3rd ISTANBUL CYBERSECURITY FORUM

FINAL DECLARATION (DRAFT)

The 3rd Istanbul Cybersecurity Forum, with the main theme of "New Cyber Economy and Turkish Products," was held jointly with the 10th Istanbul Security Conference as a side event organized by TASAM National Defense and Security Institute on November 21, 2024, at the Wish More Hotel Istanbul.

Speakers and protocol participants from various countries, regions, fields, and sectors attended the Forum. Diplomatic representatives and delegations from different countries also participated. Speeches and presentations were delivered by local and foreign experts, academics, and diplomats. Relevant authorities from Turkey, Asia, Europe, America, and African countries were represented at the Forum, and all sessions were institutionally followed.

The Forum addressed the following important topics: “Cybersecurity in Critical Infrastructures, Mobility, and Cybersecurity,” “Internet of Things and Cybersecurity,” “New Cyber Economy and Turkish Products,” “Artificial Intelligence, Virtual Reality, and Cybersecurity,” “Deepfake and Cybersecurity,” “Cybersecurity for Decision-Makers,” “Industrial Cybersecurity,” and “Cyber-Space and National Security.”

It was decided that the findings and recommendations outlined below, which aim to enhance existing achievements/institutions with a vision, should be brought to the attention of all relevant authorities and the public:

1. The rapid progress of digitalization and technological advancements gives rise to socio-cultural consequences. The impact on individuals' sexual orientations, the imposition of uniform lifestyles through social media platforms, and the construction of a new society are evident. Manipulations such as the widespread recognition of LGBTQ+ rights aimed at youth, the increase in gender reassignment surgeries, and beauty obsessions pose a significant threat to the fundamental dynamics of society. It is observed that suicide rates are considerably high in such degenerate societies.

2. These effects particularly trigger the condition of young people becoming Homo Distractus (Distracted Man). Power centers are attempting to lower the IQ levels of societies as part of their strategy to maintain hegemony. This situation is evident in the example of India, controlled by England and America. It is also observed that this strategy is applied to today's youth through various channels, particularly social media platforms. If the truth is not presented to these distracted youth, significant problems await in the future.

3. The current world system is shaped by the production and utilization of knowledge. Consequently, knowledge has become a direct instrument of power. The relationship between knowledge and power increases the risk of manipulative use of information. The security of knowledge brings about a multidimensional security framework from the individual to the international community. Thus, the concept of "Knowledge Security" evolves into a significant stage concerning the nature of life itself. This comprehensive security domain necessitates the protection of extensive knowledge.

4. In the modern era, the main struggles have shifted to the internet environment. The infrastructure systems, firewalls, and vulnerabilities of countries have become matters of national security. In this context, cyberattacks and cyber threat groups pose significant threats to states, and wars have evolved into "Hybrid Wars." The most distinct characteristics of Hybrid War include the use of advanced technological tools and methods, as well as the blurring of distinctions between civilians and military personnel. Consequently, Hybrid War redefines the current order of warfare. The most impactful attacks in this regard are cyberattacks targeting infrastructure systems.

5. Nowadays, there are five dimensions of warfare. The fifth dimension, space, which includes satellites, is breaking the mold. With potential kinetic attacks on satellites in orbit, not only ground-based systems but also satellite systems in orbit are now exposed to attacks. This elevates the importance of Space and Cyber-Space security to a critical level. Considering the present and future, it is essential to address Cyber-Space as a part of national security and to take and manage precautions according to peace, crisis, and hot conflict/war processes.

6. All passive, reactive, active, and proactive cyber conflict laws encompassing peace, crisis, and hot conflict processes should be implemented within the framework of international and national laws, United Nations Security Council resolutions, and relevant Rules of Engagement. NATO's significant investments in cyber-space should be considered, and the security measures to be taken should adhere to international standards.

7. Technology is no longer merely a tool but has become a force that determines global power balances and is used as a strategic element in international relations. Considering that countries holding technological advancements

influence global power dynamics, the concept of "Digital Sovereignty" emerges as a crucial point.

8. The most significant trigger for technological development lies in the military field. Active wars and power struggles have become the primary driving factors for technological advancement. Important investments, such as advanced weapons, UAVs, and deterrent hypersonic weapons, come to the forefront in this regard.

9. For military power to be effective, military systems must be sustainable, resilient, and integrated with new technological developments, with critical infrastructures playing a significant role. Satellite systems, 5G, and military communication are prominent in this context. Ensuring real-time communication with 5G forms a key point for enabling integration in areas such as autonomous systems, UAVs, cybersecurity, etc. For this reason, it is crucial to support and develop 5G investments and satellite systems as rapidly as possible.

10. In the field of cybersecurity, protection systems and vulnerabilities occur during the process of cyber data entry and exit. This situation renders cyber protection systems highly sensitive and vulnerable to external intervention. Therefore, regardless of the level of security measures, achieving 100% protection is not possible.

11. There is a direct correlation between ensuring data security and the integrity and security of systems. The security of existing structures created for managing critical operations such as credit card payments in the banking sectors must be questioned. Particularly in critical areas like financial analysis, ensuring the security and successful integration of data carries vital importance for minimizing security vulnerabilities.

