İÇİNDEKİLER

Sıra	Yayın Tarihi	Yayın Adı	Başlık	Sayfa
46271478	01.01.2015	Defence Turkey	ICWC IKIRKEY 2014 WAS HELD İN ANKARA	5

Yayın Adı	: Defence Turkey	Yayın Tarihi	: 01.01.2015	Küpür Sayfa	: 48
Referans No	: 46271478	Etki	: Etkisiz	Tiraj	: 5000
Renk	: Renkli	STxCM	: 109,722222	Sayfa	: 48

ICWC Turkey 2014 was Held in Ankara

2nd International Cyber Warfare and Security Conference was held in Ankara on 27-28 November 2014 with the participation of members of governmental institutions and associations, military officials, representatives from universities and national and international companies. A total number of 453 local and foreign participants attended the conference held under the auspices of the Undersecretariat for Defence Industries (SSM) with support of the Ministry of Economy and organized by Defence and Aerospace Industry Manufacturers Association (SaSaD), ODTÜ Teknokent Defence Industry Cluster (TSSK) and Defence Turkey Magazine. On the first day of the conference, 4 panels were held in which a total of 18 presentations on various subjects were made. B2B meetings were conducted on the second day and 20 local and foreign companies attended these meetings.

In the plenary session, first Mr. Hüseyin Baysak, Secretary General of the Defence & Aerospace Industry Manufacturers Association (SaSad) took the floor. Stating that all armed forces worldwide have been exerting efforts to develop a doctrine against the cyber threats, Mr. Baysak added that the armed forces are in search of human resources that are qualified in struggling against the cyber threats and attacks.

Middle East Technical University (METU) President Prof. Ahmet Acar mentioned that they have been conducting studieson cyber security issues within the university. Prof.Acar stated that they launched the "Cyber Defence and Security Research Laboratory" in the second half of 2014 as METU Informatics Institute and Comodo Group company's joint venture and added that they have trained cyber emergency response teams from Afghanistan, Macedonia, Montenegro, Moldavia and Azerbaijan at the center so far.

© ICWC

Prof. İsmail Demir, Undersecretary for Defence Industries

Turkey Attaches Importance to Information Security and Cryptology

Undersecretary for Defence Industries Prof. İsmail Demir extended the opening remark of the seminar and expressed that cyber-attacks are becoming an important threat source in Turkey, as they are in the world. Emphasizing the inevitable need for information security, Prof. Demir underlined the need for technological developments in this scope. Prof. Demir qualified the information security and technology as areas that need to be underlined as critical issues. Pointing out the ever-increasing importance of the cyber threats Prof. Demir said, "Cyber-attacks are threatening the critical infrastructures worldwide and unfortunately systems fail to sufficiently protect themselves from such intensive cyber-attacks". Prof. Demir stated the need for a centralized structure for the efficient use of limited resources in cyber security in Turkey and added, "SSM assumed an important role within this scope. Our Undersecretariat attaches great importance to the information security and cryptology". Drawing the attention of the participants on the critical importance of these cyber-attackscan be compared to armed forces Prof. Demir said, "Occasionally these attacks are disguised and thus cannot be identified. The critical point is that these threats may become real and thus be mortally dangerous. SSM is open to all types of cooperation and participation in steps taken to this end". Remarking on the importance of the second of the annual Cyber Warfare and Security Conference, Prof. Demir expressed that this conference may be the opportunity for discussing the latest technological facilities and added that even though many commercial solutions are available in battling against cyber-attacks, no efficient solutions emerged yet.

© ICWC

METU President Prof. Ahmet Acar

In his part of the opening remark, Havelsan's General Manager Mr. Sadık Yamaç emphasized the rapid development of technology and said, "At this point, from shopping to transportation, from energy to agriculture everything is 'intelligent'. Technology penetrated into all aspects of life. It became indispensable". Mr. Yamaç stated that these developments in the cyber world paved the way to the emergence of cyber threats and

© ICWC

Mr. Sadık Yamaç, General Manager of Havelsan

added, "All our data is substantial. At this stage all data is registered and recorded. We are observing that all information including personal information and individual's privacy is exposed. This is the cyber world. Nobody knows what is going on. There is only a single way to raise awareness; the systems built should be open. The problem is solved when all structures become transparent". Mr. Yamaç mentioned that as the use of technology increases, the security of countries is threatened and added, "Standing out as a reliable company becomes greatly important in this respect. Unless the issue is handled in an integrated approach with all processes, software, hardware as well as the maintenance and sustainment services, no solutions to this issue will emerge. The only thing to do is to collaborate with reliable companies".

