ISTANBUL CYBER-SECURITY FORUM

ISTANBUL DECLARATION (DRAFT)

Istanbul Cyber-Security Forum whose main theme "Post-Security, Digital Revolution, Circular Economy, and Cyber Ecosystem" was held by TASAM National Defence and Security Institute, together with the 8th Istanbul Security Conference on the date of **03 November 2022** in **Ramada Hotel & Suites by Wyndham Istanbul Merter**, simultaneously as a sub-event.

Speakers and protocols from various countries and regions, and from different fields and sectors, have participated in the Forum. Diplomatic representatives and delegations from different countries have also taken part. In the Forum, speeches and presentations were made by local/foreign experts, academics and diplomats. Relevant authorities from Türkiye, Asia, Europe, America and Africa were also represented at the Forum, and all sessions were followed institutionally.

The following issues of vital importance in present and future of Türkiye, the region and the world were discussed at the Forum; "Cyber-Security in the MENA (Middle East and North Africa) and Other Regions", "Standards and Norms in Cyber-Security", "Industrial Cyber-Security", "IoT and Cyber-Security", "Mobility and Cyber-Security","DeepFake and Cyber-Security", "Artificial Intelligence, Virtual Reality, and Cybersecurity", "Cyber-Security in Critical Infrastructures", "Cyber-Security for Decision Makers".

As a result of the Forum, the following determinations and recommendations were made, and it was decided to bring them to the attention of all relevant authorities and the public with a vision that will raise existing gains/institutions:

1. The rapid development of information technologies has brought security problems of the same magnitude. In the early years of the Internet, "accessibility" came to the fore among the three important components of information security "accessibility, confidentiality, and integrity"; First, the development and operation of the Internet were considered, and "confidentiality and integrity" remained in the background. This has caused the basic architecture and services of the Internet to cause privacy and integrity issues over time. Due to the rapid growth, problems related to "accessibility" have also increased over time, causing the concept of security to always be one step behind in developments.

2. The expected effects of new and emerging technologies on the cyber threat environment; The authorities have confirmed that the future will shape the multidimensional security environment, artificial intelligence and machine learning, autonomous devices and systems, telecommunications and computing technologies, satellites and space assets, human-machine interfaces, quantum computing and threats in cyberspace are within the scope of hybrid warfare, The 5th dimension of cyber-space action has been accepted.

3. New technologies bring dynamism to business and daily life but also contain unpredictable dangers. Today, we are faced with many new phenomena that start with the word "cyber". “Cyber-crime”, “cyber-fraud”, “cyber-bullying”, “cyber-war,” etc. Social awareness of the concepts is increasing day by day. Awareness, which started with the need for cyber-security, has already started to take its place in business life as a new profession with the education and training of experts in the field of cyber-security.

4. It remains a strong thesis that the new pandemic expected after the Covid-19 outbreak may be “problems in cyber-security and competitive governance of the ecosystem.” Because the multidimensional cyber-security field has now become the nature of life, on the other hand, the business and sustainable development model is changing rapidly under the leadership of concepts such as “green economy” and “digital revolution”, as it is better understood that moving from linear economy to “circular economy” is not an option but a necessity in the current pandemic process. This transformation, which also means new global standards, has the potential to change the competitive indexes radically. Knowledge economies focused on the “digital revolution,” which redefines the meaning and value of the concepts of power and property, will be the determinants of today and the future.

5. With the Istanbul Cyber-Security Forum, which was held for the first time in 2022, the traditional understanding of security was examined, and it was concluded that the actual value of "cyber-security" is unfortunately not given to the phenomenon of "cyber-security" at this point and that this field is not known, understood or conveyed clearly by the vast majority. Cyber-security, on which scenarios are written, is explained with technical information on TV channels every evening. Considering that almost everyone from 7 to 77 has smartphones in their hands, it is very important that cyber-security pieces of training are carried out at all levels, from kindergarten to higher education, and citizens' awareness is raised.

6. Cyber-security is one of the essential devices of today's changing security perception with globalization. When the new security theories are examined, the loss of monopoly of states in different areas and the effects of social media on countries as a field of social dynamism have also reshaped security policies. When the change of the perceptual mechanisms of individuals and societies in the modern world and the internet revolution in the context of the manufacturing element are taken as the subject, both the security threats posed by the globalizing world in the security strategies of the countries and the perception management opportunities of the general public with cyber devices will bring many risks. At this point, it is seen that countries have recently built different defense elements in the field of cyber-security as well as traditional defense devices. In today's world, where cyber security is rapidly increasing as a threat, the establishment of cyber-security units in the armies of developed countries, prioritizing measures for cyber-security in public policy processes, taking more initiatives to form the official interlocutor of the states in the cyber field and, of course, strong institutionalization have become essential.

