PERCEPTIONS

JOURNAL OF INTERNATIONAL AFFAIRS

SAM
stratejik araştırmalar merkezi
center for strategic research
Türkiye Cumhuriyeti Dışişleri Bakanlığı
Republic of Turkey Ministry of Foreign Affairs

Autumn-Winter 2021
Volume XXVI Number 2
ISSN 1300-8641

PERCEPTIONS

Homepage: http://www.sam.gov.tr

The Center for Strategic Research (Stratejik Araştırmalar Merkezi- SAM) conducts research on Turkish foreign policy, regional studies and international relations, and makes scholarly and scientific assessments of relevant issues. It is a consultative body of the Turkish Ministry of Foreign Affairs providing strategic insights, independent data and analysis to decision makers in government. As a nonprofit organization, SAM is chartered by law and has been active since May 1995.

SAM publishes Perceptions, an English language journal on foreign affairs. The content of the journal ranges from security and democracy to conflict resolution, and international challenges and opportunities. Perceptions is a bi-annual journal prepared by a large network of affiliated scholars. The views expressed in the articles are those of the authors and should not be attributed to the Center for Strategic Research.

PERCEPTIONS is a peer-reviewed journal and is included in the following databases and indexes: Columbia International Affairs Online, CSA Index, Current Contents of Periodicals on the Middle East, EBSCO, European Sources Online, Index Islamicus, International Political Science Abstracts (IPSA), Lancaster Index to Defense & International Security Literature, PAIS Index, Pro Quest, ULAKBIM TR Dizin and Index Copernicus.

To subscribe, write to the Center for Strategic Research, Dr. Sadık Ahmet Caddesi No: 8, Balgat / 06100 Ankara - TURKEY
Phone: +90 (312) 292 22 30 Fax: +90 (312) 292 27 15 - 253 42 03
e-mail: perceptions@mfa.gov.tr @sam_mfa
Printed in Ankara by: Matsa Basımevi

Printed in Ankara, December 2021
ISSN 1300-8641
e-ISSN: 2651-3315

PERCEPTIONS
JOURNAL OF INTERNATIONAL AFFAIRS
Autumn-Winter 2021 Volume XXVI Number 2

TABLE OF CONTENTS

Guest Editor: Merve SEREN

EDITORIAL

COMMENTARY

ARTICLES

BOOK REVIEW

center for strategic research
SAM
Republic of Turkey
Ministry of Foreign Affairs

Publication Ethics

Perceptions: Journal of International Affairs is a double blind peer review international academic journal which strives for meeting the highest standards of publication ethics. Publication malpractice is strictly prohibited by all possible measures.

The publication ethics of the journal is mainly based on the "Code of Conduct and Best-Practice Guidelines for Journal Editors".

Authors: Authors should present an objective discussion of the significance of research work as well as sufficient detail and references to permit others to replicate the experiments. Fraudulent or knowingly inaccurate statements constitute unethical behavior and are unacceptable. Review articles should also be objective, comprehensive, and accurate accounts of the state of the art. The authors should ensure that their work is entirely original works, and if the work and/or words of others have been used, this has been appropriately acknowledged. Plagiarism in all its forms constitutes unethical publishing behavior and is unacceptable. Submitting the same manuscript to more than one journal concurrently constitutes unethical publishing behavior and is unacceptable. Authors should not submit articles describing essentially the same research to more than one journal. The corresponding author should ensure that there is a full consensus of all co-authors in approving the final version of the paper and its submission for publication.

Authors should also make sure that:

a) There is no conflict of interest in their submissions.

b) They have obtained the approval of the "Ethics Board/Committee" for clinical and experimental studies conducted on humans and animals (including opinion polls, surveys, interviews, observations, experiments, focus group studies). This approval should be clearly stated and documented in the article (board's name, date and issue number).

c) Their submissions comply with the copyright regulations (especially for tables, graphs, illustrations, pictures, photographs).

Editors: Editors should evaluate manuscripts exclusively on the basis of their academic merit. An editor must not use unpublished information in the editor's own research without the express written consent of the author. Editors should take reasonable responsive measures when ethical complaints have been presented concerning a submitted manuscript or published paper.

Reviewers: Any manuscript received for review must be treated as confidential documents. Privileged information or ideas obtained through peer review must be kept confidential and not used for personal advantage. Reviews should be conducted objectively, and observations should be formulated clearly with supporting arguments, so that authors can use them for improving the paper. Any selected referee who feels unqualified to review the research reported in a manuscript or knows that its prompt review will be impossible should notify the editor and excuse himself from the review process. Reviewers should not consider manuscripts in which they have conflicts of interest resulting from competitive, collaborative, or other relationships or connections with any of the authors, companies, or institutions connected to the papers.

The information and views set out in this publication are those of the authors and do not necessarily reflect the official opinion of the Center for Strategic Research (SAM) and the Ministry of Foreign Affairs of the Republic of Turkey.

EDITORIAL

Promises and Perils: Exploring the Turkish Defense Industry

Merve SEREN [*]

First of all, I would like to express my sincere gratitude to the Center for Strategic Research (SAM) and the editorial board of *Perceptions: Journal of International Affairs* for the privilege of being the guest editor for this volume. The five articles of this issue are devoted to the Turkish defense industry, which has been attracting worldwide attention due to the great leap forward Turkey has achieved in this sphere over the last two decades. In fact, many people from academic, bureaucratic, industrial and commercial circles around the world question the reasons, motivations and objectives behind Turkey's increasing interest and investment in the military and defense industry.

Today, Turkey is considered to be among the most promising exporters in the defense market; the country has acquired a worldwide reputation due to its impressive progress and the high operational performance of its combat-proven defense systems and weapons. However, the upward trend in Turkey's national military-industrial complex and the acceleration of its defense capability enhancement has raised the concerns of a wide range of state and non-state actors on a global scale.

The ongoing debate about Turkey's defense industry focuses on two main points. The first has to do with the changing character of Turkey's foreign and security policy and revolves around the question as to whether Ankara is trying to free itself from the U.S.-led and NATO-dominated political roadmap that has long shaped its decisions and strategies with respect to its regional and international engagements. The second point is about Turkey's new military and defense strategy and revolves around the question as to whether Turkey's military operations, plans and doctrinal changes indicate a shift from a defensive to a more offensive approach.

[*] Assistant Professor, Department of International Relations, Ankara Yıldırım Beyazıt University, Ankara, Turkey. E-mail: mseren@ybu.edu.tr. ORCID: 0000-0002-0931-1572.

On the one hand, Mustafa Kemal Atatürk's inheritance is being preserved, since the central principle of Turkey's foreign and security policy remains strictly in accordance with the official motto, 'peace at home, peace in the world'. This means that Turkey continues to maintain its military rationality and inspiration with the goal of building and sustaining peace at all levels—from the local to the global. Contrary to the allegations that Turkey is developing a more independent and assertive foreign and defense policy in a way that alienates its traditional allies, Ankara's defense discourse is actually quite well-maintained, since the degree of convergence of security interests between Turkey and NATO is much higher compared to their degree of divergence.

On the other hand, in light of means and ends, particularly at a time when Turkey's struggle to mitigate the risks and threats emanating from its changing regional security environment urges it to make more vital choices and take more rapid actions, Ankara is favoring a more flexible, adaptive and resilient defense posture that is consistent with its actual and potential core interests. In this regard, Turkey's military and defense policy reflects its quest to become a more deterrent power while adopting a proactive and integrated approach to realizing the new parameters of its grand strategy.

From this perspective, the five distinguished authors who contribute to this issue have been specifically chosen because of their decades-long experience in the Turkish defense bureaucracy and security sector. In addition, they each have different areas of expertise and different academic backgrounds. Hence, all five authors make comparative, critical and insightful analyses about the promise and perils of the Turkish defense industry with respect to doctrinal and institutional change and operational performance.

It should be noted that Turkey's defense policy and industrial development strategy encompass a wide range of subjects, such as force projection, military diplomacy, management of production, logistics and procurement, R&D and innovation investments, prime contractors and subcontractors, intellectual property rights, export regime, offset trade, financial and budgetary policies, etc. In this regard, the process of selecting articles for this issue was quite challenging, particularly since there is a large research agenda that is still underexplored in the literature on the Turkish defense industry.

Ultimately, the five articles contributing to this issue are especially chosen as a response to the aforementioned debate points that explore Ankara's will and enthusiasm to initiate bureaucratic and industrial transformation. Therefore, the articles are expected to stimulate further academic debate on mapping Turkey's future national defense industrial ecosystem in terms of the country's ambition to realize self-sufficiency, emerge as a leading exporter in the arms market and earn the technological knowledge, breadth and depth to consolidate its position as a stronger security and defense actor on the global stage.

In his article, Hüsnü Özlü sheds light on the evolution of the Turkish defense industry from the early Republican period to the contemporary era. In addition to examining deep-rooted historical, socio-political and economic factors, he explores the changing security environment and conditions in Turkey that have triggered the transformation process in the defense industry that began in the 1980s and led to the adaptation of a new national defense industry strategy in the early 2000s.

Given the complexity of contemporary defense systems, the ever-changing dynamic conditions in which security is conceptualized, the interconnected agents and variety of fragmented and interactive domains in which security is enacted, the defense industry has become one of the most challenging topics for academics, decisionmakers and other officials to study and analyze. The article by Mehmet Hilmi Özdemir and Gökhan Özkan is the outcome of their efforts to initiate a new methodology to address new questions by adopting an innovative and holistic approach for the comprehension of the interconnectedness and interrelatedness among all the parts that make up the whole system. The authors highlight how a systems-thinking approach, together with the Viable System Model (VSM) and system dynamics methodologies, can introduce various benefits such as decision support, and provide accurate evaluations, successful judgements and strategic foresights.

Turkey's cyber awareness and readiness level also require more academic attention. In their article, A. Burak Darıcılı and Soner Çelik explore the benefits and costs of technological developments by focusing on both the advantages of cyberspace and the vulnerabilities of cybersecurity. The authors emphasize the need for and significance of preparing cyber strategies, engaging in long-term planning, establishing special institutional structures, undertaking cyber reforms, developing an international cybersecurity alliance and engaging in cooperation in order to improve cyber defense and attack capacities, since the issue is critical for survival.

Özden Özben's article discusses conceptualizations of border security and integrated border management under the rubric of homeland security, and explores the definition and reinterpretation of 'borders', which have long been analyzed within the scope of physical and technical dimensions. The author argues that today's borders are not the same as the boundaries drawn in the past; rather, they have become much broader due to multidimensional, multi-stage and multi-pronged risks and threats. Özben emphasizes the necessity of adopting 'integrated' border management in the fullest sense which requires the national defense industry to develop a more proactive approach and reach a higher level of industrial competence.

The article by Ufuk Sözübir touches upon the issue of unmanned aerial vehicles (UAVs)—probably the hottest topic of the debate regarding Turkey's defense industry in the last decade. Not only have Turkish-made UAVs become the most cited success story in the Turkish defense industry discourse, they are also considered game changers, since they have provided Turkey with greater diplomatic and operational maneuverability in foreign and security policy. They have also boosted Turkey's confidence in meeting its objective of localization and nationalization, and of achieving strategic autonomy as part of the Turkish national security strategy. Sözübir's article focuses on both the promise and the perils facing the Turkish defense industry, and discusses the advantages and disadvantages of UAV systems in terms of technological opportunities, technical risks and threats and ethical challenges with respect to international humanitarian law.

In addition to these articles, which explore various aspects of the Turkish defense industry, the current issue also includes the commentary by Ömer Kocaman, Deputy Secretary General of the Organization of Turkic States, who discusses the evolution of the role of this important international organization in the post-Covid-19 world, and the article by Sujata Ashwarya, who seeks to reveal the main dynamics that shape Israel's renewable energy strategy in light of its stated goals.

COMMENTARY

Adjusting to the "New Normal" of Post COVID-19: The Role of Organization of Turkic States in Multilateral Cooperation

Ömer KOCAMAN [*]

Abstract

The article explores the role of the Organization of Turkic States in enhancing cooperation among its Member and Observer States and across the region in the post-COVID-19 era. It also examines the changing postures of multilateralism before and after the pandemic, while referring to the significance of functionalism, the original parameters of which persist even today. After the theoretical introduction, the article first analyzes the ways in which the Organization has responded to the pandemic and provides concrete examples of tis efforts. Next, it touches upon the peculiarities of the structure of the Organization, its working system and its decision-making process, which have allowed it to respond rapidly to the needs of its Member and Observer States and their people. In line with this aim, it examines the role of the Organization in bringing the foreign policies of the Turkic States into convergence, fostering multidimensional connectivity with a sectoral approach and supporting people-to-people cooperation. Finally, it focuses on the contributions of the Organization to the capacity-building of its Member States and its support for international cooperation. Taken together, these features provide a basis to check the efficiency of the organization in terms of today's contested multilateralism.

