BİLGİ GÜVENLİĞİ
DERNEĞİ

17th International Conference on Information Security and Cryptology

isc
TÜRKİYE2024

ISCTURKIYE 2024
CONFERENCE PROGRESS REPORT

OCTOBER 23, 2024

ISCTURKIYE 2024
CONFERENCE PROGRESS REPORT

ISCTURKIYE 2024
CONFERENCE PROGRESS REPORT

The 17th International Conference on Information Security and Cryptology-ISC Turkiye 2024, with the main theme of ‘Cyber Resilience and Sovereignty’, was held on 16-17 October 2024 at the Presidency of the Republic of Turkey, National Library. Organized by the Information Security Association, the International Conference on Information Security and Cryptology is held under the auspices of the Digital Transformation Office of the Presidency of the Republic of Turkey; with the cooperation of Gazi University, Istanbul Technical University, Middle East Technical University, TOBB University of Economics and Technology, and supported by the Ministry of Transport and Infrastructure, Ministry of Industry and Technology, Presidency of Defense Industries, Information Technologies and Communication Authority, IEEE Türkiye, and the European Network and Cybersecurity Agency-ENISA.

The conference was attended by more than 1500 people, including the President of the Council of Elderly People of the Turkic Council and the last Prime Minister, Mr. Binali YILDIRIM, Minister of Transport and Infrastructure, Mr. Abdulkadir URALOĞLU, President of the Digital Transformation Office of the Presidency, Mr. Yusuf TANCAN, President of the Middle East Technical University, Prof. Dr. Ahmet YOZGATLIGİL, President of TOBB ETÜ, Prof. Dr. Yusuf SARINAY, general managers from public institutions, department heads, academicians, cyber security and IT experts, and more than 1200 people registered online and attended.

The conference started with a moment of silence for our martyrs and the reading of our national anthem in the main hall of the Millet Library. Following the opening speech of BGD Board Chairman Prof. Dr. Mustafa ALKAN, the speech of Conference Academic President Assoc. Prof. Dr. Oğuz YAYLA, the speeches of TOBB ETÜ Rector Prof. Dr. Yusuf SARINAY and Middle East Technical University Rector Prof. Dr. Ahmet YOZGATLIGİL, the President of the Presidency's Digital Transformation Office Yusuf TANCAN made his speech and then the Minister of Transport and Infrastructure Mr. Abdulkadir URALOĞLU and finally the President of the Turkic Council Elderly People's Council and the last Prime Minister of the 27th Term of the Republic of Turkey Mr. Binali YILDIRIM made his speech.

Immediately, after the opening speeches,

- **Mr. Binali YILDIRIM,**
- **Ministry of Transport and Infrastructure, Communications General Directorate**
- **National Cyber Incidents Response Center**
- **METU Applied Mathematics Institute Cryptography Program**
- **Dr. Ali Taha KOÇ**
- **İhlas News Agency**
- **Picus Security**
- **Cyber Anatolian Communities**

"BGD Cyber Security Outstanding Service Awards" were given in 8 categories.

Information Security Association "**CYBER SECURITY OUTSTANDING SERVICE AWARDS**" are determined by the BGD Board of Directors based on certain criteria and are given every year. These basic criteria are as follows;

- Technical and Scientific Contributions and Innovation
- Education, Awareness and Awareness Activities
- Ideas, Infrastructure, Organization, Products and Services for Cyber Homeland Defense
- Contributions to the Creation and Development of the Cyber Security Ecosystem
- Professional Career and Leadership and Training of Qualified Experts
- Detection and Elimination of Security Vulnerabilities, Risks and Threats
- Contributions to Legal Regulations and National Strategy and Action Plan
- Ethics and Social Responsibility
- Creating and Disseminating a Culture of Cooperation and Sharing
- National and International Awards, Standards, Certification and Compliance

Awards, are given in 6 categories: individual, institution, sector, university, media and special awards. Awards and their reasons are given below.

- **Mr. Binali YILDIRIM;** The Chairman of the Council of Elders of the Turkic Council, our last Prime Minister, Speaker of the Parliament, Minister and

Member of Parliament, for his significant contributions to the development of information security and defense of the country, for supporting our draft proposal for the national cyber security strategy and action plan that we prepared as the Information Security Association and initiating the first national cyber security strategy and action plan studies under the leadership of the UAB, for carrying out the Implementation, Management and Coordination of National Cyber Security Studies on behalf of the Council of Ministers, for personally participating in and supporting national and international events such as the information security and cryptology conference organized by the information security association and for constantly encouraging us in our studies and most importantly for his contributions to raising information security awareness in both the public and institutions, establishing security infrastructures and ensuring the security of our cyber homeland, our deputy, minister and prime minister Mr. Binali YILDIRIM was awarded the “Information Security Association Cyber Security Outstanding Service Award”.

