ISTANBUL SECURITY CONFERENCE 2018

FINAL DECLARATION (DRAFT)

Hosted for the first time in 2015 and this year the fourth, the **Istanbul Security Conference** was held on the dates of **08-09 November 2018** in Istanbul under the main theme of "Security of the Future", collectively by TASAM National Defence and Security Institute (NDSI) and Deep Learning Turkey. The **Istanbul Security Conference 2018**, which became a regional and global brand, provided wide-ranging speakers and protocol participation in all disciplines from different countries and regions. All relevant authorities from Turkey was represented at the conference and all sessions were followed institutionally.

During the conference, the **Turkey - Gulf Defense and Security Forum 2018** titled as "The Future of Security in the Gulf" (as in previous years, with the cooperation of Qatar Ministry of Defense, Center for Strategic Studies [QSSC]) and the **Turkey - Africa Defense Security and Aerospace Forum 2018** titled as "Future of Security in Africa, and Turkey" were held simultaneously as sub-events.

Istanbul Security Conference 2018, which brings together participants from 40 countries from the USA to China and from Russia to Iran; has been an important platform for the exchange of views and ideas about new competitive perspectives of Turkey-based security architecture in the light of the facts of ""Industry 4.0" and "Artificial Intelligence".

It was stated in the opening speeches that the last years of conventional security lived and "the security of the future" would be shaped within the framework of the changing state nature. In the conference, the factors that are likely to have an impact on all aspects of the security of the future have been extensively studied. Within the scope of the conference, "Cyber Security", "Deep Learning" and "Artificial Intelligence in Future Security" panels were held. The **TASAM Strategic Vision Awards**, which have been made traditional by TASAM for 11 years, have been entrusted to the successful people and institutions that have strategic vision in a ceremony held during the conference.

As a result of the conference, the following determinations and suggestions were made and it was decided to present to the attention of all relevant authorities and the public:

1. Despite the fact that 500 days have passed since the beginning of the embargo on the Qatar State, no concrete data on the reasons for the implementation of the embargo has yet to be provided. The, "Khashoggi" event, which should be seen as an opportunity for the administrators to correct their mistakes in the Gulf, and it has become a subject that has wounded the conscience of the world and has become completely politicized.

2. Strong Turkey, is the guarantor of Gulf security. The Western Balkans are also very vulnerable in terms of security. The conflicts in these regions are carried out in such a way as to reflect the interests of the great powers and human life is not seen as a priority in politics and is not considered as a priority.

3. Countries should establish their own security systems without rely upon imported safety, otherwise their management may be undermined.

4. No armed force shall express an absolute value in terms of numbers, but may represent a value if it fulfills such tasks as "deterrence", "interference", to be imposed on it by the political authorities. Conventional war will continue to exist. Thoughts that new types of war, such as hybrid warfare that would be the only method of warfare should be considered.

5. Although conflicts do not recognize borders, the decreased limits that have an impact on their spreading are beginning to gain importance again. Globally, more than 60 countries build walls against their neighbors and security is increasingly regionalized. Smart city works across the globe, should be fictionalized not only by technology but also by asymmetrically changing security threats.

6. Hybrid warfare; artificial intelligence, space warfare and cyber-attack should be addressed from an analytical perspective. In this regard, China has been actively working to become a world leader until 2025. The United States formed a space command as “security force element". China has also come a long way in space warfare. The aim of the studies in this area is the military satellites in low-orbit around the world. Non-state actors should be prevented from developing or obtaining an anti-satellite system.

7. The United States stated that it would conduct cyber-attacks on the attack in the cyber security strategy, which was published in 2018, and this situation has taken the issue of cyber-attacks to a wider dimension. The financial resources spent in cyber wars across the world have reached $ 8 trillion. It has been reported that the data of 5 million personnel has been stolen. Until the year 2022, it is foreseen that the need for cyber security experts worldwide is 1.8 million people. The effect size of cyber-attacks will be much greater if they are not trained in the desired quality.