12. During integration processes, the necessity of the concept of an "integration specialist" should be considered. Encrypted algorithms must be standardized to prevent data vulnerabilities, and projects that ensure integration between different systems must be developed. When considering that the power of data in the new digital world system is more effective than bullets and bombs, the importance of ensuring data security becomes even clearer.

13. Major power competition is taking place in the field of artificial intelligence, and collaboration and competition among significant international actors have

largely begun to revolve around this axis. The European Union has published an Artificial Intelligence Act in this regard. It is possible to see how artificial intelligence integrates into our lives through 3D printers, robots, and even wearable technologies.

14. The relationship between China and the United States progresses within the framework of both cooperation and competition. This great power rivalry is evolving beyond economic competition into artificial intelligence and technology wars. The wars of today are wars of technology and ideas. The focus point in this process should be how prepared we are for new technological developments. We must construct our security strategies on this axis.

15. 15. Digital currencies (CBDCs), which can also be defined as virtual representations of value, have become an integral part of today's reality. The advantages of digital currency systems, such as faster financial transactions, reduced transaction costs, and better tax control, make these currencies more attractive. Thus, it is observed that traditional monetary systems are beginning to be replaced by digital currency systems. However, the vulnerabilities of digital currency systems, such as market manipulations and cybersecurity threats, should not be overlooked.

16. Today, it is stated that digital currency systems will render physical money obsolete and that virtual currency will dominate the market. Specifically, in Turkey, digital currency has been activated as of 2021 and is being developed through HAVELSAN and ASELSAN. However, it is observed that the central bank is not actively involved in this matter. Preparations for digital currency systems are critical, particularly for the future. It is essential to educate the public about these systems through training and other means and to establish necessary legislation for CBDC systems.

17. Israel's act of exploding pagers demonstrates how digitalization can also pose a threat and how digital dependency makes us vulnerable to external threats. Many areas of digital technology that initially appear unrelated to security also have an attack or defense dimension. Considering attacks on devices that can be considered outdated in terms of today's digital technologies, it is estimated that many attack projects are being prepared for more advanced ones. To avoid such threats, integrating the level of production and accumulation we have reached into the domestic market and enacting this as law is of vital importance.

18. In our country, significant research and production units in this context are present through various institutions, and these technologies are extensively utilized in tools used for counterterrorism. Despite these realities, a new attack/defense/security threat can arise in the field of artificial intelligence from technologies that may initially seem unrelated or outdated. Therefore, while focusing on advanced technological fields and software systems, it is critically important not to neglect areas that may appear trivial.

19. The mistake of sourcing all electronic devices, apparatuses, and products, especially mobile phones, from the international market for economic reasons should be avoided. Encouraging, supporting, controlling, and developing domestic production for even the most basic components of electronic devices and procuring them through reliable domestic companies are of significant importance.

20. Israel, with its military capacity and intellectual accumulation, stands out as a powerful country in the Middle East geography. With its high-tech investments, minimization of foreign dependency, and R&D investments to ensure national security in its region, Israel is among the most advanced countries in the world in defense technologies. It possesses a high-capacity military infrastructure and leads in R&D investments. Over the next 20 years, it is likely to dominate the Middle East in the fields of R&D and technology. Israel's strategic moves in the region, its power in international relations, and its high R&D investments make it an actor that must be taken into account.

21. Corruption is one of humanity's common problems. Technological advancements, developments in media and communication, and the emergence of global markets and corporations are among the main factors that have made corruption a global phenomenon. Corruption, also observed in Western-origin companies, becomes more complex and harder to detect as the market and its volume grow.

22. As corruption in Western companies is hidden and grows for long periods, its effects are substantial and destructive. These companies, equipped with advanced technological capabilities, can commit corruption more easily. However, this situation necessitates that the legal authorities combating corruption possess more advanced technological tools, making the fight more challenging and costly. Detecting and exposing corruption leads to the

strengthening of Western institutions and rules, thereby reinforcing Western hegemony.

23. With the advancement of the digital age, particularly the entry of social media into our lives, the concepts of digital ethics and security have become more critical. The embedding of digitalization into every aspect of our lives has brought the concept of "post-truth" into prominence. In this era, online behaviors, information manipulation, and misinformation have become widespread, evolving into societal influence through social media. In Turkey, measures have been taken against this problem, such as monitoring fake news under the Directorate of Communications. However, social media has become a powerful tool for changing people's thoughts and behaviors.

24. In the post-truth era, emotions and personal beliefs come to the forefront instead of facts, deepening issues of information security and digital ethics. States face not only physical threats but also cyber-attacks and digital manipulations. False news and propaganda can change societal perceptions and lead to social and political instability. Therefore, the public must be correctly informed, and appropriate guidance against perception management must be provided. The security of states now requires a strong defense strategy against digital threats.

25. States' security strategies must be reshaped in response to new threats brought by the digital age. Information wars, hybrid threats, and cybersecurity are among the most significant dangers states face. Conspiracy theories, cyber-attacks, and media manipulations undermine trust between the public and the state and threaten the stability of states. Therefore, to ensure digital security and control the flow of accurate information, states must develop effective security networks and formulate policies in line with digital ethical principles.

November 22, 2024, Istanbul