- **Ministry of Transport and Infrastructure, Communications General Directorate;** The “Information Security Association Cyber Security Outstanding Service Award” was given to the General Directorate of Communications of the Ministry of Transport and Infrastructure for its contributions to the preparation, publication and coordination of the first National Cyber Security Strategy and Action Plans in our country, the monitoring of national plans and activities, and the updating and publication of the strategy and action plan that sets forth our country's vision in the field of cyber security for the years 2024-2028.
- **The National Cyber Incidents Response Center;** is a unit established within BTK within the scope of the cyber security strategy and action plan in our country, its very important contributions to the cyber security and defense of our country to date, its development of many local and national solutions such as AVCI, AZAD, KASIRGA, ATMACA, SINKHOLE, KULE, SOME Communication Portal, its establishment and management of SOME infrastructures, and its contributions to the elimination of national cyber security risks, the National Cyber Incidents Response Center, or USOM, was awarded the "Information Security Association Cyber Security Outstanding Service Award".
- **METU Applied Mathematics Institute Cryptography Program;** for the development of cryptology science in our country, training hundreds of qualified experts and undertaking advanced studies, pioneering the establishment of cryptographic test modules and system security laboratories, being the program that has the most theses written in the field of cryptology, contributing to the increase in the country's knowledge in the field of cryptology with the events it organizes, transferring academic knowledge to the sector and institutions, and most importantly being the

supporter and eponym of the cryptology section of this conference since the first day, the METU Applied Mathematics Institute Cryptography Program was awarded the "Information Security Association Cyber Security Outstanding Service Award".

- **Dr. Ali Taha KOÇ;** was awarded the “Information Security Association Cyber Security Outstanding Service Award” for his contributions to the establishment of the cyber security department within the Presidency of Digital Transformation Office, updating the country’s cyber security strategy and action plan, preparation and publication of the Information and Communication Security Audit Guide, conducting the activities of the Turkey Cyber Security Cluster Platform together with the Presidency of Defense Industries, pioneering the establishment of cyber security high schools, supporting scientific studies in the field of security and cryptology, and most importantly, increasing the interest of young people in cyber security.
- **IHLAS NEWS AGENCY;** The Ihlas News Agency was awarded the “Information Security Association Cyber Security Outstanding Service Award” for providing news that informs the society in the field of information security and cryptology in our country, contributing to raising the awareness of the society in the field of information security, and especially including the opinions of information security experts in its news.
- **PICUS SECURITY;** Picus Security was awarded the “Information Security Association Cyber Security Outstanding Service Award” for offering the first and only Offensive Security Verification solution that brings together Automatic Penetration Testing, Cyber Breach and Attack Simulation and Intrusion Detection Rule Verification capabilities on the same platform, for its pioneering contributions to the development of cyber security in our country, for the products it has developed, for its successes at home and abroad, for having its products in the DMO catalog, for having more than 500 corporate customers in more than 50 countries worldwide, and for having recently received an investment of 80 million dollars and having a worldwide success story.
- **CYBER ANATOLIAN COMMUNITIES;** Cyber Anatolian Communities were given the "Information Security Association Cyber Security Outstanding Service Award" for increasing the interest of university youth in cyber security, bringing together many cyber security student communities at universities under one roof, cooperating and joining forces, transforming cyber security awareness into behavior and spreading it among students, the training they provided, the competitions they organized, and most importantly, increasing the interest of young people in the field of cyber security.

After the award ceremony, plaques were given to 19 companies that supported the Conference as Platinum, Gold, Silver, Collar and Stand Sponsors by Mr. YILDIRIM and Mr. URALOĞLU.

Videos of the opening speeches and the Awards Ceremony can be accessed here.

After the tea and coffee break, the session titled "Cyber Resilience in Communication" started, in which Türksat General Manager Ahmet Hamdi ATALAY, Turkcell Network Technologies Deputy General Manager Prof. Dr. Vehbi Çağrı GÜNGÖR, Türk Telekom Deputy General Manager Ali TAŞKIN, Vodafone Turkey Executive Vice President Özlem KESTİOĞLU made their speeches.