8. In the security of the future, the defense sector should be structured according to the security needs of each country. Due to ignoring the law of armed conflict such as humanitarianism and military generality, many civilians have lost their lives in the operation areas. In the near future, the human need will continue to be important in directing the systems of laser weapon systems, autonomous systems and similar systems that expected to enter the inventory of armies.

9. China, which is a candidate for US legitimacy which is rapidly deteriorating in the global village, is seen as a closed box as it has been throughout history and leads to doubts about the legitimacy it will undertake.

10. It is very difficult for Africa and China to gain equal partnership, and although this work path has not been completed yet, it is seen that it is much more equal in its relations than in Africa - America and Africa - Europe.

11. When the concept of “soft power” began to be used for the first time in the early 1990s, the authorities emphasized that the concept of “hard power” was not an effective tool for achieving

foreign policy and national goals, whereas the notion of soft power would be a new instrument in foreign policy implementations. However, until now, it has been seen that the concepts of soft power and hard power are insufficient to reveal the truth, they have been found to be inadequate to explain foreign policy and they are not realistic. The new concept of "smart power" must be dwell on.

12. In foreign policy applications, states are not the sole actors. There is still a system in which non-governmental actors such as non-governmental organizations, multinational corporations and even terrorist organizations affect states. The notion of soft power alone cannot be sufficient in the multi-dimensional plane and, when necessary, hard power can be adopted as a method. The power components can be balanced so that the notion of smart power is revealed.

13. In recent years, it has been determined that China may constitute an important precedent in the use of smart power. Because it is difficult to separate economic development and cooperation from political structure, China avoids political impositions when it offers economic cooperation to states outside the region and the region, thus creating a global attraction in recent years. Presence in humanitarian activities in Turkey's region and its efforts to increase gradually in recent years, the region provides an important soft power capacity to occur in favor of Turkey.

14. The power distribution in the years when the concept of "Soft Power" was introduced is the bipolar order of the Cold War period, but today it is not a good idea to talk about the bipolar power distribution. The system perspective should not be ignored in order to reveal a future perspective with soft power and neither soft power nor smart power inferences can be revealed by ignoring the system approach.

15. In recent years, defense industries have been carrying out robotic breakthroughs and conducting R&D studies for the concept of robotic war. Especially after the September 11 attacks, there has been a dramatic increase in semi-autonomous unmanned aerial vehicle technologies. Autonomous weapons systems are the last stage of this dramatic rise. Besides, there is no codification in international law for autonomous weapons systems and there are serious gaps in the context of international human rights, humanitarian law, criminal law and responsibility during its use and these gaps need to be codified immediately.

16. Hybrid battles cover all areas of internal and external security, as states develop attacks with nonlinear methods by taking advantage of the weaknesses in decision-making structures. Democratic societies are vulnerable to hybrid attacks and threats due to their fragility. For this reason, in order to cope with hybrid threats and to be ready for hybrid warfare, it is very important for states to improve their co-ordination and cooperation through a totalitarian and comprehensive approach.

17. In 2017, China initiated a government program called the New Generation Artificial Intelligence Development Program and formulated its steps in the field of artificial intelligence in a strategy paper. One of the most striking aspects of this perspective is that China is aiming for global leadership with the steps to be taken in the field of artificial intelligence until 2025.

18. With the development of network technologies, the importance of "cyber security" on the world agenda has become an increasing issue day by day. Therefore, due to risk-based approaches, states spend a high level of expenditure. Compliance agreements are made in order to eliminate violations. The development of information technologies made out the notion of asymmetric warfare.

19. Funding support for further progress of artificial intelligence work in Turkey should be increased. Besides that, the integration of the deep learning system into education and defense is also of great importance.

20. Security cameras are key factor in the security of the future, with the contribution of artificial intelligence and deep learning studies. There are 256 million security cameras around the world, but they are not smart cameras and cannot highlight the findings that experts can seek solutions to security problems. Intelligent cameras with qualitative features; In the observation of the students in educational institutions, in identifying the malicious people arriving at any entertainment venue, in the detection and prevention of possible security problems in a crowded airport, shopping center, bus / train station or city square, they are used in the identification of provocative and malicious people in actions and depending on these, security vulnerabilities in cities can be solved by smart cameras.