7. With the Post-Pandemic, digitalization has increased in all areas of our lives and has led to a transformation in working conditions as well as individual uses. Companies, institutions, individuals, and even governments have held their meetings online. Although digital tools have increased, primarily due to their economic and ergonomic nature, humanity has suddenly found itself in an unplanned and unconscious digitalization. A rapid entry has been made to a world whose borders are not yet fully known and where all information and documents can be easily accessed. In this direction, the weakness of critical infrastructure security has become a reality faced by many states. There is no compensation for being late in capacity building in this area.

8. Today, most meetings, exams, and interviews are preferred online. Considering there is a race against time in the globalizing world, although these choices lead to savings in both economies, time, and space, the perception of "reality" in all these works should be questioned. The authenticity of the addressee, documents, information, and documents bears a big question mark. While the forgery in employment increases from 6% to 30%, and the number of websites preparing fake documents is increasing daily, it is essential that "verification" channels are used in all areas to detect this situation.

9. Today, the concept of “crime” is an act sanctioned as a penalty or security measure by the governing institutions in the state of law. The person who commits the crime is called the criminal or the perpetrator. However, the definition of “cyber crime” that takes place in the cyber world is still unclear today. Therefore, the creation of new legal fields such as Cyber Law, IT Crimes, IT Law, the creation of new crime forms, and the continuous updating of the strong regulations related to this are the foundations of the latest security ecosystem.

10. While nation-state societies are leaving their place to global communities, today, they are transforming into cyber network societies. Every citizen is an active user of at least one cyber network (Google, Youtube, Amazon, etc.), and today it is seen that this situation has turned into a state-citizen relationship rather than shopping, education, or the provision of any service. Another problem is that these cyber networks, which can access and keep personal data with a single click, unfortunately, do not control the data they have in the centers where they are established. For example, Amazon, a US entity, keeps personal data in Ireland. Here, in front of states, the “How will the cyber homeland or cyber lands be defined, and how will they be protected?” question arises. The lack of a physical equivalent of the cyber world shows that it is impossible to put physical barriers in the cyber or virtual world and necessitates searching for different solutions.

11. Metaverse, or virtual/fictional universe in Turkish, is seen as the future of the internet; With the transfer of different phenomena to the fictional universe, the support of the states and multinational companies, and the fact that real cities began to move to the virtual universe, it is seen that there are perceptual changes in the concept of space and today humanity spends more time in the virtual universe. Being in imaginary reality and investing in it brings a different perspective to form the new world order. In this context, it was emphasized that it is crucial to consider new technologies within the framework of state policies beyond individuality.

12. Cryptocurrency, which was rapidly increasing in popularity in today's world before the transition to the virtual universe, and also called “identityless money”, has revealed the threat of taking away the monopoly of printing money, which has historical importance in ensuring the legitimacy of the states. Printing money has become almost uncontrolled and unmediated. This has the potential to create many paradoxes and threats in terms of financial security. It has been stated that there is an urgent need for regulation and profound work to control all this "unidentified money", which is seen as a reaction to the state's monopoly of printing money and its power to collect taxes.

13. Cyber wars occur when states carry out mutual cyber-attacks, damaging each other's information networks or causing interruptions. The actors involved in this war are countries, their armed forces, intelligence organizations, legal authorities, the private sector, individuals, or some groups. Critical national infrastructures, military systems, or essential industrial structures for the country are targeted in cyber warfare and attacks. In this context, it has been proposed to create different expenditure items and infrastructures than traditional security methods with high competitiveness.

14. The concept of "nation-state", which emerged after a need, is at a crossroads in terms of leaving its place to different state approaches today. The digitalization process has carried the concept of "electronic state" to an extra dimension, and the digitization of states has accelerated. As political actors, states have opened websites for every institution within their structure, so the state's inaccessible and rigid bureaucratic structure has turned into an easily accessible and flexible form - even a system with increased accountability - with these developments. Today, there is no need for long bureaucratic processes for documents requested and required by any institution. Thanks to the e-government application, they can be obtained in seconds with a single click. The digitalization movements in the public sector transformed the New Public Administration understanding and led to great disintegration in the Classical Weberian bureaucracy understanding. These innovations have moved the public sector away from the traditional sense.

15. Quantum technology, which dates back to the 1980s, leads to discussions that it may cause a new war between countries such as the USA and China in terms of including nuclear factors. The most important feature of this technology is the password-cracking technology it contains. Because of the existence and use of this technology, the world's best-protected computer networks are at risk of being decrypted in seconds. There are claims that they send information in the form of photons to space with the quantum teleportation technology developed by China and that they receive critical information from other countries. There are also theories that China has a technology that can change the direction of missiles. Beyond all these claims and assumptions, the fact that Quantum technology is an area that requires more work and investment in terms of ensuring critical infrastructures and data security has been emphasized.