Taking the floor on behalf of Aselsan, Vice General Manager of Communications and Information Technologies Mr. Yavuz Bayız stated that Aselsan has been after creating new generation intelligent and integrated cyber solutions and that they have established an Information Technologies and Cyber Security Group at Aselsan. Mr. Bayız remarked that as Aselsan, they have 25 years of experience in communications and information security and that they exported products related to these areas to more than 10 countries in the previous years. Mr. Bayız added that as the company, they are ready to offer all defence industry institutions the solutions they may need domestically as well as internationally in cyber security issues.

Dr. Kenneth Geers, Senior Global Threat Analyst-NATO CDDCOE Ambassador

TÜBİTAK Informatics and Information Security Research Center (BILGEM) President Mr. Arif Ergin expressed that "the individual" is the most prominent factor in cyber security area and said, "We must split up our human resources based on their type of usage. Driving forces of various elements shall be identified and directed collaboratively".

Cyber Threats are Shaping the World

Invited as the Keynote Speaker to the Conference, Dr. Kenneth Geers, Ambassador at the NATO Cooperative Cyber Defence Center of Excellence, initiated his speech with mentioning the results of the cyber-attacks and threats that emerged during 2014. In his presentation, Dr. Geers particularly pointed out the importance of the systematic attacks that could not be recognized for a long while and were initiated in order to hamper Iran's nuclear program and continued, "The cyber warfare started a long time ago, and if you wait for the crisis to emerge in order produce solutions you may be too late. The governments have to adopt their measures immediately; they should not wait until the crisis. Dr. Geers mentioned that the cyber area started altering warfare, crime and espionage concepts rapidly and said the changing balances in the world are seen in cyber area as well and added that the ever-increasing conflicts in the cyber area would be shaping the nations' comprehensive security policies too. Stating that cyber-attacks became international threats in our day and therefore the solutions should be discussed in international platforms, Dr. Kenneth Geers also expressed that the most important plan against the cyber-attacks was the creation of an alternative plan.

UK Allocates £860 mln for the "National Cyber Security" Program in the Next 5 years

A session on "Strategy and Doctrine for Cyberspace" was held at the first panel of the day with SSM Head of Communications, Electronics and Information Systems Department Mr. Süreyya Yiğit acting as the moderator. First speaker of the panel, Ms. Caley Robertson, Cyber Security Exports Advisor - Critical Infrastructure at UK Trade and Investment Defence and Security Organization, made a presentation on "International Cyber Security Strategies and Critical Infrastructure Security Measures". Ms. Robertson informed the participants on the Cyber Defence Strategies adopted by the United Kingdom (UK) and how this defence strategy is established through selecting the relevant

Mr. Yavuz Bayız-Deputy General Manager, Aselsan

institution and/or association. Stating that the United Kingdom invested greatly to Cyber Security in the last 5 years, Ms. Robertson underlined that as a result of these investments the United Kingdom is regarded as one of the most prominent cyber defence forces in the world against cyber threats. Ms. Robertson emphasized on the 22 % growth in the Cyber Industry in United Kingdom in 2013 and added that the United Kingdom shall be investing an additional amount of 860 million pounds in the next five years within the scope of "The National Security Program" that would cover all institutions and associations. Stating that 11 excellence centers conducting researches on Cyber Security exist in United Kingdom Universities, Ms. Robertson mentioned the sensitivity of the cyber security issue and strongly emphasized the importance of following a common path in this respect and underlined the need for establishing partnerships between countries.

Taking the floor after Ms. Robertson, the panelist Brig. Gen. R. Krzysztof Bondaryk, Minister's Plenipotentiary for Cyber Security in Poland MoD, Director of National Centre of Cryptology, made a presentation on "Cyber Defence in the Polish Ministry of Defence". Bondaryk extended information to the participants on the organization and operational structure of the Cyber Defence in the Polish Ministry of Defence. Commenting on the importance attached to Cyber Security by Poland in recent years, Bondaryk stated that they established a substantial infrastructure in both national and international scales on cyber security issue within the scope of the regulations and laws prepared and put into effect particularly in the years 2011-2014.

Mr. Antti Sillanpaa, Senior Researcher at the Secretariat of the Security Committee at Finland Ministry of Defence, made a presentation on "Finland's Cyber Security Strategy and its Implementation". Mr. Sillanpaa stated that the growing economies, rapidly increasing population, global terrorism, technology, climate changes, natural resources, non-governmental actors and changes in many parameters lied beneath the increase in cyber threats. Mr. Sillanpaa underlined the need to identify initially an organizational chart, as well as the tasks and threats, pointed out the importance they attach to this issue by mentioning their comprehensive approach, added that Finland is prepared for any kinds of cyber threats.