[*] PhD, Deputy Secretary General of the Organization of Turkic States.
E-mail: okocaman@turkkon.org. ORCID: 0000-0003-0355-3965.

Received on: 10.09.2021
Accepted on: 12.12.2021

Keywords

Organization of Turkic States, Turkic cooperation, multilateralism, COVID-19 pandemic, capacity-building.

Introduction

The COVID-19 pandemic has functioned as an important "wake-up call" for the entire international system. This unexpected development has reminded us of the necessity of adding new components, such as health care and security, to the priority list of global affairs. The pandemic reaffirmed that a virus does not have any "passport" or any "border" from the global economy to our daily life, it affects all aspects of the current global order, in which multilateralism has already faced severe challenges. Robert Keohane had defined multilateralism in 1990s as "the practice of coordinating national policies in groups of three or more states, through ad hoc arrangements or by means of institutions."[1] Although this definition remains valid for today, the needs that give rise to multilateralism have changed enormously; we now face a multi-polar system that is more unpredictable than ever, and teeming with a complex, inter-related variety of threats in areas ranging from security, the economy and health to environmental disasters. Together with this chaotic picture, there is another undeniable fact: the tremendous increase in the number of multilateral organizations worldwide. While the number of multilateral intergovernmental organizations was fewer than 100 in 1945, today it has reached 7,804.[2] Whether this skyrocketing increase has brought with it an equivalent rise in efficiency is of course a big question that needs to be addressed.

Multilateralism had already come under a lot of stress and criticism before the outbreak of COVID-19; many were interrogating the effectiveness of international organizations, their representativeness, the rapidity of their decision-making system, and questioning whether it was their nature to be value-based or to remain stuck in pure realism. The creator of the theory of functionalism in international relations, David Mitrany, in his pamphlet titled, "A Working Peace System: An Argument for the Functional Development of International Organization," dated 1943, explains why the League of Nations system failed, and sketches out the broad lines of a functional organization of international activities. In his foresightful pamphlet, he points out that "these activities would be selected specifically and organized separately each according to its nature, to the conditions under which it has to operate, and to the needs of the moment."[3] So, before the establishment of UN and its system, the necessity to address "the needs of the moment" was an important criterion for the effectiveness of international organizations to ensure a robust international order. Actually, the UN and Bretton Woods Institutions had been structured in line with this aim. However, over the years, they became less responsive to changing needs. Thus, in the present day, in which we are experiencing globalization 4.0 together with " the challenges associated with the Fourth Industrial Revolution (4IR) that also coincides with the rapid emergence of ecological constraints, the advent of an increasingly multipolar international order, and rising inequality," [4] we are obliged to equip international organizations with adequate means to provide shared global governance for the future. While doing so, we must not forget that despite the fact that the world has become a "global village," nationalism has spread again worldwide in a way reminiscent of its profusion between the two World Wars.

Nationalism, coupled with globalization, has triggered "an environment of mistrust toward all things foreign," resulting in the enforcement of protectionist measures, disruptions vis-à-vis supply chains, the building of walls between countries and the closing of borders when deemed necessary.[5] As Kissinger recently elaborated, "nations cohere and flourish on the belief that their institutions can foresee calamity, arrest its impact and restore stability."[6] Yet the COVID-19 pandemic has shown that even the "strongest" nations and their institutions were lacking in preparedness in the face of such a global threat.

The pandemic has also amplified the already existing mistrust toward the ongoing international order and its institutions. It has opened once again the "Pandora's box" concerning the immediate need to strengthen multilateral cooperation in an effective, comprehensive and resilient way. Just after the onslaught of the COVID-19 pandemic, states inherently launched the most Hobbesian measures to protect their borders and their people. How to develop vaccines and share them with other countries or not has become a matter of serious discussion all over the world. Hence, with the emergence of state behaviors based on elements of pure realism, a protectionist approach immediately became predominant worldwide. This even spawned the emergence of "vaccine wars," together with their strong geopolitical connotations. However, it soon became clear that the implementation of isolationist/protectionist measures is not sustainable; the world needs multilateral cooperation more than ever to combat this scourge. Thus, the decisions taken at both the national and international levels to tackle the pandemic will play significant role in shaping the world order and international system in the post-COVID-19 era.[7]

Being aware of such a responsibility, since its establishment in 2009 as a regional inter-governmental organization, the Cooperation Council of Turkic Speaking States (Turkic Council), the name of which changed into the Organization of Turkic States at the Istanbul Summit held on November 12, 2021 has worked for the enhancement of cooperation among its Member States and an increase of collaboration across the region; as a result, the Organization has contributed to the empowerment of multilateralism. Covering an area of 4.5 million $km,^2$ with an economic potential of over 2 trillion USD and a population of 160 million, the Organization of Turkic States is a rising regional power in Eurasia. Its outstanding performance during the COVID-19 pandemic has been a remarkable example to this end. In this regard, after analyzing the ways in which the Organization of Turkic States has responded to the pandemic, we will focus on (1) the peculiarities of the structure of the Organization, its working system, decision-making process, etc.; (2) its role in coordinating the foreign policies of the Turkic States; (3) its fostering of multidimensional connectivity with a sectoral approach; (4) its assistance with people-to-people cooperation; (5) its contribution to capacity-building as a cross-cutting responsibility; and (6) its support for international cooperation. The article will conclude with an assessment of the Organization's efficiency in light of today's contested multilateralism.

Addressing the Needs of the Times: COVID-19 and Beyond

The Organization of Turkic States, with its Member States, Azerbaijan, Kazakhstan, Kyrgyzstan, Kazakhstan, Turkey and Uzbekistan, and its Observer countries, Hungary and Turkmenistan, has been involved in intensive cooperation across a wide range of areas from foreign policy, economics, transportation, customs, ICT, agriculture, tourism, media, education and diaspora to youth and sports. The pandemic has not stopped the Organization from engaging in these areas and even expanding into new essential sectors such as health and migration. Thus, just after the outbreak of COVID-19, at the request of H.E. Ilham Aliyev, President of the Republic of Azerbaijan, as the Chairman-in-office of the Organization of the Turkic States, the Heads of State of the Organization of Turkic States came together for the first time at an Extraordinary Summit held on April 10, 2020 in a video-conference format with the theme of "Solidarity and Cooperation in the fight against the COVID-19 pandemic." This timely Summit was the first regional gathering to take place after the G-20 Virtual Summit, and was attended by the Presidents of the Member States, the Prime Minister of Hungary and the Secretary General of the Organization of Turkic States. The Director-General of the World Health Organization, Dr. Tedros Adhanom Ghebreyesus, also took part in the meeting. At the Summit, the leaders of the Turkic World voiced their determination to engage in enhanced cooperation to fight the pandemic in all its aspects on the basis of a strong political will that would further strengthen solidarity among the Turkic-speaking peoples. They identified health, the economy & trade, transportation, customs and migration as priority areas in this fight, and tasked the relevant Ministries to collaborate in an innovative way to address these priorities.

The pandemic has not stopped the Organization from engaging in these areas and even expanding into new essential sectors such as health and migration.

Starting from the outbreak of the COVID-19 pandemic, the Organization of Turkic States had already confirmed their capacity to react quickly and collaborate successfully in times of crises.[8] They were the first to share hospital facilities, provide humanitarian aid and testing kits and exchange clinical expertise and medical support to each other, and to share information on containment and mitigation measures. Director-General Ghebreyesus praised this cooperation during the Extraordinary Summit, stating, "this is an example of the kind of cross-border cooperation we need to get through this pandemic."[9] The decisions taken at the Summit by the Heads of State laid the foundations for a turning point for cooperation within the Organization at such a difficult time. The Extraordinary Summit was followed by intensive consultations of among the Foreign Ministers of the Organization of Turkic States to draw a road map for the implementation of the Summit decisions. The meetings of the Ministers of Health (April 28), the Ministers of Transport (April 30), the Ministers of Economy and Trade and the Heads of Customs Administrations (May 6) and the Heads of the Migration Services and related Authorities (May 7) were the concrete outputs of this road map. Moreover, a task force at the level of Deputy Ministers dealing with health, transportation, customs, border control, migration and economy was established within the Organization as a mechanism of coordination. [10]

The Meeting of the Ministers of Heath was essential to discuss measures to combat COVID-19 and to establish systematic cooperation for the prevention, diagnosis, treatment and epidemiological monitoring of other dangerous infections in the future. At the meeting, the countries of the Organization of Turkic States committed to continue sharing best practices, organizing capacity-building programs and intensify cooperation on the development of well-equipped modern hospitals. The Ministers agreed to establish the Health Coordination Committee, which will host a Supply Chain Group tasked with seeking areas for cooperation in the production of medical equipment and pharmaceuticals that the Member States require the most. A Health Scientific Group was also established within the Organization. Furthermore, through the signing of a Memorandum of Understanding (MoU) on September 11, 2020, the Organization and the UN World Health Organization (UN WHO) engaged in active collaboration in the field of health, including areas such as "universal health coverage, protecting against health emergencies and promotion of the well-being of the populations in the Member States of the Organization of Turkic States."[11] Overall, the cooperation in the era of COVID-19 is an example of how the Organization can mobilize itself quickly in time of crisis to address emerging needs. Its values, structure, working system and decision-making mechanism facilitate such mobilization.

Institutionalization of Cooperation through Adequate Means

Since its establishment in 2009, the Organization of Turkic States has played a crucial role in establishing structured and systematized cooperation among the Turkic States. The existence of the Organization as a regional mechanism has institutionalized cooperative relations between the Turkic States within a multilateral framework. This institutionalization was achieved as an outcome of efforts dating back to the 1990s, and constitutes a perfect tool with which to set the rules of collaboration in the Turkic region, to secure the terms of its management, avoiding any regression, and to take measures for its deepening and diversification. Relying on the continuous political will of the Member States, this solid framework has enabled them to score significant achievements in various cooperation areas within the Organization in a short period of time. The keys of this successful performance are embedded in the principles and structure of the organization, and in its result-oriented approach in political, economic, cultural-educational and human fields. Furthermore, its collaboration as an umbrella organization with other Turkic cooperation organizations, such as Parliamentary Assembly of Turkic Speaking States (TURKPA), International Organization of Turkic Culture (TURKSOY), the Turkic Culture and Heritage Foundation (TCHF) and the Turkic Academy, has contributed to the enhancement of Turkic cooperation at the parliamentary, cultural, academic and scientific levels.[12]

Since its establishment in 2009, the Organization of Turkic States has played a crucial role in establishing structured and systematized cooperation among the Turkic States.

There is no doubt that respect for sovereign equality, territorial integrity, the inviolability of internationally recognized borders, non-interference in one another's internal affairs and adherence to all universally recognized principles and norms of international law empower the Organization of Turkic States. Based on these principles, the last eleven years have proved that decisions and actions taken within the Organization are comprehensive and inclusive. In that time, the Organization has become a rising regional actor that acts not only for the benefit of its Member States but for all stakeholders in the region. The accession of Uzbekistan to the Organization in 2019 as a Member State is a significant outcome of the successful regional cooperation cherished within the Organization of Turkic States.[13] Similarly, the rapprochement between the Organization of Turkic States and Turkmenistan is another recent critical achievement. The fact that the Organization has proven itself to work for the benefit of all Turkic States has gravitated Turkmenistan toward it, and led the country to officially apply to become an Observer country in 2021. Hungary's participation as an Observer to the Organization, granted in 2018, constitutes another milestone. After being granted this status, in a short period of time, Hungary has engaged in most of the cooperation schemes in the Organization from transportation to education. Upon Hungary's proposal, a Representation Office of the Organization of Turkic States was opened in Budapest by the Foreign Ministers of Member and Observer States. The Office has been mandated to promote the Organization and its activities in Europe, while contributing to the enhancement of its relations with European institutions.[14] Hungary's Observer status opened up new discussions for the addition of new observer countries to the Organization. As of October 2021, ten countries have submitted a request to become Observers of the Organization, while seven other states have demonstrated interest in cooperating with the Organization under different modalities. This interest indicates that the organization has become a center of attraction not only for the Turkic States but for regional partners.[15]

The simplified decision-taking process within the Organization of Turkic State has enabled decisions to translate into actions in a rapid way. The existence of working groups and ministerial meetings in each cooperation field, the submission of decisions taken at these mechanisms to the Heads of State during the Annual Summit of the Organization and the instructions given by them to materialize these decisions by the time of the next Summit have paved the way for successful outcomes. With streamlined bureaucratic procedures and enhanced coordination provided by the Secretariat, the Organization could widen and deepen the scope of its agenda. [16] The fact that each Summit of the Organization is dedicated to a specific theme has rendered the cooperation among the Turkic States more structured and focused, with measures taken in a timely way. It should be noted that the themes of all previous Summits, from "economy," "culture-education-science," "transportation and connectivity," "tourism," "media and information," "youth and national sports," "support for SMEs" to "health" were carefully chosen as areas where there is ample room for improved multilateral cooperation. Moreover, the regular meetings within the Organization among the Heads of State of Member States, their foreign ministers and other ministers of areas of existing collaboration, as well as officials of the relevant national authorities have also provided the Member states with a better understanding of one another's working mechanisms, and have resulted in the convergence of national agendas creating a common working culture.