21. In the field of law, artificial intelligence studies are carried out in the world, the use of ethics and judicial process are emphasized and artificial intelligence can be assumed instead of a judge in the future. The USA has been working in this field in recent years.

22. R&D startup companies in Turkey should be supported in terms of financial resources and investment funds. It should be considered on public and private sector adaptation.

23. According to US security reports, China and Russia are developing weapons systems that can disable US military satellites. In 2018, US President Donald Trump's statement that he had built the Pentagon's space forces as the sixth force is an important fact in understanding the future level of security in space. Concordantly, in the near future, it is foreseen that a covert struggle between the United States and China.

24. There are satellites used for military espionage in the context of Low Earth Orbit, which is defined as LEO (Low Earth Orbit) in the space war. Particularly, the US develops new weapons systems and war approaches to eliminate the approach of the "Global Network-Based War Doctrine" in Iraq War, to cut the information and intelligence and to make the states blind and deaf in war environments.

25. Although the US does not have an official definition for space warfare, China has developed a definition; “a combat technique based on the mutual operation of the two states in an area called outer space for attack and defense purposes”.

26. In the context of military espionage, especially through military satellites, the United States can take high-resolution photos of all parts of the world, have special communication facilities, and have the

capacity to listen and receive. The US also has long range missiles that can be sent from space to anywhere in the world from 30 to 60 minutes. All these issues must be followed and evaluated with great importance.

27. During the Ukraine Crisis in 2015, Russia included the information warfare in its military defense strategy document. Another target of Russia, which aims to cut off all information support of the enemy in war and similar situations, is the orbit of the US spy satellites.

28. Non-state actors can buy satellites that can broadcasting television in order to create propaganda, disinformation and information pollution in space and similar satellites can also be purchased by terrorist organizations.

29. The United States has created a reserve mechanism that can restore the satellite system with the B52 aircraft to developed in order to prevent its satellites from being turned blind and deaf. This is even a clear example of how far the United States has taken into account the struggle in space and how seriously it takes space technologies. Turkey, which plans to build a spaceport in the capital Ankara and this is one of the innovative steps of Turkey.

30. The transfer of 28 billion barrels of oil from the South China Sea every year is a commercial statistic that need to be emphasized. In addition, the political problems experienced by the coastal states in the past and now have made the South China Sea one of the most problematic waters in the world. As a matter of fact, this situation will bring the issues of South China Sea to the academic agenda in the future perspective. The problems in the South China Sea can be severely spread all over Asia.

31. The spread of the Internet has led to the change extent of terrorism and the emergence of new concepts. Terrorist organizations have specialized in social media, and this has created the notion of "new terrorism". As a result, terrorist organizations have begun to obtain opportunities to spread the manipulative knowledge to large masses and to gather supporters from a wider audience. The acquisition of these amenities by terrorist organizations would require the security forces to develop their communication and coordination capabilities.

32. In countering terrorism; gaining knowledge cannot increase the power of foresight. It is vital that analysis units should be trained and reach a sufficient number in producing predictions for surprise attacks.

33. There should be some principles that international organizations must adopt to maintain their legitimacy in the context of peace and stability; international organizations should focus on conflict prevention, not on interference. This will prevent the emergence of wars and reduce human losses. Therefore, it is necessary to focus on the plans and projects for the prevention of wars.

34. Internationally, strategic and inclusive partnerships are vital importance. Necessary coordination should be ensured at local and regional level with security forces, NGOs and non-state organizations. All these elements have as much role as the state in peacekeeping.

35. The success of programs related to peacebuilding is directly related to its sustainability. For this reason, international organizations should approach sustainable development programs with maximum care.