Commander Namık Kaplan at Plan Project Coordination Branch Head at Cyber Defence Command, Turkish Armed Forces

Turkey Identified the Road Map against Cyber Threats

Commander Namık Kaplan at Plan Project Coordination Branch Head at Cyber Defence Command, Turkish Armed Forces mentioned that Cyber Defence is the number one issue at at this time and added that in addition to air, land, space and sea warfare, cyber warfare now exists as "cyber space". Kaplan stated that the worldwide attacks are becoming more and more severe each day and expressed that they formed cyber warfare units with all service commands and governmental institutions and associations under the coordination of Turkish Armed Forces in order to respond to these attacks and threats. Kaplan said, "Turkish Armed Forces attaches great importance to cyber-attacks and threats. The quicker one responds to a cyber-attack, the less damage shall emerge". Underlining the need for the coordination between all the governmental institutions and associations in the country to this end, Kaplan emphasized on the essence of participation in the national and international operations to be conducted and added that Turkey attended the "Cyber Coalition Exercise" held on 17-21 November 2014 with the participation of Turkish Armed Forces, Ministry of Foreign Affairs, Ministry of Transport, Maritime Affairs and Communications, TÜBİTAK and National Cyber Emergency Response Center.

"Active Cyber Defence"

At the "Active Cyber Defence" session moderated by METU Informatics Institute Director Prof. Nazife Baykal, current cyber threats, trainings on cyber threats in the upcoming term and cyber defence issues were discussed in detail.

The first speaker of the session Mr. StéphaneTaillat made a presentation titled "Cyber Defence: A French View of Cyber Warfare". Mr. Taillat started his presentation by drawing the audiences' attention to the history of Cyber Defence and spoke of the steps France has been taking from past todate, the stages the country has been through and of its current

Founder and head researcher of the SignalSEC Company, Mr. Celil Ünüver

status. Mr. Taillat, conveyed to the audience the ways of accomplishing cyber security through public and private companies' joint efforts.

Founder and head researcher of the SignalSEC Company, Mr. Celil Ünüver emphasized the zero-day concept in his presentation. Mr. Ünüver said, "In order to make my living, I detect the gaps in major applications (zero-day), conduct researches on these and sell the results to such companies". Mr. Ünüverstated that the cyber-attacks should be inspected in two stages and added, "First group of these attacks are composed of those with the aim of making money. Others are more systematic and organized; these ones target countries, governments and economy". Mr. Ünüver mentioned that the greatest fear of the companies and governments is the "zero-day" and stressed that it is not ethical to directly sell information detected through the zero-day to governments.

Mr. Fatih Karayumak, Researcher at TÜBİTAK BİLGEM Cyber Security Institute, stated during his presentation on "Training the Future Cyber Security Specialist: A Novel Approach" that in order to achieve a better level of protection against the hacker attacks, the institutions shouldhave a better understanding of their own systems. Mr. Karayumak underlined the fact that defending is harder than attacking and added that technical information alone is not sufficient to resist against cyber-attacks. Karayumak claimed that technology, monitoring and policy have to function jointly with the human factor in a compatible manner for achieving an effective cyber defence. Mr. Karayumak mentioned that Turkey needs to produce the know-how as a counter-measure against cyber-attacks and added that they accomplished security tests with 26 governmental entities in the last 4 years in Turkey to this end. Mr. Karayumak said that in this respect, they conducted Penetration Tests in BDDK (Banking Regulation and Supervision Agency), 38 banks (which are international subsidiary banks), GSM companies and Reassurance Companies in 2011. He concluded that they have trained 610 personnel from 55 governmental entities in 15 various courses on this subject up to date.

Mr. Jonathan W. Hoyle, Vice President Europe and Americas, Lockheed Martin

"Government, Academia and Industry Cooperation on Cyber Security"

On the "Government, Academia and Industry Cooperation on Cyber Security" panel led by Mr. Paolo Venturoni, Vice Chairman of European Organization for Security, cooperation between academia, state and industryand cyber policies of these institutions were discussed.

Qualified Human Resources against Cyber Threats

One of the speakers of the panel on "Qualified Human Resources against Cyber Threats", Mr. Jonathan W. Hoyle, Vice President Europe and Americas, Lockheed Martin, extended information to the audience on Lockheed Martin's stance on cyber security, the programs executed and future plans. In his presentation, Mr. Hoyle stated that each day, a new cyber threat emerges and stressed that in order to struggle against these attacks the industry, government and academies need to collaborate. Mr. Hoyle also referred to the importance of information exchange by governmental entities and mentioning the requirement for trained and qualified labor in this regard, he concluded that the trainings and efforts for raising awareness are the only measures to resist against such threats.