The involvement of all stakeholders in each cooperation area is another asset that fortifies solidarity between the Member and Observer States of the Organization of Turkic States. Hence, in all cooperation areas, private sector actors are actively on board. Furthermore, a series of round tables that the Organization carries out with representatives of civil society, academia and the media has raised awareness about the Organization and its activities. The Secretariat, as a permanent body, is the key player for the institutionalization of cooperation within the Organization, which has been gradually reinforced over the last decade. This body serves to prepare documents and arrange meetings while ensuring regularity in the work of the Organization and acting as a follow-up mechanism.

The Secretariat, as a permanent body, is the key player for the institutionalization of cooperation within the Organization, which has been gradually reinforced over the last decade.

From Institutionalization to Convergence of Foreign Policies among Turkic States

The institutionalized cooperation among the Member States of the Organization of Turkic States has led to the convergence of their policies on several items, including foreign policy. As a result, the Member States have gradually become more vocal in expressing their joint approach on pressing regional and global issues. Thus, in the Organization's Summits, in addition to the declarations signed by the Heads of State, the practice of releasing joint statements has been established.

As a recent example of this practice, the Council of Foreign Ministers convened on September 27, 2021 in Istanbul an extraordinary meeting to discuss the latest developments in Afghanistan and their implications for the Member States of the Organization of Turkic States, upon the invitation of H.E. Mevlüt Çavuşoğlu, Minister of Foreign Affairs of the Republic of Turkey. As the first regional initiative to address such a crucial topic, the meeting was a testament to the Organization's capacity to raise a strong, common voice on an issue of common interest. Thus, at the end of the meeting, the Foreign Ministers of the Member States adopted the "Statement of the Council of Foreign Ministers of the Organization of Turkic States on the Situation in Afghanistan" and decided to remain in consultation and coordination regarding the various aspects and repercussions of developments in Afghanistan, including in the fields of humanitarian efforts, human rights, migration and refugee flows, counter-narcotics and counter-terrorism.[17] This timely meeting transmitted a strong message to the world, not only regarding Afghanistan, but also about the readiness of the Organization to act together when and if necessary.

The "Joint Statement on Egypt" made by the Council of Foreign Ministers in 2013 in Gabala, Azerbaijan, is another example of the Organization's Member States formulating a joint understanding on an issue of common interest. Moreover, on several occasions, the Heads of State of the Organization of the Turkic States reaffirmed in Summit Declarations their shared position on the need to reach a negotiated and mutually agreed-upon political settlement in Cyprus based on existing realities, the political equality of the two peoples and their co-ownership of the island and to express their solidarity with the Turkish Cypriot people. They also reiterated the strongest support for the earliest settlement of the Armenia-Azerbaijan Nagorno-Karabakh conflict, on the basis of the sovereignty, territorial integrity and the inviolability of the internationally recognized borders of the Republic of Azerbaijan. In keeping with this position, the Member States and the Secretariat demonstrated strong solidarity with Azerbaijan during the "44 Days Patriotic War" and supported the liberation of its occupied territories and the restoration of Azerbaijan's sovereignty over them, according to the norms and principles of international law and the relevant UN Security Council Resolutions.[18]

The "Joint declaration of the Member States on the relations between the Organization of Turkic States and the Organization for Security and Cooperation in Europe (OSCE)," voiced by the Organization's chairmanship during the 20th OSCE Ministerial Council annual meeting in Kyiv in 2013, established its commitment to acting together within other international organizations. These steps make it clear that the foreign policy preferences of Member States of the Organization have been converging in areas of mutual interest. Thus, the projects and programs launched within the Organization are supportive of such a convergence. The mechanism of security consultations within the Organization constitutes an important platform to this end.

The junior diplomats training program, launched in 2014, is among the successful activities of the Organization on foreign policy cooperation. This program aims to increase awareness of the common historical, cultural and linguistic ties in the Turkic region while raising a new generation of diplomats who will contribute to the enhancement of Turkic cooperation. More than 150 young diplomats have attended the courses of this visionary program so far. They have since been dispatched throughout the world on diplomatic missions, and have already started to take a leading role when an issue related to the Organization is concerned. Similarly, the internship program initiated in 2016 by the Center for Strategic Studies under the President of Azerbaijan has resulted in the production of a report titled, "Turkic Council Countries: Infrastructure, Trade, Logistics and Transportation," which presents a comprehensive study of the different aspects of connectivity in the Turkic region.[19]

The cooperation process among the official foreign policy research centers of Member States of the Organization of Turkic States, initiated in 2013, has also been very productive in fortifying ties on foreign policy issues.[20] The regular meetings held by these centers and the joint publications prepared with the support of the Secretariat are the outcomes of this cooperation process.[21] In this regard, the special publications prepared by the Secretariat and Center for Strategic Research under the auspices of Turkey's Ministry of Foreign Affairs to honor the 5th, 6th and 7th Summits are "the "Fifth Summit of the Turkic Council: A Rising Actor in Regional Cooperation in Eurasia," "the 25th Anniversary of the Independence of Azerbaijan, Kazakhstan and Kyrgyzstan, and Turkey's Contribution to Development and Cooperation in the Turkic Region" and "The Turkic Council: 10th Anniversary of the Nakhchivan Agreement," respectively. With the support of the abovementioned mechanisms, the Member States of the Organization of Turkic States have become more practiced in acting together on foreign policy issues of common concern.[22]

Fostering Multidimensional Connectivity with a Sectoral Approach

Since the first Summit, launched with the theme of economic cooperation, the Organization of Turkic States has continued to work on empowering the economic structures of the Member States, ensuring their diversification, generating the strong engagement of the private sector, increasing trade relations within the Turkic region and attracting investments to the area. The sectorial approach that the Organization has brought to economic cooperation supports efforts to this end. Multidimensional connectivity in far-ranging areas, from economics, transportation and customs, ICT, energy and tourism, requires such a comprehensive approach.

In addition to the Ministerial and working group mechanisms it mobilizes to address the economy, the Turkic Business Council's activities, and the Business Forums that bring national authorities together with business persons from the region have played an important role in obtaining results in uplifting economic ties among Member States of the Organization of Turkic States. On top of this, the decisions to establish the Turkic Chamber of Commerce and Industry (TCCI) and the Turkic Investment and Development Fund are turning points in boosting cooperation in the field of economy. The TCCI, with its permanent Secretariat hosted by the Union of Chambers and Commodity Exchanges of Turkey (TOBB) in Istanbul, is a concerted effort for the institutionalization of economic relations among the business communities of the Turkic World.[23] Moreover, the TCCI is committed to implementing joint projects, training programs and exchanges of experience in areas of mutual economic interest. The Turkic Business web portal that was previously prepared provides an access point for the active engagement of business actors in the endeavors of the TCCI. The establishment of industrial zones, techno-parks and trade houses proposed by the Secretariat will undoubtedly contribute to the development of economic relations among the Member States. Moreover, once the Turkic Investment and Development Fund is operationalized, it will provide an initial amount of 600–700 million USD to be allocated for the enhancement of the capacities of SMEs and the diversification of economies.[24]

Interconnectivity among the economies of the Member States can be ensured through increased cooperation in the fields of transportation and customs. Based on this premise, the Organization of Turkic States promotes comprehensive cooperation among its Member States in the field of transportation through instruments such as its Ministerial and working group meetings and its Sister Ports initiative.

As a concrete outcome of this cooperation, with the purposes of phasing out the existing impediments in the way of efficient transportation operations and of developing stable, integrated and seamless transportation along the Trans-Caspian International East-West Middle Corridor passing through our countries, the Member States have been working to finalize the "Agreement between Azerbaijan, Kazakhstan, Kyrgyzstan, Turkey and Uzbekistan on the International Combined Transport of Goods." Once entered into force, the agreement will be the first combined transport agreement in the region. As a result of support provided by the Organization of Turkic States, there have already been significant improvements along the Middle Corridor in the last couple of years. Thus, the Secretariat has been vocal about the necessity of tapping the great potential of this route. Accordingly, the reduction of logistical expenses along the corridor and the simplification of customs procedures in the Caspian ports are important outcomes of the efforts that have flourished within the Organization.[25] Moreover, the Secretariat has assisted the Trans-Caspian International Transport Route (TITR) in developing relations with the relevant organizations of the Member States. Through the efforts of the Secretariat, the State Railways of the Republic of Turkey (TCDD) acceded to the TITR agreement in November 2014 and became a full member of the TITR in February 2018.

As a result of support provided by the Organization of Turkic States, there have already been significant improvements along the Middle Corridor in the last couple of years.

Lastly, the Secretariat of the Organization of the Turkic States has had a remarkable stake in the liberalization of transportation between Turkey and Kyrgyzstan. With the support of the Secretariat, the importance of the issue has been better understood by the relevant transport authorities of the Member States. As a result, during the Turkish-Kyrgyz Land Transport Joint Commission Meeting, held on September 15–16, 2021, in Bishkek, important decisions were taken in the field of international road transport to this end. With the signing of the liberalization agreement between the two countries during this meeting, Turkish and Kyrgyz carriers were empowered to carry out bilateral and transit transportation without the restriction of transit documents. This decision is an exemplary step for the liberalization of transportation between other Turkic-speaking States, which has been a long-anticipated step in enhancing their connectivity in logistical and economic means.[26]

As for customs cooperation, which is an inseparable part of collaboration in transport, there is a well-structured working mechanism within the Organization of Turkic States. In addition to the regular working group and ministerial meetings, training seminars have been held on specific topics, and field visits have been carried out at the border gates of the Member States. As a result of these visits, the Organization facilitated the modernization of ten border gates in Kazakhstan by the Customs and Tourism Enterprises (GTI) of TOBB using the build-operate-transfer model. Furthermore, the ongoing collaboration with the World Customs Organization (WCO) is yielding successful outcomes in customs cooperation.

The establishment of working group and ministerial mechanisms for ICT and energy, as two key topics for the region, is an important step in itself to boost cooperation on these issues to foster further interconnectivity. Cyber-security, development of the Trans-Eurasian Information Super Highway (TASIM) project, fortification of fiber-optic infrastructure in the region, implementation of satellite services as well as mutual recognition of certificate on e-signature are among the promising cooperation topics that the Organization will build upon in the field of ICT. As for energy, cooperation in renewable energy with wind, solar and hydraulic power stations, development of means of investment in Member Countries in this field as well as sharing of knowledge in the training of nuclear engineers, nuclear infrastructure, and uranium mining are the priority agenda topics that were carefully chosen to serve for the benefit of all Turkic Member and Observer States.

Multidimensional connectivity also involves enhancing collaboration among the Member States in the tourism sector. One example of this collaboration is the transformation of the historical Silk Road into an attractive tourism destination. The Modern Silk Road Joint Tour Project,[27] as a unique tour package, offers an unprecedented opportunity for tourists to visit Member States of the Organization of Turkic States, and is the cornerstone of its activities carried out in the tourism sector. The Joint Tour Package plays a vital role in increasing the flow of tourists among the Turkic Speaking States, and boosts touristic visits from third parties to these countries.[28] The promotional activities and the feedback gathered during the many international tourism exhibitions indicate a high level of interest in this touristic destination. The documentary prepared by TRT-AVAZ on the project has brought awareness of the tour's natural attractions combined with historical and cultural heritage to broader audiences.

There is no doubt that COVID-19 has negatively impacted the tourism sector all over the world. Facing this reality, Tourism Ministers of the Member and Observer States of the Organization of Turkic States convened on June 23, 2020 to coordinate their efforts in the fight against COVID-19 in the tourism sector by sharing the measures on inspection, sanitation, certification and safety applied by the Member States within the Organization. They also consented to launch new online training programs on certain topics to aid in fighting the pandemic. Beyond the measures related to the pandemic, projects such as the Silk Road Tourism Capitals, Tourism Week and the initiation of a Silk Road visa are among the promising projects within this cooperation area.