36. Motivating to maintain peace at national level as well as international will reduce the burden of international organizations in resolving crises. There is a wide network of responsibilities, including international organizations as well as political parties, youth organizations and the private sector.

37. Women's social, political, business life and more contribution in every field is one of the most important points that should be emphasized in the reduction of violence, peace building.

38. Turkey's activities towards ensuring security in Somalia is one of the illuminating examples of the construction of peace. Likewise, Turkey has provided similar support to 8 countries. Turkey ranks second after the US in terms of humanitarian aid to all over the world, but it is the first in the world in terms of the gross domestic product rate of financial assistance, which is worthy of any kind of appreciation.

39. The US Country / Homeland Security Organization and the 2018 World Economic Forum assesses that strategic cyber-attacks have the highest destructive power after the nuclear war and cyber warfare has emphasized that it has a very sensitive position in the security of the future.

40. New technologies such as “big data analysis”, “machine learning” and “deep learning” should be utilized to prevent damage after cyber-attacks and to minimize their losses and besides that, corporate awareness should be owned by senior management and cyber-attacks should be based on a technically systematic and holistic approach.

41. Cyber activities are inherently anomalous. In addition, with asymmetric effect in cyber activities, obscurity and continuity sit at the center of the process. If it is considered within this framework, it is not a war but a struggle and hybrid personnel group with special expertise for each specialized struggle, flexibility and maneuverability in planning is extremely essential.

42. Information Technologies (IT) are designed to adapt to very fast changes and are renewed every 3-4 years to meet the needs. On the other hand, Automation Technologies (AT), are designed to operate for 25-30 years without any intervention. In this time, with the digitalization IT systems and AT systems have started to integrate and this integration is a candidate for new vulnerabilities in the security of the future.

43. Factories with power plants is connected to the internet so that it can be managed remotely and the data can be collected and measured and this situation raises the danger of cyber-attack. According to statistics, there are 516 cyber-attack attempts per day in Turkey and according to research, recognition of a cyber-attack takes average 5 months in the worldwide and day by day, it is become more difficult for institutions to resist and respond agile in the face of increasing cyber-attacks in terms of diversity and violence.

44. With cyber security activities, it is very important to make a quick and accurate response before the possible attacks occur. Identification and administration of threats and vulnerabilities, tracking of the threats towards security for the detection of attacks, an active strategic governance to allow an active process of intervention for the cyber incidents following an attack, transformation and achieving most updated security standards by creating an active cyber security framework for defense of cyber incidents are only possible with an end-to-end cyber security framework.

45. In the field of cyber security, a paradigm shift from the "control-based approach in traditional administrative systems" towards an approach in which technical vulnerabilities are continuously scanned, identified and eliminated with the current threats considered is evident.

46. Recently, cyber security operation centers, cyber threat simulations, red team applications, cyber abuse investigation and cyber risk insurance concepts are seen as cyber security trends.

47. It is the duty of a state to ensure a future of uninterrupted security and perpetual prosperity for its people. Prosperity and security, two things that can only be improved in a financially systematical economy through proper education, not only is threatened by matters involving arms, but also by matters where the national currency of the target nation is put to test by foreign financial manipulation, as seen in the examples of Qatar and turkey.

48. As a precaution against this attack, the target countries have the means to minimize financial risks through long-term macroeconomic analysis, and the main instrument is to provide monetary security. Indeed, basic development indicators are, low inflation, acceptable "convertible" currency, high-demand government bonds, demographic stable balanced population growth and digital weighted technological development. Today, technological development is building a capitalist system without capitals with digital inputs.

49. In terms of political economy perception, economic security and country security come together in the same macro balances. The developments in our period include the signs of the upcoming new economic orders because of depreciation of TL by external factors, trade wars between the US and China, the reaction of the EU to the Italian national budget, Brexit, Iran sanctions etc. The quest for global economic leader countries is emerging and it is necessary to initiate processes that include the R & D and the real sector in the regional and national plan, including the guarantees that will attract international investors in the fiscal discipline to restrain inflation for this new order.

09 November 2018, Istanbul