16. One of the early-stage issues where Türkiye can act proactively against new major cyber threats, together with friendly and brotherly countries, is the upcoming cyber threat called “Deepfake.” It is a new generation media type in which the image and voice of people can be changed with those of other people - in sizes that the human eye and ear cannot distinguish - using artificial intelligence-supported neural networks. These file types are produced by applying deep machine-learning techniques and creating identical clones of the original media files. The fact that deep-fake content is being used to generate fake news, as well as inappropriate counterfeit videos of celebrities and even being involved in financial frauds, has raised serious concerns around the world. Even with the use of the voice portion of this technology, countless possibilities are possible, such as issuing critical orders and instructions, triggering political crises, causing stock market manipulations and a nationwide emergency declaration, deceiving military units, and taking part in covert intelligence operations.

17. Deep-fake technology attracts much attention worldwide, not only with its security dimension but also with its civilian dimension. Creating deep-fake content with a very short video, picture or audio recording of a person, whether he is alive or not, takes place in many sectors and sub-units such as the entertainment industry, education sector, culture, tourism, communication, art, textile, film, advertising, health, retail. Has begun to receive. The first application program called Synthetic Reality Technology within the scope of BRAINS² Türkiye (Biotechnology, Robotics, Artificial Intelligence, Nanotechnology, Space, Strategic Services) developed by TASAM; With the theme of “Deepfake Product and Defense Ecosystem Construction”, it has been confirmed that it has a great vision and cooperation potential.

18. Again, within the scope of BRAINS² Türkiye, the “Disruptive Innovation Blockchain Technology” application program developed with the theme of “Internet of Governance and Crypto Assets Strategy” was appreciated for its vision and cooperation potential. Blockchain; Although its popular application is described over cryptocurrencies, Blockchain 3.0 applications, defined as the Internet of Governance, have the potential to have a revolutionary impact on the entire civilization, especially on the economy, security, and smart cities. In this respect, it covers not only technology but also process and governance innovation. It is expected to seriously affect traditional central institutional structures, especially "citizen", "state", "academy", and "private

sector", and even transform communication among themselves. In this context, the Disruptive Innovation Blockchain Technology program; references the definition of the ecosystem in macro and sectoral dimensions for Türkiye and friendly-brother countries, the construction of competitive capacity, its promotion and regulation, and the focus on destructive risks and strategic opportunities focused on security and economy.

19. In the change and transformation of the traditional meritocratic infrastructure based on staff security, the official definition of cyberspace as a new operation area, as well as land, air, sea, and space, within the relevant security/defense authority of the countries, and the "cyber-directorate" as an independent command/presidency on strategic cyber intelligence. -security command/ directorate " has been proposed to be established.

20. It was also recommended that a combat battalion affiliated with the proposed cyber-security command/directorate be structured as an offensive cyber force. This structure's primary purpose should be an operation-defense attack.

21. Establishing an army consisting of professional programmers and coders, whose identities are protected and who are always at the keyboard, who will operate in many areas, who can serve in hot regions and cyber wars, under the roof of "promoting emotional and mathematical intelligence together", and that this army It is proposed to develop and use technologies that enable automatic processing of data by using “big data” analytics to obtain real-time cyber intelligence.

22. For Türkiye, it is a priority to review the cyber industry's scale size and establish a national investment and capacity program in the ecosystem to serve friendly and brotherly countries. The creation and interactive updating of the ecosystem inventory as a model project by using the technology represented by the industry is a priority for tracking the potential and making the right decisions.

23. Involving the representatives of the cyber industry, which includes strategic dimensions that are much more efficient and economical than classical foreign trade and service products, in VIP travels and commercial contacts will increase the sector's motivation. Strengthening the existing cooperation mechanisms between countries in this field will also be a historical awareness.

24. Owning a domestic and national operating system, ensuring a gradual transition, making the internet work independently of global internet providers, establishing a system where “big data” can be processed with artificial intelligence, and possible offensive operations can be

predicted, artificial intelligence supported IPS and IDS systems are developed and “cyber- It was emphasized that it is important and urgent to speed up the work on the “security law” and that the regulation of digital space is a national security/sovereignty problem.

25. For the Cyber Industry, it has been proposed to establish a Ministry or a Directorate within the Presidency of the Republic of Türkiye.. At the same time, the importance of supporting cyber crises and the multidimensional external potential in this field by diplomacy was emphasized using a "cyber industry unit" within the Ministry of Foreign Affairs.

03 November 2022, Istanbul