In addition to the abovementioned sectors, the Organization works to expand the scope of the collaboration that already embraces health, agriculture, environmental protection and preparedness for natural disasters. Taking into account the needs of its Member and Observer States as well as both regional and global developments, the Organization updates and shapes its agenda of collaboration with a dynamic approach.

Enhancing People-to-People Cooperation

The common culture, language and history of the Turkic States are found at the heart of people-to-people cooperation within the Organization of the Turkic States. Culture, diaspora, media and information, education, youth and sports constitute the most important elements of this collaboration. Thus, the Organization attributes the utmost importance to increasing people-to-people contacts and spreading common Turkic values in the Turkic region.

Culture is the cement of collaboration within the Turkic World. The Organization supports the activities of all relevant actors to this end. In this regard, besides its regular meetings of Ministers of Culture of the Turkic Speaking States, TURKSOY's Cultural Capital of the Turkic World initiative constitutes a flagship event to highlight and celebrate cultural cooperation in the Turkic region. The TCHF is actively expanding ties between Turkic-speaking peoples to preserve and develop their rich and diverse cultural heritage. While doing so, it carries out numerous activities aimed at enhancing ties among several segments of Turkic societies, including among women and children.

In addition to cultural cooperation among the Turkic-speaking people living in the Member States, enhancing coordination and cooperation among the Turkic-speaking diasporas and the diaspora institutions of the Member States has continued to be a priority for the Organization of Turkic States since its establishment. Based on the Turkic Speaking Diaspora Joint Activity Strategy of the Organization prepared by the relevant institutions of the Member States in line with their joint action plans, this cooperation process strengthens the spirit of solidarity among the institutions responsible for diaspora issues. It also consolidates the ties among nationals from Turkic States living abroad and creates further awareness through common Turkic values. In addition, Turkic Diaspora Forums aim at enhancing ties among Turkic-speaking diasporas.[29]

In addition to cultural cooperation among the Turkic-speaking people living in the Member States, enhancing coordination and cooperation among the Turkic-speaking diasporas and the diaspora institutions of the Member States has continued to be a priority for the Organization of Turkic States since its establishment.

Media, with all its components, is a cross-cutting key tool to empower Turkic cooperation. The MoUs among the national TV channels and official news agencies, as well as the public broadcasting institutions of the Member States of the Organization of Turkic States, lay the foundation of cooperation in this field. The decision regarding the establishment of a Joint FTP Pool where viewers can download programs and videos on agreed-upon categories constitutes an important part of this cooperation process. Furthermore, the decision to prepare documentaries, short films and videos on prominent Turkic figures is another important measure intended to raise awareness about the rich cultural and historical heritage of the Turkic world. The TRT Avaz channel, with its insightful programs on the Turkic world, has already been acting as the common channel of the Turkic-speaking states.[30]

Education is the *sine quo non* for the enhancement of cooperation among the Turkic speaking people. The preparation of common history, geography and literature books by the Turkic Academy with the support of the Secretariat of the Organization of Turkic States for the young generation of the Turkic states is itself a significant achievement. It is also instrumental in instilling a collective conscience in Turkic youth. Once the preparation of these books is finalized by the Turkic Academy, various school materials will be available to benefit Turkic youth in better understanding their commonalities. As an outcome of the efforts within the Organization, an elective course covering the period from antiquity until the 15th century has been already issued for 8th grade students in Azerbaijan, Kazakhstan and Turkey and has reached almost 10,000, 15,000 and 50,000 youngsters in these respective countries.

The exchange program for high school students within the Organization of Turkic States also serves as an important tool for raising next generations who are fully aware of their common roots, languages and history. The exchange program for high school educational professionals and the Sister Schools Project that are on the agenda within this cooperation area will certainly contribute to the same purpose. Moreover, the establishment of the Turkic University Union in 2013 within the Organization of Turkic States with the participation of universities from the Member States has generated a comprehensive cooperation process at the level of higher education. In a short period of time, the number of universities involved in this cooperation reached 22, including a university from Hungary. The Orkhon Process, which is the exchange program for academic and university students within the Turkic

University Union, started its first pilot project in academic year 2017–2018. Since then, there has been a high volume of student mobility among member universities. The Student Council of the Union has also been instrumental in seeding a cooperation culture in the minds of university students through the realization of various activities.[31]

The sizable young population of the Turkic States constitutes the key target group that will enhance Turkic cooperation in all its dimensions; since 2015, the Organization of Turkic States has organized youth activities, including youth camps, festivals and forums. It provides platforms where Turkic youngsters can learn from each other and generate a common vision for the future. So far, these platforms have welcomed more than 3,000 young participants coming from the Turkic Member and Observer States, as well as from other regional countries. The establishment of the Youth Platform of the Organization of Turkic States in 2017 is a milestone in increasing cooperation and coordination between young people from the Turkic States through different projects and activities. This platform brings them together under one roof and offers them the possibility of representation in regional and international youth platforms. As the first activities of this platform, three Young Leaders Forums were organized in Nakhchivan in 2018, in Turkistan in 2019 and in Osh in 2021 with broad participation from the region.[32] These forums were instrumental in bringing youngsters together, sharing the same history, culture and language, and preparing a future generation of leaders with an increased sense of awareness of regional problems.

Sport is an area that also cements cooperation among young people, channeling their energy and dynamism toward common causes. With this in mind, the first university sports games of the Organization of Turkic States (Turkic Universiade) were successfully hosted in Baku in 2018 with the participation of 400 athletes in 7 branches. Because of its emphasis on shared culture and history, the Turkic Organization supports the revival and protection of traditional sports. Thus, the Organization significantly contributed to the preparation and realization of the three World Nomad Games initiated by and hosted in Kyrgyzstan in 2014, 2016 and 2018.[33] The Heads of State of the Organization of Turkic States attended the opening ceremony of the 3rd World Nomad Games, which coincided with the 6th Summit of the Organization of

Turkic States held on September 3, 2018 in Cholpon-Ata, Kyrgyzstan. Over 4,000 athletes from about 100 countries, and thousands of audience members from around the world attended the World Nomad Games, for which there is growing global interest. The UN General Assembly has already recognized the importance that the Games place on intercultural dialogue and their valuable contribution to promoting social cohesion, peace and development.[34] Secretariat of the Organization, Ministry of Youth and Sports of Turkey and World Ethnosport Confederation (WEC) are all participating in the organizing committee of the 4th Games to be hosted by Turkey in 2022, under the leadership of the WEC. The Organization and the WEC, based on the MoU between them, closely cooperate in developing Turkic ethno-sports.

The above-mentioned cooperation areas are tangibly contributing to enhancing people-to-people cooperation in the Turkic region. As long as Turkic-speaking people directly benefit from the outcomes of the projects carried out by the Organization of Turkic States in different sectors, this cooperation will be further bolstered.[35]

Capacity-Building and Vocational Training as a Cross-cutting Responsibility

Capacity-building and vocational training are significant elements of international development cooperation. Expressing its firm commitment to the achievement of the UN 2030 Agenda for sustainable development, the Organization of Turkic States carries out capacity-building and vocational projects in different areas. In addition to the training of young diplomats mentioned above, the Secretariat facilitates the implementation of projects in the fields of economy, transport, customs, tourism, media, diaspora and health, led by its Member States, through experience- and knowledge-sharing. It also benefits from the expertise of the international organization in most of these areas.

The capacity-building programs undertaken by the Ministry of Trade of the Republic of Turkey, together with Turkey's Small and Medium Enterprises Development Organization (KOSGEB) for its counterparts in the Organization of Turkic States on investment statistics and investment climate trainings, combined with information- and experience-sharing programs in the field of development of SMEs, have started to yield tangible results. Furthermore, the joint publication of the Organization and the Statistical, Economic and Social Research and Training Centre for Islamic Countries (SESRIC), titled "Trade and Investment Relations among the Turkic Council Member States,"[36] published in 2021, is important capacity-building research that will serve to improve economic ties among the Turkic States in a multilateral way.

In the field of customs, the Organization of Turkic States has so far organized several regional and international workshops on "Post Clearance and Risk management," the "Authorized Economic Operator (AEO) System," "Customs Transit Facilitation" and the "Electronic TIR System" in Ankara, Astana, Baku, Bishkek and Izmir through the support of relevant authorities from its Member States. During these events, the Organization has closely collaborated with international organizations and platforms such the United Nations Economic Commission for Europe (UNECE), the World Customs Organization (WCO) and the International Road Transport Union (IRU). The Organization of Turkic States is also working for the expansion of the e-TIR pilot project between Uzbekistan and Kazakhstan, which aims to digitalize the system of transport of goods and allow holders to carry cargo without the need for customs control procedures at the borders of other Member States.

As for tourism, the Ministry of Culture and Tourism of the Republic of Turkey carried out vocational training programs on the service sector for the tourism employees of the other Member States in coordination with the relevant Ministries and tourism associations. As a result, over the course of 2014–2017, more than 1,000 tourism employees in Azerbaijan, Kazakhstan and Kyrgyzstan were trained, of whom 50% were women. This capacity-building initiative became the subject of several UN reports, and is considered a best practice for the achievement of Sustainable Development Goals (SDGs). Moreover, the Organization of Turkic States has contributed to the development of relations with its Member States and the UN World Tourism Organization, especially in the field of capacity-building. In this regard, the Organization contributed to the adoption of international standards in the field of tourism by all Member States. The fact that the tour agencies involved in the Modern Silk Road Joint Tour Package project signed "the Code of Ethics of the UNTWO" constitutes an example in this direction.[37]

Another tangible capacity-building activity prevails in the field of media cooperation. The Social Media Training Program of the Organization of Turkic States was organized in Istanbul on July 29–30, 2021 by the Directorate of Communications of the Presidency of the Republic of Turkey. During the training program, which was attended by 100 participants from the Member States, issues related to the use of social media, combating disinformation, addressing cyber-security threats and Turkey's experience in these fields were discussed, and a decision was taken to continue these trainings in a regular way. Similarly, the capacity-building trainings carried out for diaspora institutions in Berlin and New York in 2019, attended by more than 200 participants, were also instrumental in the exchange of information and knowledge on the working system for diaspora affairs of the Member States.[38] As a concrete outcome, the initiatives generated for cooperation among the diasporas of the Turkic States within the Organization paved the way for the signing of bilateral agreements between Azerbaijan, Turkey and Kazakhstan.

As for cooperation in the field of health, the first face-to-face Vaccine Workshop of the Health Scientific Group of the Organization of Turkic States, hosted by the Ministry of Health of the Republic of Turkey with the coordination of the Secretariat on August 24, 2020 in Izmir, was a timely capacity-building event. Despite the challenges posed by the pandemic, this event brought together medical professionals from the Member States and provided a forum for the exchange of knowledge about COVID-19 and the vaccine development process. Moreover, within the framework of a MoU on cooperation between the Organization of Turkic States and the UN WHO, the two organizations are planning to join forces in exchanging information, including methodological and regulatory documents on public health, and in ensuring sanitary and epidemiological well-being; they plan to hold joint events for capacity-building in areas of mutual interest.

As indicated above, capacity-building and vocational training in several areas rest at the core of the activities of the Organization of Turkic States. This approach paves the way for the needs assessment of the Member States, and facilitates the putting forward of adequate responses to these needs through the mutual exchange of information, knowledge and experience.[39]

Support of the Organization of Turkic States for International Cooperation

Regional cooperation is essential for the enhancement of international collaboration. In line with this perspective, the Organization of Turkic States has succeeded in building strong ties with regional and international organizations in a short period of time. Becoming an observer to the Economic Cooperation Organization (ECO) in 2012, the Organization is making considerable efforts to obtain observer status at the UN General Assembly and the Organization of Islamic Cooperation (OIC), and has established fruitful relations with the specialized institutions of these organizations. MoUs signed with the UN Development Program (UNDP), the UN Office for South-South Cooperation (UNOSSC), the United Nations Alliance of Civilization (UNAOC), the UN World Tourism Organization (UNWTO) and the UN WHO constitute the road map for relations with the UN and its specialized institutions. The international conference co-organized with the UNDP in 2015 on the role of informational technologies for development, attended by more than 150 high-level experts from 15 regional countries, and the global event on the role of youth to prevent violent extremism co-realized with UNAOC with 300 young leaders coming from 40 countries, are just a few examples of how the Organization has partnered side by side with the UN to address global concerns. Furthermore, the support that the Organization provided to the UNOSSC helped to make the 2017 Global South-South Development EXPO hosted by the Turkish government in Antalya a successful event, in which more than 800 high-level officials from 120 countries participated. In addition, the activities that the Organization of Turkic States has organized on SDGs with the UNDP and UNWTO have reiterated its commitment to the successful implementation of the 2030 Agenda for sustainable development. Thus, the UNOSSC report, titled "South-South in Action: How the Turkic Council Uses South-South Cooperation to Promote Regional and Global Development,"[40] launched in 2017 in New York on the margins of the 72nd session of the UN General Assembly outlines and praises the work of the Organization of Turkic States in this area.