METU Informatics Institute Director Prof. Nazife Baykal

Dimensions of an Ideal Effective Cooperation

METU Informatics Institute Director Prof. Nazife Baykal delivered aneloquent presentation to the audience on the importance of cooperation in Cyber Security issues. Answering questions such as "What is cooperation? How do we cooperate? How to achieve trust while collaborating? What are the advantages of cooperation?", Ms. Baykal stated that as of now, many types of cooperation are conducted piecemeal and therefore it was getting hard to see the big picture. Stating that in order to achieve efficient cooperation, all the parties would have to compromise and added that a multi-dimensional approach is necessary to create ideal cooperation and in this respect, government, academia, industry and citizen need to be in harmony with one another regarding trust, cost-sharing, risk-sharing and obligations. Baykal claimed that the "risk" factor is essential for success and continued, "All parties need to prepare themselvesfor failures in the short run on risk-sharing and to certain infringements. Moreover all the actors must be ready for their parts in financial obligations (research and development Project) in cost -sharing".

In her presentation, Ms. Emine Yazıcı Altıntaş, Head of Cyber Security Department, Republic of Turkey Ministry of Transport, Maritime Affairs and Communications informed the audience on the Cyber Security studies conducted in Turkey. Ms. Altıntaş declared that the Cyber Security studies in Turkey are launched with a decree of the Council of Ministers adopted in 2012 and added that through gaining legal grounds, these studies started to become more important since 2014. Ms. Altıntaş mentioned that the Cyber Security Council formed in February 2014 adopted major decisions in that year and pointed to the article on the "Establishment of an Action Plan" within this scope. Ms. Altıntaş said that the objective of the Action Plan is to provide the security of the institutions and associations' systems that produce data or service or store such data, enabling the security of the information systems of the critical infrastructures operated by public or private entities, stabilizing the level of the impacts of Cyber Security incidents at the lowest level and identifying the measures that would allow the systems resuming their operations rapidly after attacks. Altıntaş also expressed that in universities human resources training and activities for increasing awareness are being initiated.

© ICWC

Delivering a presentation on "A Conceptual Model for Government, Academia and Industry Cooperation on Cyber Security" on behalf of STM, Mr. Emre Barış Aksu, IT Solutions Group Manager searched for an answer on what the responsibilities of the institutions should be in the cooperation between academia, Industry and Government. Mr. Aksu stated that instead of short-term solutions, the Government needs to determine an action plan and identify responsibilities among institutions through creating the required fund and by adopting a long-term strategy for 5-10 years. Stating that too many responsibilities fall onto the industry in this cooperation, Mr. Aksu emphasized that the industry needs primarily to build a strategy and create a road map in R&D and product development with qualified labor, budget and efficient organizational structure. Mr. Aksu added that academiawould have many obligations in this cooperation and commented that academiashould be establishing their own cyber research strategies. Lastly, Aksumentioned that through creating know-how by achieving proper strategies, curriculum, specialized researchers, laboratory, infrastructural support and required budget,academia needs to become centers of excellence.

Nearly 70 military and defence officials from Governmental institutions, Prime Ministry, General Staff, National Defence Ministry, Transportation, Maritime Affairs and Communications Ministry, Economy Ministry, the Undersecretariat for Defence Industries and General Directorate of Security attended the 2nd International Cyber Warfare and Security Conference that lasted for two days. Military attaches and senior officials from foreign embassies showed great interest in the conference and diplomatic representatives from Malaysia, Poland, Tunisia, South Korea, Indonesia, Kuwait, Greece, Finland, Germany, Canada, United States of America, Russia, France, Australia, Iran and South Africa attended the event. The faculty members and researchers of METU, Bilkent University, Gazi University and TED University were amongst the participants of the conference as well.

Aselsan, Havelsan, STM, TÜBİTAK, Bilgem, MilSOFT, Biznet, CTECH, Labris, Oran Teknoloji, ATOS from Turkey were the local sponsors of the conference while Lockheed Martin, Selex ES, Thales, Thales Raytheon, Codenomicon, Honeywell and IBM companies supported the event as foreign sponsors. The International Cyber Warfare and Security Conference, growing stronger each year with the participation and support of the Transportation, Maritime Affairs and Communications Ministry, Economy Ministry, the Undersecretariat for Defence Industries, TÜBİTAK and Middle East Technical University, national and international companies and institutions, is expected to have a richer content with various workshops, demos in addition to the existing panels and greater international participation in 2015.

© ICWC