Later, the first session of "Cyber Resilience and Maturity" was held, in which the President of the National Intelligence Academy Prof. Dr. Talha KÖSE, UAB Communication Deputy General Manager Onur GENÇER, ASELSAN Deputy General Manager Mustafa YAMAN, STM Cyber Security and Information Systems Director Bülent ARSAL, Vodafone Turkey Corporate Technology Solutions Director Burcu ALTINTAŞ made their speeches.

After the lunch break, the second session of "Cyber Resilience and Maturity" was held, in which Ankara Development Agency Secretary General Av. Dr. Duhan KALKAN, Huawei Turkey Cyber Security and Privacy Officer Boran DEMİRCİLER, Kıta Bilişim Area Advisor E. Brig. Halil İbrahim BÜYÜKBAŞ, Havelsan Cyber Security Director Salih TALAY made their speeches.

Afterwards, Bilkent University faculty member Prof. Dr. Serdar KOZAT, as the Invited Speaker/Keynote Speaker, gave his speech titled "Big Step from LLM to Artificial General Intelligence with Big Language Models".

In the session titled "Cyber Security and Authentication in Digital Services", Ministry of Treasury and Finance, General Manager of Information Technologies Dr. Mert ÖZARAR, MEB Innovation and Education Technologies General Manager Mustafa CANLI, Türksat Cyber Security Management Director Mehmet Ali ERKUL, BiOnay Deputy General Manager Nusret Atilla BILER made their speeches.

On the second day of the conference, 17 articles were presented by academics in 4 different sessions, namely "Cyber Security and Threat Detection", "System Security and Design", "Cryptography", "Machine Learning and Artificial Intelligence Applications".

In parallel with the academic sessions; Student Projects Presentation Session was held under the presidency of BGD Young President Oğuzhan ALKAN.

In the session;

- Blockchain Based Academic Article Publishing Platform
- Artificial Intelligence Supported Blockchain Intelligence Tool
- Developing Intelligent Cyber Security Solutions for Smart Grids: Artificial Intelligence Supported Attack Detection System Development
- Threat Intelligence and Defense with Artificial Intelligence
- Increasing Cyber Security Awareness with Large Language Models
- The projects titled were presented by students and project advisors from 10 different universities.

After the project presentations, the “BGD YOUTH SESSION” was held under the presidency of BGD Youth President Oğuzhan ALKAN, in which Cyber Anatolian Communities and METU Cyber Security Community President Şakir ŞİMŞEK, TED University Cyber Security Community President Fatih PURTAŞ, Gazi University Cyber Security Community President Elif Nur MERCAN, Gazi University Cyber Security Research and Development Community President Tolga DEMİREL, TOBB ETÜ Cyber Security Community President Alperen Tolga KARAÇAM, Ankara Yıldırım Beyazıt University Cyber Security Community President Bilge KELEŞ made their speeches and shared their activities, projects and future goals with the participants.

Finally, in the “Education Session”, USOM Security Tests Team Leader Hacı Özdemir gave training titled “USOM National Activities” and Havelsan Cyber Security Expert Ata Seren gave training titled “Artificial Intelligence in Cyber Security”.

The conference was hosted by Prof. Dr. The meeting ended with the closing and evaluation speeches of , Prof. Dr. Şeref SAĞIROĞLU, Prof. Dr. Oğuz YAYLA, Prof. Dr. Ali Aydın SELÇUK, Secretary General Oğuz YILMAZ on behalf of the Information Security Association, and Chairman of the Board of Directors Prof. Dr. Mustafa ALKAN.

CONFERENCE CONCLUDING DECLARATION

Cyber resilience and sovereignty are concepts that are critical to the security of a country's digital infrastructure, the protection of its economy, and the sustainability of its digital future. While cyber resilience refers to a system's ability to protect, recover, and maintain itself against cyber attacks and threats, cyber sovereignty indicates how advanced and sustainable these processes are. In this context, studies and recommendations that can be made when considering the cyber security of countries are listed below:

1. Although it is evaluated that the importance is given to the issue of “Cyber Resilience and Sovereignty” in our country, that our strategic goals and objectives are determined based on the themes of “human”, “defense”, “deterrence” and “cooperation” in the National Cyber Security Strategy and Action Plan prepared by the Ministry of Transport and Infrastructure covering the years 2024-2028, and that it will contribute to this goal, that it includes 6 strategic goals, 18 targets and 61 action items, and that it is important to focus on Cyber Resilience, Proactive Cyber Defense and Deterrence, Human-Centric Cyber Security Approach, Safe Use of Technology and Its Contribution to Cyber Security, Domestic and National Technologies in Combating Cyber Threats, and that it will contribute to the achievement of the targeted outputs, it is known that the contribution of previous strategies to national cyber security could not be measured well, could not be audited or the assigned tasks were not fully performed. Since the auditing of the tasks assigned in the action plans and the continuity of the audit-based cyber security approach are important, special importance should be given to this issue.
2. Within the scope of proactive cyber defense and deterrence studies, necessary measures should be taken to increase the competence levels of cyber incident response teams, to develop and increase capabilities for the detection and notification of cyber risks and threats, and to obtain and share cyber threat intelligence.
3. By adopting a human-centered cyber security approach, importance should be given to awareness-raising activities and the competencies of professionals working in this field should be increased. Higher-level measures should be taken to strengthen our country's human resources and increase competence with a human-centered cyber security approach.
4. By determining measures with the "zero trust" approach, it is necessary to ensure a secure cyber environment and digital transformation, to evaluate, determine and implement the requirements and minimum security criteria for the security of new technologies.
5. In the field of cyber security, necessary steps should be taken to support innovative ideas and R&D activities in the development of domestic and national cyber security technologies, to open cyber security technoparks, and to further expand the use of domestic products.
6. Countries should create a holistic cybersecurity strategy and keep it up to date. The strategy should include both public and private sector collaborations. In addition, there should be an emergency plan and crisis management procedure that can be used for rapid intervention in times of crisis.
7. Cybersecurity approaches based on regulations and inspections carried

out through these regulations should be adopted more in determining and implementing cybersecurity measures in critical infrastructure sectors such as defense, communications, energy, finance, and health.

8. Considering that the work carried out before, during and after a cyber incident is as important as the work carried out during and after the incident, the work carried out with a proactive cyber defense approach in terms of taking measures to prevent risks and threats before they occur or at early stages will increase cyber resilience. One of the essential points for ensuring and increasing cyber resilience is to give more importance to risk-based analysis approaches at sectoral, institutional and national levels, which are designed on mechanisms where security risks are determined, evaluated, risk reduction efforts are carried out and monitored.
9. Zero trust architectures should be widespread. Zero trust means that each access request requires authentication and increases cyber resilience. This structure will minimize cyber attack risks and contribute to the proactive monitoring of security vulnerabilities.
10. Automatic intervention systems supported by artificial intelligence and machine learning should be developed. Since these systems will respond quickly to attacks, detect and prevent threats without requiring human intervention, and prevent critical infrastructures from collapsing, infrastructures should be established and operated in these areas.
11. Cybersecurity Maturity Models (e.g. CMMI - Cybersecurity Maturity Model) must be used to increase cybersecurity maturity. Special importance should be given to these models as they enable organizations to analyze their current security status and identify areas for improvement.
12. Cyber threat intelligence is one of the fundamental elements of increasing cybersecurity maturity. Collaborations should be developed at both local and international levels for threat intelligence sharing, and real-time information exchange should be carried out on cyber threats. In particular, companies within the Cyber Cluster should come together on a common platform and do this as in world examples.
13. National capacity and capabilities for the detection of cybersecurity vulnerabilities, notification to relevant parties, and sharing of up-to-date cyber threat intelligence should be increased, and more work should be done to early detect and prevent elements that threaten national cybersecurity with artificial intelligence and big data infrastructures, infrastructures should be established, new programs should be opened, and open ones should be supported.
14. In terms of protection from cyber threats, more comprehensive studies should be carried out on the creation of local and national product projects and the development of certification and accreditation

mechanisms with the principle of “security-by-design”.

15. Artificial intelligence-supported fraud detection systems should be developed and disseminated to prevent DeepFake, fake news, deception and fraud.
16. As cyber threats gain international dimension, countries should participate more in global cooperation for cyber security, benefit from directives such as European Union NIS2 and NATO’s cyber defense initiatives, and new regulations and standards should definitely be used in relevant areas.
17. Countries are developing comprehensive data privacy laws to protect digital privacy. In our country, in a period when artificial intelligence is rapidly developing, work should be done on artificial intelligence security issues, new solutions should be developed and, if necessary, enacted.
18. In order to protect digital privacy, investments should be made in advanced encryption technologies such as post-quantum encryption, infrastructures should be established, and existing laboratories should be supported. The emergence of quantum computers threatens existing cryptographic methods. Therefore, research in the field of post-quantum cryptography should be accelerated and existing infrastructures should be made compatible with this new technology.
19. With the rapid spread of 5G and/or 6G networks and internet of things devices, the security of these technologies is gaining great importance. The security of 5G networks should be ensured, and strong authentication methods should be used when connecting IoT devices to each other.
20. Explainable artificial intelligence technologies should be developed to increase the reliability and transparency of artificial intelligence systems. In this way, decisions taken by artificial intelligence systems can be better understood, errors can be detected more easily, and more durable systems can be developed.
21. Since the importance of cyberspace in the new world foreign policy will increase even more, the cyber dimension of international relations should be addressed, and units for cyber foreign policies should be established. A cyber “CYBER HOMELAND” unit should definitely be implemented within the Ministry of Foreign Affairs, which will manage our foreign policy on cyberspace and digital technologies and aim to resolve potential cyber crises through diplomacy. This unit can be called the “Ministry of Foreign Affairs Cyberspace and Policy Bureau”, which focuses on developing Turkey’s leadership in determining global cyber standards. It can be divided into two structural units, namely International Cyberspace Security and International Information Policy, and carry out its work. In fact, this structure can be organized together with the Turkish states; a Cyber Treaty Organization can be established,