Relations with the OIC have equally improved in recent years. The MoU signed with this international organization supports the bid of

Organization of Turkic States to obtain observer status. The cooperation with SESRIC on economic issues, and the Islamic Cooperation Youth Forum (ICYF) on youth-related areas, fortify the ties between the Organization and the OIC. In addition to this, the working relations built between the Organization and the OSCE have proved the former's readiness and firm will to contribute to stability and prosperity in Eurasia. The regular participation of the Secretary General in the annual OSCE Ministerial Council meeting upon the invitation of the OSCE Chairmanship is an essential practice that the Organization of Turkic States values to this end.

The strong ties between the Organization of Turkic States and regional and international partners enable the Organization to closely track global agendas and incorporate them in its work. In addition to its cooperation with UN specialized agencies, its close ties with the World Customs Organization (WCO), the International Centre for Sports Security (ICSS), the Sports Integrity Global Alliance (SIGA) and the WEC yield tangible outcomes in this direction. Moreover, the contacts that the Organization has initiated with a wide range of organizations from the European Union, the Black Sea Economic Cooperation (BSEC), the Conference on Interaction and Confidence-Building Measures in Asia (CICA) to the Association of Southeast Asian Nations (ASEAN) constitute additional testimony to its active collaboration with actors of various regions.

Organization of Turkic States also engages actively in international development assistance. Within this framework, the ongoing cooperation between the Organization and the Turkic Cooperation and Coordination Agency will be instrumental in implementing joint developmental projects in the region. All of these relations with external parties have reconfirmed the role of the Organization of Turkic States as a promoter of partnerships and collaboration on global development topics that require joint engagement while contributing to the development of inter-regionalism in Eurasia.[41]

The strong ties between the Organization of Turkic States and regional and international partners enable the Organization to closely track global agendas and incorporate them in its work.

Conclusion

As we witnessed in the case of the COVID-19 pandemic, the Organization of Turkic States is a regional cooperation mechanism capable of adapting itself and responding meaningfully to emerging conditions. With its fast decision-making process, practical working mechanisms and selective cooperation areas, the Organization can mobilize itself to answer to the needs of its Member and Observer States and their people. Its multi-faced approach to cooperation aligns with the miscellaneous nature of these needs. The Organization's active role in converging foreign policies of the Turkic States on issues of common interest, fostering multidimensional connectivity with a sectoral approach from economy to tourism, and its firm assistance to increasing people-to-people contacts constitute the important assets that the Organization brings to Turkic cooperation. Moreover, its contribution to the capacity-building of its Member States in areas including but not limited to diplomacy, economy, transportation, customs, tourism, media, diaspora and health services benefit not only its Member and Observer States but also their people. The Organization's growing relations with the UN and its specialized agencies as well as other regional and international actors constitute a testimony to its active role in global governance. With these instruments in its toolkit, the Heads of States of the Turkic States adopted the "Turkic World Vision 2040" during the 8th Summit of the Organization of Turkic States hosted by Turkey on November 12, 2021 as a strategic document to draw the road map of cooperation for the next decade. This is another proof of the Organization's ability to evolve responsively to face the needs and recognize the opportunities of the upcoming decade.

With its fast decision-making process, practical working mechanisms and selective cooperation areas, the Organization can mobilize itself to answer to the needs of its Member and Observer States and their people.

David Mitrany spoke truly when he stated that an international organization can be functional when its activities are commensurate with the conditions under which it has to operate, and when these activities meet the needs of the moment. This perspective is certainly supportive of the development of multilateral cooperation and multilateralism. The Organization of Turkic States' achievements in various areas since its establishment run in close parallel with this understanding. The Organization catches the spirit of the times, and shapes its agenda and carries out its functions accordingly. Being a resilient member of international community requires nothing less. The Secretariat, as the permanent body of the Organization, should continue its tireless efforts to turn the idea of Turkic cooperation into reality. The political will displayed at the level of the Heads of State of the Turkic States to deepen their ongoing multilateral cooperation should be reflected in the actions of all stakeholders. We cannot predict the future, but we can prepare ourselves for its management. In this context, the Organization of Turkic States is equipped with the adequate means to remain a functional international organization meeting today's needs as well as tomorrow's, based on the *motto,* "together we are stronger".

Endnotes

1 Robert O. Keohane, "Multilateralism: An Agenda for Research," *International Journal*, Vol. 45, No. 4 (Autumn 1990), p. 731.

2 Union of International Associations (ed.), *Yearbook of International Organizations 2020–2021*, Vol. 4, Leiden: Brill, 2020, p. 25.

3 David Mitrany, *A Working Peace System: An Argument for the Functional Development of International Organization*, London: Royal Institute *of* International Affairs, 1943, p. 35.

4 Klaus Schwab, "Globalization 4.0: What Does it Mean?" *The World Economic Forum*, November 5, 2018, https://www.weforum.org/agenda/2018/11/globalization-4-what-does-it-mean-how-it-will-benefit-everyone/.

5 Tara Rao, "Rising Nationalism in Europe and Asia in the Age of COVID19," *Observer Research Foundation*, September 1, 2020, https://www.orfonline.org/research/rising-nationalism-in-europe-and-asia-in-the-age-of-covid19-72587/.

6 Henry A. Kissinger, "The Coronavirus Pandemic Will Forever Alter the World Order," *The Wall Street Journal*, April 3, 2020, https://www.wsj.com/articles/the-coronavirus-pandemic-will-forever-alter-the-world-order-11585953005.

7 Meltem Müftüler Baç, "Küresel Salgın Tehdidine Karşı Küresel Sistem," in Ufuk Ulutaş (ed.), *Covid-19 Sonrası Küresel Sistem: Eski Sorunlar, Yeni Trendler*, Ankara: SAM Yayınları, 2020, p. 20.

8 Turan Gafarlı, "Turkic Council's Growing Role in Tackling Crises of 2020," *Anadolu Agency*, September 10, 2020, https://www.aa.com.tr/en/analysis/analysis-turkic-councils-growing-role-in-tackling-crises-of-2020/1968547.

9 "Speech at the Turkic Council Extraordinary Summit," *WHO*, April 10, 2020, https://www.who.int/director-general/speeches/detail/the-cooperation-council-of-the-turkic-speaking-states---10-april-2020.

10 For further information on these meetings, see https://www.turkkon.org.

11 For the details of the MoU, see https://www.euro.who.int/en/about-us/regional-director/news/news/2020/09/whoeurope-and-the-turkic-council-sign-a-memorandum-of-understanding-strengthening-new-partnerships-in-the-who-european-region.

12 Pelin Musabay Baki, *Cooperation among the Turkic Speaking States and the New Regionalism*, unpublished Ph.D. thesis (in French), Galatasaray University, Istanbul, 2020, Chapter III, p. 420–429.

13 Altay Atlı, "Turkic Council and Limits to Ethnic Unity in Eurasia," *Asia Times*, September 14, 2021, https://www.asiatimes.com/2015/09/article/turkic-council-and-limits-to-ethnic-unity-in-eurasia/.

14 Teoman Ertuğrul Tulun, "Macaristan'ın Türk Dili Konuşan Ülkeler İşbirliği Konseyi'ne Katılımı," *AVIM*, September 14, 2018, https://avim.org.tr/tr/Analiz/MACARISTAN-IN-TURK-DILI-KONUSAN-ULKELER-ISBIRLIGI-KONSEYI-NE-KATILIMI.

15 Merve Aydoğan, "Interview with Secretary-General of the Turkic Council Baghdad Amreyev," *Anadolu Agency*, March 30, 2021, https://www.aa.com.tr/en/world/turkic-council-eyes-forming-united-states-of-turkic-world/2192579.

16 Pelin Musabay Baki, "Avrasya'da Bölgesel İşbirliği Sürecinden İşbirliği Mekanizmasına: Türk Konseyi," *Bilge Strateji*, Vol. 6, No. 11 (2014), pp. 157–158.

17 For the full text of the "Joint Statement of the Council of Foreign Ministers of the Cooperation Council of Turkic Speaking States on the Situation in Afghanistan," September 27, 2021, see https://www.turkkon.org/en/haberler/statement-of-the-council-of-foreign-ministers-of-the-coopertion-council-of-turkic-speaking-states-on-the-situation-in-aghanistan_2344.

18 Kenan Kıran, "Turkic Council Aims to Boost Cooperation among Turkic World: Hajiyev," *Daily Sabah*, September 3, 2021, https://www.dailysabah.com/politics/diplomacy/turkic-council-aims-to-boost-cooperation-among-turkic-world-hajiyev.

19 Mahir Humbatov & Kazim Sari, "Turkic Council Countries: Infrastructure, Trade, Logistics, and Transportation," *Center for Strategic Studies*, Vol. 18–19, November 2017, pp. 12–13.

20 For the "Joint Statement of the Council of Foreign Ministers regarding events in Egypt," August 16, 2013, see https://www.turkkon.org/en/haberler/joint-statement-of-the-council-of-foreign-ministers-regarding-events-in-egypt_36.

21 For these publications, see https://www.turkkon.org/en/yayinlar.

22 Musabay Baki "Avrasya'da Bölgesel İşbirliği Sürecinden İşbirliği Mekanizmasına," pp.151-152.

23 Ufuk Ulutaş, "The Turkic Council on the 10th Anniversary of the Nakhchivan Agreement: A View from Turkey," in Ceyhun Şahverdiyev & Dr. Cavid Veliyev (eds.), *The Turkic Council on the 10th Anniversary of the Nakhchivan Agreement*, Baku: Turkic Council and Air Center, 2019, p. 121.

24 "Turkic Council to Launch $700 Million Investment Fund," *Hürriyet Daily News*, June 27, 2019, https://www.hurriyetdailynews.com/turkic-council-to-launch-700-million-investment-fund-144527.

25 Kurşad Zorlu, "Şimdi Orta Koridor Zamanı," *Habertürk*, May 5, 2020, https://www.haberturk.com/yazarlar/prof-dr-kursad-zorlu/2673011-simdi-orta-koridor-zamani.

26 "Kırgızistan ve Türkiye, Orta Asya ve Türk Dünyasında Örnek Alınacak İlk Serbestleştirme Adımını Attı," *Uluslararası Nakliyeciler Derneği*, September 17, 2021, https://www.und.org.tr/medya-detay/undden-haberler/kirgizistan-ve-turkiye-orta-asya-ve-turk-dunyasinda-ornek-alinacak-ilk-serbestlestirme-adimini-atti.

27 For further information, see http://www.modernsilkroadtour.com/.

28 Eli Hadzhieva, "Silk Road, Revived," *Skylife Magazine*, April 2018, https://www.skylife.com/en/2018-04/the-silk-road-revived.

29 Farid Shafiev, "The Turkic Council on the 10th Anniversary of the Nakhchivan Agreement," in Ceyhun Şahverdiyev & Dr. Cavid Veliyev (eds.), *The Turkic Council on the 10th Anniversary of the Nakhchivan Agreement*, Baku: Turkic Council and Air Center, 2019, p. 73.

30 Firuza Vahid, "Baghdad Amreyev: Cooperation in Media Field is One of the Most Important Issues in Turkic Council," *APA*, April 10, 2021, https://apa.az/en/xeber/media-news/Baghdad-Amreyev-Cooperation-in-media-field-is-one-of-the-most-important-issues-in-Turkic-Council-346516.

31 Shafiev, "The Turkic Council on the 10th Anniversary of the Nakhchivan Agreement," p. 69.

32 Zhanna Nurmaganbetova, "Turkic Council Young Leaders Forum Held in Turkestan," *KAZINFORM*, April 23, 2019, https://www.inform.kz/en/turkic-council-young-leaders-forum-held-in-turkestan_a3519879.

33 For further information, see http://worldnomadgames.com/en/page/About-the-WNG/.

34 Nicholas Muller & Chris Rickleton, "Kyrgyzstan Hosts Third Nomad Games, and Passes the Torch," *Eurasianet*, September 7, 2018, https://eurasianet.org/kyrgyzstan-hosts-third-nomad-games-and-passes-the-torch.

35 Musabay Baki, *Cooperation among the Turkic Speaking States and the New Regionalism*, pp. 487–489.

36 Kenan Bağcı, Cem Tintin & Erhan Türbedar, *Trade and Investment Relations among the Turkic Council Member States*, Istanbul: Turkic Council Publications, March 2021.

