the widespread use of cyber systems. Therefore, critical infrastructure protection will be one of the most important agenda items of all governments in the near future.

References

Alcaraz-Tello, Cristina, et. al., "Secure Management of SCADA Networks" *The European Journal for the Informatics Professional* 9 (December 2008).

Beltran, Fernando, Fontenay, Alain, Alameida Marcio, “Internet as a Critical Infrastructure: Lessons from the Backbone Experience in South America”, *Communications & Strategies*. 58 (2005).

CNET, *available at* http://news.cnet.com/8301-1009_3-10104496-83.html (last visited 13 June 2012).

Department of Defense, "Strategy for Operating in Cyberspace" (July 2011).

IBM X-force, "2010 Trend and Risk Report" (March 2011).

Igure, Vinay, M., Laughter, Sean, A., Williams, Ronald, D., "Security Issues in SCADA Networks", *Computers & Security* 25 (2006).

Jayawickrama, Wipul, "Managing Critical Information Infrastructure Security Compliance: A Standard Based Approach Using ISO/IEC 17799 and 27001" *Book Chapter: On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops* (2006).

Kilman, Dominique, Stamp, Jason, "Framework for SCADA Security Policy", Albuquerque, Sandia National Laboratories (2005).

Kshetri, Nir, "Information and communications technologies, strategic asymmetry and national security" *Journal of International Management* 11 (2005).

Kshetri, Nir, "Patterns of Global Cyber War and Crime: A Conceptual Framework" *Journal of International Management* 11 (2005).

Lewis, James, A., "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats" *Center for Strategic & International Studies* (December 2002).

Mandiant, M Trends Report, "The Advanced Persistent Threat" (2010).

Miller, Ann, "Trends in Process Control Systems Security", *IEEE Security & Privacy* 3 (2005).

New York Times, *available at* http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all (last visited 13 June 2012)

New York Times, *available at* http://www.nytimes.com/2012/05/31/technology/researchers-link-flame-virus-to-stuxnet-and-duqu.html (last visited 13 June 2012)

Packetstormsecurity, *available at* http://packetstormsecurity.org/news/view/16185/Testimony-Hackers-Better-Organized-Than-Government.html (last visited 13 June 2012)

Presidential Executive Order 13010, Critical Infrastructure Protection, *available at* http://www.iwar.org.uk/cip/resources/eo/eo13010.pdf (last visited 13 June 2012)

Prichard, Janet, J., MacDonald, Laurie, E., "Cyber Terrorism: A Study of the Extent of Coverage in Computer Security Textbooks" *Journal of Information Technology Education* 3 (2004).

The Senate of United States, "The Draft Cyber Security Act of 2012", *available at* http://www.hsgac.senate.gov/download/the-cybersecurity-act-of-2012-s-2105 (last visited 13 June 2012)

Stouffer, Keith, Falco, Joe, Scarfone, Karen, "Guide to Industrial Control Systems (ICS) Security", National Institute of Standards and Technology, Special Publication 800-82 (June 2011).

US - China Economic and Security Review Commission, "2008 Report to Congress" (November 2008).

The White House, "Presidential Decision Directive/NSC-63", *available at* http://www.fas.org/irp/offdocs/pdd/pdd-63.htm (last visited 13 June 2012)

Wikipedia, "Duqu article" *available at* http://en.wikipedia.org/wiki/Duqu (last visited 13 June 2012)

Wired, *available at* http://www.wired.com/dangerroom/2008/11/army-bans-usb-d (last visited 13 June 2012)

Bibliography

Bilge KARABACAK received his B.S. degree from Bilkent University, in 1999 in Electronics

Engineering. He received his M.S. degree from Gebze Institute of Technology, in 2003 in Computer Engineering. He is currently pursuing his Ph.D. studies at the Middle East Technical University. He has been working as a chief researcher at the Scientific and Technological Research Council of Turkey since February 2000. He is a member of the OECD ICCP WPISP (Working Party on Information Security and Privacy) working group. Main topics of interest are information security risk analysis, information security standards, information security governance, cyber security, critical information infrastructure protection and computer forensics. He is the author of several journal and conference papers in the fields of information security risk analysis, cyber security, collaborative information security, critical information infrastructures protection and information security standards.

Ünal TATAR received his B.S. degree from Bilkent University, in 2004 in Computer Engineering. He received his M.S. degree from the Middle East Technical University, in 2009 in Cryptography. He is currently pursuing his Ph.D. studies at Yıldırım Beyazıt University-Management and Organizations Program. Mr. Tatar completed Information Technology Law Certification Training by the Ankara Bar Association. He has been working as a senior researcher at the Scientific and Technological Research Council of Turkey since October 2004. He is the coordinator of TR-CERT, The National Computer Emergency Response Team of Turkey. He is a member of The National Cyber Security Exercise Steering Committee. Main topics of interest are computer security incident handling, cyber defense exercises, IT security awareness trainings, information security risk analysis, and computer forensics. He is the author of several journal and conference papers in the field of information security.