and both an offensive and defensive institution can be created in the cyber field. In general, cybersecurity policies in the international arena are focused on defense. However, offensive capabilities should now also be included in policies. The card of resorting to offensive methods in ensuring national cybersecurity should be put on the table. It is obvious that Turkey needs a new model in this area. This model should include the following;

- A “Cyberspace Defense Force” should be established.
- A communication battalion should be structured as an offensive cyber force and the main objectives of this structure should be; Operation, Defense, Attack, Infiltration.
- A secret Army called “Science Cavalry” should be established consisting of professional programmers and coders, whose identities are hidden, who are constantly at the keyboard, who can operate in many areas, and who can serve in hot zones and cyber wars. This Army should develop and use technologies that enable automatic processing of data using big data analytics to obtain real-time cyber intelligence.
- A “Cyber Security Ministry” should be established.
- A “Cyber Embassy” should be established within the Ministry of Foreign Affairs. There should be a unit that will work to solve cyber crises through diplomacy and operate diplomacy in protecting the cyber homeland.
- By amending the intelligence law; all banking movements of individuals and companies suspected of financing terrorism, espionage or violent extremism should be monitored and precautions should be taken.
- A Psychological Defense Unit should be established to identify, analyze, prevent and respond to the inappropriate effects of misleading information.
- Cybersecurity should be accepted as an important component of economic security as well as National Cybersecurity, and measures should be taken.

22. The “Cyber Homeland” phenomenon, which is accepted in our country and increases our awareness, should be expanded, and our country should take the lead in developing the “Turkish World Cyber Homeland” phenomenon.

23. The rapid development of quantum technologies is one of the areas of concern in the world. We are on the verge of a period in which global cyber security agreements will be made with international cooperation and joint efforts will intensify to increase quantum security. The fact that quantum key distribution will become the standard method in financial transactions and high-

security data transmissions should not be ignored. Since a cyber security ecosystem resistant to quantum threats will be established, it is necessary to be prepared for this period. We call for increasing national and international cooperation, adapting existing cryptographic systems to the post-quantum world and accelerating research and development studies in order to ensure the security of critical infrastructures.

24. Focusing on cyber resilience, cyber security, digital sovereignty and artificial intelligence applications, this conference focused on the steps taken by Turkey in these areas, as well as globally prominent cyber security applications and the magnitude of the risks to be encountered in the future, and considering these, large language models for national security should be developed and put into use. In particular, large language models and general artificial intelligence applications specific to our country and language should be developed and put into use.

25. Reducing external dependency with domestic national products with international certifications and increasing security measures against cyber attacks with artificial intelligence support are of great importance. However, since ensuring the sustainability of domestic and national products is very important for the development of these products, these areas should be supported specifically.

26. Key exchange standards offered for post-quantum cryptography have reached a certain maturity and have begun to be used in daily applications. However, active studies should continue in order for quantum computer-resistant signing algorithms to provide the targeted security and performance. Even if the post-quantum algorithms with the targeted features become standard one day, discussions and research should be conducted on how these algorithms can be used in protocols such as TLS and DNSsec for cybersecurity. Although it is not expected that a large-scale quantum computer will be built in the near future and will break existing asymmetric cryptography algorithms, encrypted conversations recorded today will be able to be listened to decades later thanks to the invention of such a quantum computer. Therefore, as some countries aim, Turkey should also aim to transition to post-quantum cryptographic algorithms in 2030-2040, and focus on issues such as developing appropriate infrastructures, test centers, software, and hardware.

It is respectfully announced to the public.

Information Security Association
ISCTurkiye 2024 Organizing Committee