37 Astrid Schnitzer-Skjonsberg, *South-South in Action, Turkic Council: How the Turkic Council uses South-South Cooperation to Promote Regional and Global Development*, New York: UNOSSC Publications, 2017, pp. 37–39.

38 For further information, see https://www.turkkon.org/en/haberler/turkic-councils-health-scientific-group-vaccine-workshop_2048.

39 Musabay Baki, *Cooperation among the Turkic Speaking States and the New Regionalism*, p. 437.

40 Schnitzer-Skjonsberg, *South-South in Action*, p.51.

41 Musabay Baki, *Cooperation among the Turkic Speaking States and the New Regionalism*, p. 473.

ARTICLE

The Foundation and Development of Turkey's Defense Industry in the Context of National Security Strategy

Hüsnü ÖZLÜ [*]

Abstract

This article aims to provide an overview of the development of Turkey's defense industry from a historical perspective within the context of the country's national security strategy. Due to its unique geostrategic location and deep-rooted historical, socio-political and economic relations with the countries of its neighboring regions, it is appropriate for Turkey to possess a multidirectional foreign policy and defense concept. Since 1980, Turkey has been taking impressive steps to build a modern defense industry, launching initiatives at the national and international level, leading to the emergence of a new national defense industry strategy and defense concept for the 21st century.

Keywords

Turkish defense industry, national security, military strategy, Turkish armed forces, defense spending.

[*] Professor, National Defense University, Alparslan Defense Sciences Institute, Ankara, Turkey. E-mail: husnuozlu@hotmail.com. ORCID: 0000-0002-8724-4061.

Received on: 07.04.2021
Accepted on: 26.10.2021

Introduction

Turkey sits in one of the most strategic positions in the world, given its unique geographical location. The Anatolian peninsula, situated between the Asian and European continents, is regarded as a connection point between Western and Eastern civilizations. Partly for this reason, Anatolia has a rich history and cultural legacy, and has been constantly exposed to great threats. Turkey is thus an important center in geopolitical and geostrategic terms; it sits right in the middle of several conflict zones that are important for the shaping of global geopolitical balances, such as the Middle East, the Balkans and the Caucasus.[1] At the same time, Turkey is an important country on NATO's southern flank, which further contributes to its strategic value in the eyes of the Western world.

Geographical location, including proximity to significant regions and power centers, defines the value of a country's geopolitical importance as well as its status in the world. In this sense, each of the geographical characteristics that constitute Turkey's geopolitical power are of great importance, and Turkey's threat perceptions emerge in relation to these characteristics.[2] Turkey must closely monitor and address the geopolitical and security-related issues that arise from its geographical location, including issues arising from other continents like Europe, Asia and Africa; the need to address such a broad array of considerations is a decisive factor in the formulation of its defense policy. Turkish leaders must always be well-prepared, since tackling symmetrical and asymmetrical threats and risks requires them to plan and implement both traditional and non-traditional defense options in a holistic manner.[3]

States' national security policies' are determined foremost by their national interests and objectives. It is necessary to develop both soft power (political, diplomatic and psychological) and hard power (military and economic) capacity in order to attain these national objectives. The protection of national interests and the achievement of national objectives requires states to develop political, diplomatic, economic and psychological power.[4] The national security policy prepared by the government determines the security precautions that need to be taken by a state against internal and external threats. Thus, a state's national security policy is of utmost importance.[5]

Within the framework of national security policy, it is essential for the Turkish Armed Forces (TAF), whose duty is to defend the Turkish territories—which have faced so many threats for centuries—to be served and supported by a domestic, national defense industry that provides it with cutting-edge military equipment and modern arms.

Turkey's national security policy is stated openly in the "White Paper" prepared by the Ministry of Defense. As defined in Law No. 2947, national security "refers to the protection and utilization of the state's constitutional order, national existence, integrity, all interests including those that are political, social, cultural and economic, and contractual law in the international scene against all kinds of internal and external threats." In Law No. 2945 in the same publication, national security policy is defined as follows: "a policy that includes principles regarding the internal, external and defense courses of action put forward by the Council of Ministers within the framework of the views determined by the National Security Council in order to ensure national security and achieve national goals."[6]

Within the framework of national security policy, it is essential for the Turkish Armed Forces (TAF), whose duty is to defend the Turkish territories—which have faced so many threats for centuries—to be served and supported by a domestic, national defense industry that provides it with cutting-edge military equipment and modern arms.

Countries formulate their defense policies in line with their strategy documents, and organize and manage their plans for defense targets according to their predetermined objectives;[7] the views regarding the formulation and implementation of Turkey's national security policy are determined by the National Security Council. The principles, priorities and main programs of the armed forces regarding personnel, intelligence, operations, organization, education, training and logistics requirements are prepared accordingly. The national military strategic concept is developed by determining the programs and priorities related to military requirements that are based on the national security policy and national objectives. In this regard, meeting the present and future needs of the armed forces and managing a successful defense economy are coordinated with other relevant authorities. Within the framework of the defense policy and according to the predetermined principles, priorities and programs, the defense industry, health services, construction/real estate and infrastructure services are provided along with weapons, tools, equipment, as well as all kinds of logistical requirements. [8]

The purpose of this article is to discuss the establishment and development of Turkey's defense industry in accordance with its national security strategy. To this end, the first section will focus on Turkey's efforts to build a defense industry, especially in the early Republican period, while the second section aims to shed light on the more recent development of the country's defense industry strategy and policy. The last section discusses the modernization of the defense industry and defense spending in Turkey in the 1980–2020 period.

Efforts to Build a Defense Industry in the Early Republican Period

Strategy is the use of combat to achieve the goal of war. Carl von Clausewitz defines strategy as the combination of all methods and means implemented and followed in order to achieve a predetermined goal. [9] Grand strategy is the theory of how a state can ensure its security in accordance with its political-military purposes and means. Grand strategy should both address potential threats against a state in a concrete way, and anticipate the necessary political, military and economic measures that should be taken to counter these threats.[10] In this sense, the relationship between Turkey's tangible and intangible resources, and those of its neighbors and non-neighboring regional powers are the determining factors of its grand strategy.[11] In terms of defense industry strategy, this means that the procurement of all kinds of weapons and ammunition required by the armed forces should be made from the national defense industry.

The defense industry, also known as the war industry, is a group of enterprises that design, develop and produce the weapon systems necessary for a state's armed forces. During the period of the rise of the Ottoman Empire, the Turkish war industry was considered to be ahead of its time. The remarkable improvement in Ottoman cannon production achieved during the reign of Fatih Sultan Mehmet in the mid-15th century should be particularly emphasized in this regard. However, this superiority ended due to the acceleration of technological developments in Europe starting in the 18th century; by the end of 19th century, the Ottoman Empire lagged behind the European states in terms of war industry.[12]

Nevertheless, by the middle of the 19th century, the Ottomans had built some new arms factories, and had added new facilities to the already functioning factories in the Tophane, Zeytinburnu and Bakırköy districts of Istanbul. As the Ottoman Empire had to fight many wars, it allocated a sizable budget to arms production in the 19th century, and the activities of the factories in Tophane became even more important. A significant shortage of supplies arose in the important raw materials needed for the arms industry, such as copper, iron and steel, as these materials were largely imported from other countries.

By the beginning of the 20th century, the European states had made significant advances in arms technology. Private companies in Germany, Austria, Britain, France and the U.S. in particular pioneered rapid development in arms technologies, and the use of electric, automatic looms in European and American arms factories quickly overshadowed the Ottoman Empire's relatively more primitive mode of arms production.[13]

In terms of the Ottoman army's organization structure, the Ministry of War was established on July 22, 1908; a year later, the General Directorate of Warfare Production (İmalât-ı Harbiye-i Umumiye Müdürlüğü) was established, and the entire arms industry in the empire was placed under the authority of this newly founded directorate.

In terms of the Ottoman army's organization structure, the Ministry of War was established on July 22, 1908; a year later, the General Directorate of Warfare Production (*İmalât-ı Harbiye-i Umumiye Müdürlüğü*) was established, and the entire arms industry in the empire was placed under the authority of this newly founded directorate. During the years of the First World War, the military requirements of the army were largely met from domestic sources and factories operating under the General Directorate.

Under the conditions of the armistice signed at the end of WWI in 1918, the production of arms in the factories affiliated with the General Directorate was stopped; however, with the start of the Turkish War of Independence one year later, the materials of these factories in Istanbul were smuggled to Anatolia and their facilities were reorganized on March 19, 1920. As a result, some manufacturing and repair workshops were opened in Anatolian cities such as Ankara, Eskişehir, Kayseri, Konya and Erzurum.

These factories and facilities were linked to the General Directorate of Military Factories (*Askeri Fabrikalar Umum Müdürlüğü*), which was re-established as a brand new organization on January 10, 1921, and thus started working in a more systematic way. Following WWII, the war industry, which had previously been united under the roof of this General Directorate, was placed under the Mechanical and Chemical Industry Corporation (MKE) founded in 1950.

During the years of the Turkish War of Independence, the activities of the General Directorate of Warfare Production were mainly concentrated in Ankara and the surrounding cities. The military factories working under the directorate in this period could be placed in three categories based on the product they produced: arms, ammunition or chemical materials. The first group included the Ankara Arms Factory, the Kırıkkale Rifle Factory and the Kırıkkale Cannon Factory.[14] The ammunition factories, which mainly produced bullets, cartridges, capsules, fuses and training bullets used in light and heavy weapons to complement arms production, included the Kırıkkale Ammunition Factory, the Ankara (Gazi) Cartridge Factory and the Silahdarağa Cartridge Factory, which later merged with the Kayaş Capsule Factory in 1968. Chemical production factories included the Kırıkkale Gunpowder Factory, the Bakırköy Gunpowder Factory, the Elmadağ Barut Factory, the Konya Güherçile Kalhane and the Mamak Gas Mask Factory. After the proclamation of the Republic of Turkey in 1923, some of these military factories were restructured, but the General Directorate of Military Factories still played a crucial role in the development of the Turkish arms industry. In addition, the Ministry of National Defense, which was restructured in 1923 in the early Republican period, played an important role in the supervision of the activities of these factories.

The first factory to be founded by the private sector in the early years of the Republic belonged to Şakir Zümre Bey, who had settled in Turkey right after the proclamation of the Republic; Bey's factory served to meet the needs of the TAF for a long time. Another important figure in terms of the private sector's efforts in the Turkish war industry was Nuri Killigil, who was asked by the Turkish government to establish a pistol factory in 1942 in order to assist the Turkish army during WWII.[15] This factory received various incentives and support from the Ministry of National Defense.[16]

The new Turkish state had ambitious plans in the naval sphere from the very early years. Many warships were purchased and/or ordered from the national budget during the Atatürk period. Some of these include the Adatepe, Kocatepe, Tınaztepe and Zafer destroyers; Doğan, Martı, Deniz Kuşu assault boats; and Birinci İnönü, İkinci İnönü, Dumlupınar, Sakarya, Gür, Saldıray, Atılay, Yıldıray and Batıray submarine ships. Efforts to build a new shipyard began in Gölcük as early as 1926. Until the early 1960s, only the Haliç and Camialtı shipyards and the Taşkızak and Gölcük military shipyards built the small, auxiliary-class warships used by the Turkish Naval Forces. Meanwhile, an agreement was made with Germany in 1936 for the construction of four submarines for the Turkish Naval Forces. Eventually, the submarines "Atılay" and "Yıldıray" were put into service on August 14, 1937 and September 9, 1937, respectively. Re-established in 1941, the Taşkızak shipyard has accelerated its development, especially since 1960, and has continued to meet the needs of the Turkish naval forces with activities in the fields of modernization and installation.[17]

Aviation efforts in Turkey started in 1911 during the Turkish-Italian war in Tripoli. On June 11, 1911, an air commission was established under the second branch of the Inspectorate of Science and Combat Garrisons (*Kıtaat-ı Fenniye ve Mevaki-i Müstahkeme*), which paved the way for the foundation of the Turkish Air Forces. After the proclamation of the Republic, the Turkish Airplane Association (*Türk Tayyare Cemiyeti*) was established on February 16, 1925.

In the early years of the Republic, a decision was taken by the government upon the personal instructions of Atatürk to build an airplane factory in Kayseri, and the German Junkers Company was contacted for this purpose. Due to the emergence of a positive atmosphere in Turkish-German relations during this period, the two countries eventually decided to build a joint airplane factory under the name Turkish Aircraft and Engine Corporation (TOMTAŞ). After the inauguration of TOMTAŞ, private sector initiatives in the field of aviation gained speed in Turkey; Nuri Demirağ opened the first private airplane factory in Turkey in Beşiktaş, and the Turkish Aeronautical Association's Etimesgut Airplane Factory and the Airplane Engine Factory were established between 1939 and 1941, at the beginning of WWII, upon the request of the General Staff. In 1950, both factories were transferred to the MKE.

Defense Industry Strategy and Policy in Turkey

Within the context of defense industry strategy, it is of great importance for a state to make sure that all of the arms and ammunition required by its armed forces are provided domestically from the national industry. However, it is quite difficult to achieve this objective. The technologies of the Turkish armed forces that are related to defense issues can be grouped into three categories. The first includes the systems and technologies that must be produced exclusively from national sources, while the second includes those that require technology transfer and joint production with foreign cooperation, as they cannot be produced in Turkey. The last category includes all the other systems and technologies that remain outside the first two categories.[18]

Developments in military technology are very dynamic and are constantly transforming the quality of defense industry products. Arms systems develop over time in accordance with radical changes in military technology, and these developments significantly change the strategic balance of defense between countries; this balance not only affects the causes, conduct, degree of violence and consequences of war, but also significantly influences states' national security policies and military relations.[19]

States' foreign policy strategies and doctrines reflect decisionmakers' perceptions about international and local developments. A strategy is created in accordance with a state's place in the world as well as its national interests and the instruments it is able to employ to reach them.[20] A national security strategy in this regard depends on the intermediate and long-term policies followed by a state in its international relations. States' threat perceptions emerge as a result of various international considerations. Yet, ensuring the security of the state and protecting its national interests can only be possible if the state possesses an efficient defense industry with developed defense systems and powerful production capabilities. It is extremely important in this sense to establish a connection between science/technology plans and military requirements.[21]

The goal of the Turkish defense industry policy and strategy is to formulate a vision that is based on realistic assessments and scientific data in order to enable Turkey to meet its defense requirements with its available resources. It is imperative for Turkey to plan all its defense industry activities and the procurement of its defense products in accordance with this strategy.[22]

Mustafa Kemal Atatürk's principle of "Peace at home, peace in the world," which has constituted the essence of Turkish foreign policy ever since the Republic was founded, highlights principles such as the peaceful resolution of conflicts in Turkey's neighborhood and in the world, non-interference in the internal affairs of other states and maintaining good relations with neighboring countries. Within the framework of these principles, Turkey provides direct support to the activities of the United Nations for the resolution of global issues as well as regional disputes.

In the development process of Turkey's national defense industry, remarkable investments were made in the 1933–1939 period; however, events such as the outbreak of WWII and the start of significant Western military aid to Turkey in the second half of the 1940s slowed down the development of the Turkish national defense industry.

In the development process of Turkey's national defense industry, remarkable investments were made in the 1933–1939 period; however, events such as the outbreak of WWII and the start of significant Western military aid to Turkey in the second half of the 1940s slowed down the development of the Turkish national defense industry. Yet, especially following the military embargo implemented by the U.S. against Turkey after the Cyprus Peace Operation in 1974, the necessity of establishing a national defense industry became crucial. Therefore, one could argue that the foundations of the core organizations of Turkey's national defense industry were laid after the Cyprus operation. More recently, the Undersecretariat for Defense Industries (SSM), established in 1985, has launched remarkable projects with the purpose of producing all kinds of weapons, tools, equipment and ammunition needed by the TAF by relying on domestic resources.[23]

In order for the Turkish state to thrive in its geography and secure its future interests, it is of utmost importance that it possess a strong defense industry to take its security to a higher level. In this sense, Turkey's fundamental policy should be to refrain from taking any steps that could weaken its defense industry capacity. This is because the military power and deterrence capability of states whose defense industries do not depend on national technology are vulnerable. States control the development of their national defense technologies in order to maintain the confidentiality of their arms systems. Therefore, the defense industry needs to be national in every state.[24] However, the delicate balance between the development of a national defense industry and the security of the state should be preserved, the national industry should not be put at risk due to unnecessary concerns, and obstacles to the technological development of the national industry should be removed.

The most important factor that could help support the development of Turkey's domestic defense industry is to increase the "domestic contribution rate", which generates additional costs; it is impossible to make further investments and achieve greater technological gains without paying higher prices. Some of Turkey's national defense industry companies have been encouraged to compete with each other on certain projects, while they cooperate on other projects that are important for the interests the country. The export activities of all of the national defense industry companies should be actively supported by all the organs of the state without discrimination.[25]

The principles of military strategy in Turkey are first of all based on the total defense concept and the capacity to have a deterrent military force structure. To this end, superior mobility; the ability to intervene in events in a short time; forward defense; maintaining readiness for high-intensity battle; possessing modern weapon systems and operating in all kinds of terrain, visibility and weather conditions are very important. The execution of these duties is the responsibility of the TAF. This responsibility can only be provided by powerful, modern and well-equipped military forces. Thus, the military force structure of the TAF is equipped with specifically developed command-control and combat systems, military units with superior mobility and early warning capability and improved air defense and response systems. The modernization of the TAF should be continuous and uninterrupted in order to elevate Turkey's defense technologies to a level that is renewable and capable of responding to future threat perceptions. [26]

Although intensive efforts were made to achieve lasting peace and security globally and in Turkey's neighborhood in the post-Cold War period, the emergence of regional conflicts could not be completely prevented. New security problems have emerged due to instability and uncertainty in the regions defined as 'rimland' zones. Regional, ethnic and religious conflicts, nuclear proliferation, proliferation of weapons of mass destruction, drug trafficking and international terrorism are important challenges to security, both for Turkey and the world at large.

The Modernization of Turkey's Defense Industry & Defense Spending (1980–2020)

The defense industry has its own unique characteristics. Defense industry products are expected to be confidential and reliable. The use of the most advanced technologies possible, the development of powerful, large and reliable companies, and the smallest degree of dependency on other countries are important features of a state's defense industry.[27] There is a very close relationship between a state's defense capabilities and the level of development of its defense industry. Since the defense industry is a sector in which advanced technologies are used, national defense capabilities are directly related to the technological level of development. In addition, the most obvious criterion for the production of defense systems is privacy. This means that the features of military systems should be confidential, and their strong and weak points should be known only by their users. Otherwise, the effectiveness of the arms systems will be significantly weakened.

Meeting the needs of the armed forces in a secure and stable manner forms the basis of the Turkish defense industry strategy. For this purpose, it is necessary to produce high-tech combat weapons and vehicles on a national basis, to form the necessary technology base as well as production facilities and to encourage and support the national defense industry. R&D activities have great importance in this process, as a low R&D capacity increases a state's external dependency. In fact, developed countries that possess advanced defense industries owe their technological and industrial achievements mainly to the R&D activities they have been conducting for many years.[28]

The most important factor that could negatively affect the development of the national defense industry is the failure to base procurement activities on R&D. The most important task to complete in this regard is to undertake critical defense projects with R&D-based procurement.[29] When one takes a look at the last 40 years of the Turkish national defense industry, apart from utilizing ready-made options in terms of meeting supply needs, new implementation programs have also been started. Since the 1980s, Turkey has introduced new production models based on smart procurement, production under license, joint production/technology transfer, original design and R&D. [30]

One of the most important concepts in the defense industry is "technological depreciation." This means that a new weapon that is developed in tandem with progress in new technologies reduces or completely eliminates the military effectiveness of the previous weapons that had been produced for the same purpose. In other words, as new technologies are developed, weapon systems lose their economic and military value and become obsolete before they complete their life cycles. In this respect, defense industry companies and corporations need to constantly renew and improve their techniques in order to remain competitive. [31]

The defense industry is an area that is directly related to the security of the state, and because it is dependent on the level of technological development, it requires the allocation of large resources from the state budget.

When one takes a look at the last 40 years of the Turkish national defense industry, apart from utilizing ready-made options in terms of meeting supply needs, new implementation programs have also been started.

Since the risks to be confronted in the case of failure are immense, the defense industry is a sphere that should be controlled by the state. This is also because the knowledge, experience, investments and capabilities gained in the field of defense industry are very valuable and should be passed on to future generations.[32]

The defense industry is also a strategically important sector; states aim to use the most up-to-date technologies to elevate their competitiveness, especially in the field of R&D and innovation. This aim remarkably increases the share of defense expenditures in some states' national budgets.[33] High performance and quality are quite important in the assessment of the effectiveness of defense industry products. In this regard, it is once again crucial to use advanced technology, although this requires significant R&D investments, both in terms of the allocation of greater financial resources and the employment of more researchers.[34]

From World War II until the Cyprus operation in 1974, Turkey chose to meet the needs of its armed forces, including weapons, vehicles, equipment and materials, mainly from abroad by using foreign aid and credits in addition to resources allocated from the national budget. After 1974, however, efforts to develop the defense industry gained speed as a result of the U.S. embargo imposed on Turkey. However, it should be noted that developments in the defense industry were very slow until the early 1980s, while particularly from 1990 onwards the Turkish defense industry has gained significant momentum and has started to produce a much larger share of the requirements of the TAF.

The development of an independent defense industry is only possible when a state has an independent technology base; therefore, important initiatives to produce critical technologies are required. In the process of transitioning to a modern defense industry, it is important to coordinate activities with foreign companies without undermining national capabilities. The national defense industry should be supported by the state as much as possible in order to keep the resources used to meet the needs of the armed forces inside the country.

In Turkey, more modern and organized working programs in the field of the defense industry were developed at the beginning of the 1980s. The General Directorate of Defense Equipment Enterprises was established in 1983 for the purpose of placing the Turkish defense industry on a more solid basis with more guidance from the government. This organization was later transferred to the Directorate of Defense Research and Development (SAGEB) together with its capital before it could perform any meaningful activities. SAGEB was established in 1985 to coordinate defense industry activities and enable Turkey to develop a self-sufficient industrial defense capacity. SAGEB later continued its activities under the name of Undersecretariat for Defense Industries (SSM), which was established by the Ministry of National Defense as a legal entity aiming to modernize the TAF along the lines of a much more efficient and functional model.[35]

Within the scope of Law No. 3238, dated November 7, 1985, the Defense Industry High Coordination Board and the Defense Industry Executive Committee (SSIK) were founded, and the Defense Industry Support Fund (SSDF) was formed to coordinate financial structuring under the umbrella of the SSM. The SSM has been mainly responsible for the production of defense systems in accordance with the TAF's strategic targets and plans, while supporting the establishment and development of the defense industry in Turkey. For this purpose, the task of carrying out defense procurement activities, such as planning, programming, budgeting, organization, coordination, fund management, incentives, credits and investments, foreign capital, technology transfer, R&D, manufacturing, quality assurance, contract management, export and off-set implementations were all assigned to SSM within the framework of the decisions of the Defense Industry Executive Committee.[36]

Since its foundation, the main goal of the SSM has been the development of a national defense industry in Turkey that is compatible with current technological advances in accordance with the existing industrial capacity of the country.

Since its foundation, the main goal of the SSM has been the development of a national defense industry in Turkey that is compatible with current technological advances in accordance with the existing industrial capacity of the country. By taking advantage of the capabilities of the Turkish defense industry, the SSM aims to meet the needs of the TAF from national resources to the maximum extent possible. In this sense, priority is given to efforts for bringing the defense industry into the most ideal structure and maximizing the efficient use of resources, time and personnel.[37]

The establishment of the SSM in 1985 was a very important step for the modernization of the TAF and the development of a modern infrastructure for the defense industry. With the support of a constant and stable annual budget that exceeds $1 billion provided by the SSDF, the weapons, tools and equipment needed by the TAF have started to be met from national sources.

The SSM was placed under the Presidency of the Republic of Turkey with the amendments made in 2017; under Decree-Law No. 703, it was restructured under the name of Presidency of Defense Industries (SSB) in 2018. With the ratification of Law No. 3238, an efficient and flexible system was established to ensure that the needs of the TAF and other security forces would be supplied more rapidly, and to develop the modern defense industry in Turkey. The fundamental mechanisms of this system are the SSB, SSIK and SSDF.[38]

Defense services protect national sovereignty and ensure the security of the state against all kinds of illegal activities that could take place inside the country. In this regard, since defense expenditures ensure the maintenance of national sovereignty and thus the state's very existence, states allocate large shares from their national income for defense purposes at the expense of their wealth.[39]

Defense expenditures are generally one of the largest and most important categories of government spending. For this reason, changes in a country's defense expenditures affect all sectors of a country's economy. The positive aspect of this influence is that increases in defense expenditures can help stimulate industry demand and economic growth.[40] However, particularly during periods when the arms race intensifies between states, increased defense spending creates various difficulties, as governments allocate a larger part of their economic resources to armament, which could trigger inflation, unemployment and a decrease in the country's growth rate.[41]

The "Turkish Defense Industry Policy and Strategy," which was approved by the Council of Ministers and entered into force after being published in the Official Gazette on June 20, 1998, sets out the principles for short-, intermediate- and long-term planning for the development of the defense industry and the production of the weapons, tools and ammunition needed by the TAF from Turkish national resources and using indigenous capabilities to the maximum possible extent.[42]

According to the "White Book" published by the Ministry of National Defense in 1998, the sources of funding necessary for defense expenditures are defined as follows: "Resources allocated from the national defense budget, resources of the defense industry fund, resources of the Foundation for Strengthening the TAF, budget of the Gendarmerie General Command, budget of the Coast Guard Command and credits given by the state or companies whose repayments are guaranteed from the budget of the Undersecretariat of Treasury."[43]

In all countries of the world, defense expenditures are financed largely from the state budget. This is because defense is an area that should be completely under state control. In Turkey, the share of defense expenditures in the state budget in the early years of the Republic was very high, as necessitated by the conditions of that period. The country's struggle to protect its national sovereignty immediately following the War for Independence obviates the importance of defense issues. In 1924, Turkey's defense expenditures were around 48 million Turkish liras, equal to a 36% share in the budget. In other words, more than one third of the Turkish budget was allocated to defense expenditures, while the share of defense expenditures in Turkey's GNP for that fiscal year was 4%. Comparatively, 8 million Turkish liras was allocated to education and health expenditures, which made up only 5.5% of the budget.

The world economic crisis in 1929 caused a sharp decline in Turkey's defense spending; in 1929 its defense expenditures were around 78.5 million Turkish liras, while their share in the budget was 30.8% and the defense spending/GNP ratio was 3.8. Although defense expenditures increased between 1924 and 1934, their share in the budget decreased in the same period. In the 1935–1944 period, the effects of WWII should be taken into consideration; during this period, the share of defense expenditures in the budget increased considerably—from 30% in 1938 to 43.1% in 1939, 53.2% in 1940 and 55% in 1941. In the 1945–1954 period, the share of defense expenditures in the budget gradually decreased as WWII came to an end, and Turkey joined the NATO alliance and started receiving greater foreign aid from the West.[44]

Weapons technologies and production, which developed after WWII, were an important factor in the increase in many country's military expenditures. Global defense expenditures reached their highest level in 1987, then started to decline.[45] The emergence of the Cold War and a bipolar international system also contributed to the increasing share of defense expenditures in state budgets all around the world. With the emergence of the bipolar world order, the need to develop national capabilities increased in terms of the development and production of weapon technologies. In this period, new companies were established, especially in the U.S., while the production of the new weapons of the missile age also gained speed.[46]

The trajectory of Turkish defense expenditures, like that of many countries during the Cold War period, reflects the strong influence of the global arms race of the 1960s, characterized by the rapid development and production of arms technologies. In the 1970s, Turkey had the highest increase in defense expenditures of all NATO members, allocating significant resources for defense purposes mainly due to the influence of the Cyprus issue. This trend continued in the 1998–1999 period, as evidenced by the 2006 SIPRI report, which indicates that Turkey's defense expenditures rose from $5 billion in 1998 to $12 billion in 1999, then declined to $8 billion in 2004.

At the beginning of the 2000s, Turkey ranked seventh ($7,792 million) globally in terms of its defense spending, sixth in the number of soldiers (820,000), 25th in terms of its GDP ($193,500 million), 41st in defense burden (4%) and 50th in per capita defense spending ($123).[47] While Turkish defense expenditures were 6,248 million Turkish liras in 2000, this figure increased to 65,566 million liras as of 2017—an almost tenfold increase in only 17 years.

Turkish defense industry expenditures increased by an average of 9.7% during the ten years between 2007 and 2016, and its defense spending reached $14.8 billion as of 2016. With new incentives and additional resources, the defense budget in 2017 increased to $18.2 billion. This total includes the budget of the Ministry of National Defense as well as the expenditures of other security forces. According to SIPRI data, Turkey's defense spending in 1998 was $7,703 million, almost doubling to $15,084 million in 2017.[48] By 2018, Turkey had become one of the top fifteen countries of the world with $19 billion in defense spending.[49]

In the 2017–2018 period, Turkey acquired a large share of its arms imports—totaling $7,679 million—from the U.S., which held the first place among all states in terms of its defense spending. In 2017, Turkey's total arms imports were $410 million, while Turkey made the highest total of arms imports in 2014.[50] According to the 2020 SIPRI report, when the 2011–2015 period is compared with the 2016–2020 period, Turkey's arms imports decreased by 59 percent. The U.S., Italy, Spain and Russia have been Turkey's top import partners in the last five years, with warplanes and missiles among the top military products imported by Turkey.

Especially in the 2010s, greater emphasis was placed on original design programs under the guidance of the country's primary national contractors with the purpose of developing critical technologies from domestic sources. The SSM's 2012–2016 Strategic Plan aimed to make Turkey a leading country in terms of defense and security technologies; industrialization, technology and procurement programs were planned in the field of defense and security. By initiating these programs, the SSM sought to prepare the TAF for the future combat environment, enhance competence in defense and security technologies and support the development of platforms and systems required for technological superiority, and Turkey's dependence on other countries was reduced significantly.[51]

Especially in the 2010s, greater emphasis was placed on original design programs under the guidance of the country's primary national contractors with the purpose of developing critical technologies from domestic sources.

The number of projects launched by the Turkish defense industry increased almost tenfold between 2004 and 2018, and the production of new military equipment such as unmanned aerial vehicles (UAVs), tanks, helicopters and rockets played an important role in reducing Turkey's dependency on foreign sources, while helping Turkish defense companies take their place among the top 100 defense companies in the world. The achievements of the Turkish defense industry have expanded far beyond the national borders, and Turkish expenditures in this sphere have increased exponentially. While a total of $5.5 billion was spent on the defense industry in 2002 with the initiation of new investments and projects aiming to reduce dependence on other countries, this figure reached $60 billion in 2018. The ratio of meeting defense needs from national sources, which was around 25% in 2002, reached 60% in 2018. Finally, the production capacity of the defense industry rose from $1.3 billion in 2012 to $6 billion in 2018.[52]

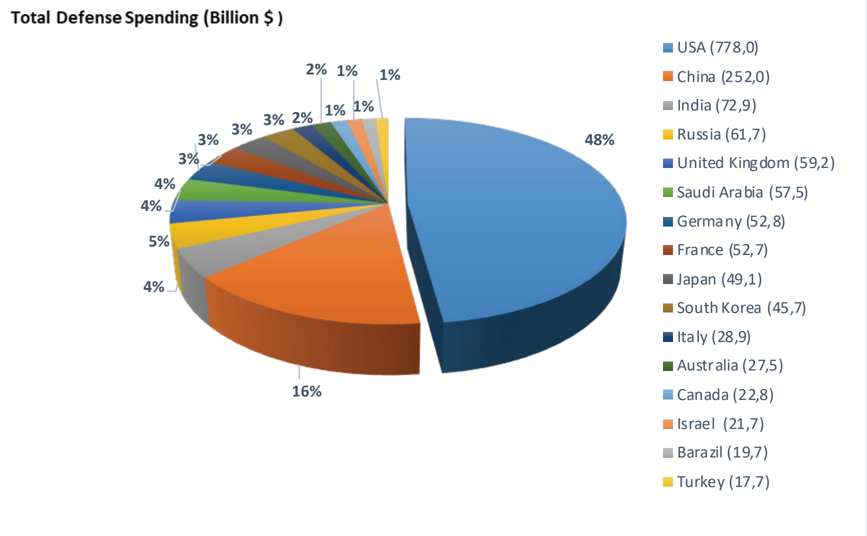
Turkey's MİLGEM corvettes, Altay tanks, Atak attack helicopters, Anka and Bayraktar UAVs, Hürkuş training airplanes, Göktürk-1 surveillance satellite, newly designed patrol boats, rapid intervention boats, national infantry rifles, mine-proof vehicles and air defense and missile systems are the results of projects that have reduced Turkey's dependency in the defense industry. The TAF and SSB are currently among the world's leading institutions in their fields. Resources allocated by Turkey to its defense from the national budget as well as other funds now consist of around $6 billion annually; $2.5–3 billion are allocated to the purchase of defense equipment and services when one excludes personnel costs and other running expenditures.

Determining Turkey's defense spending parameters and the allocation of related resources are decision processes carried out within the framework of the Planning, Programming and Budgeting System (PPBS). Planning includes the process of determining military strategy, strategic goals and force structure for the intermediate (10 years) and long term (11–20 years). Programming involves projecting how the goals determined by the planning branch will be achieved based on the available resources in a specific time frame. Budgeting is the process of deciding where, with what purpose and how much of the possible resource allocations specified in the ten-year procurement program will be made in a specific budget year.[53]

Defense expenditures may have positive and negative effects on production. The positive effect emerges as an increase in the defense budget, which also contributes to economic growth, especially in cases where the underemployment percentage is high. Expenditures related to scientific research for military purposes and technical developments also contribute positively to production, and encourage further scientific research and technical progress.

Globally, the highest defense spending occurs in America, Asia, and Europe, while the highest increase in defense spending was measured in the U.S. and Asia between 2000 and 2009. Comparatively, the increase was quite low in Western and Central European countries. In the Middle East, defense expenditures increased by 40% during the 2000–2009 period. In 2009, defense expenditures increased in Syria, Bahrain, Lebanon and Jordan. Oman, Bahrain, Kuwait, Saudi Arabia and the United Arab Emirates (UAE) are responsible for almost 60% of the defense expenditures in this region.[54] In 2017, the share of Saudi Arabia's defense expenditures in public expenditures was approximately five times higher than Turkey's, while the same figure for Oman was four times higher.

Figure 1: Global Defense Expenditures (2020)

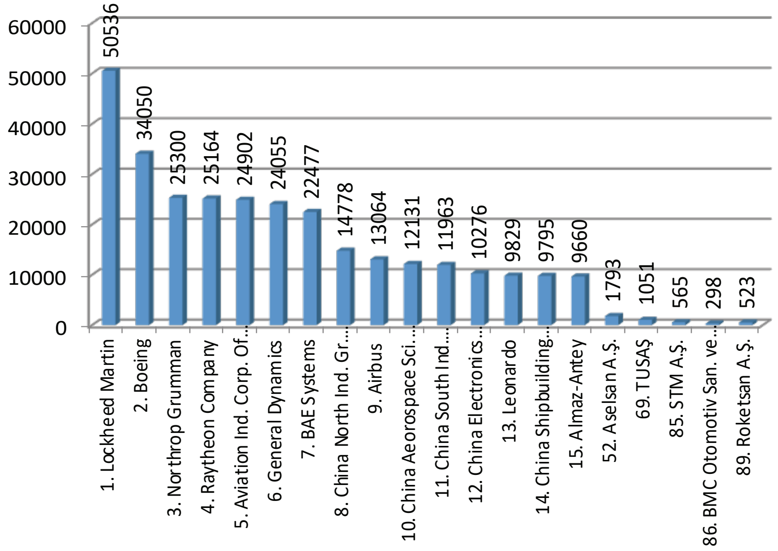


Source: SIPRI Military Expenditure Database 2020

In 2010, the 73 companies responsible for the majority of global arms sales were based in the U.S. and Western Europe—accounting for approximately 90 percent of total arms sales. The U.S.-based Lockheed Martin topped the list, and Britain's BAE Systems came second. U.S. Boeing, Northrop Grumman and General Dynamics were the other notable companies. In 2015, the ranking was almost the same, with

Lockheed Martin first, Boeing second and BAE Systems third.[55] In 2020, Lockheed Martin still ranked first, while Boeing ranked second and Northrop Grumman ranked third. It should be noted that three Chinese companies (AVIC, NORINCO and CETC) entered the top ten for the first time in 2020, and the number of Turkish companies in the list increased to seven as of 2020: ASELSAN A.Ş. at 48, TAI at 53, BMC at 89, ROKETSAN at 91, STM A.Ş. at 92, FNSS at 98 and HAVELSAN at 99.[56] The latter two companies entered the list in 2020 for the first time.

Figure 2: Top 100 Arms Companies in the World (2019)



Source: Top 100 Defense News for 2019, https://people.defensenews.com/top-100/

Responsible for one-third of global arms sales, the U.S. was the largest exporter of arms in the 2011–2015 period. Its most important customers are Saudi Arabia, the UAE and Turkey. Russia ranks second in arms exports with a share of 25%; its most important customers are India, China and Vietnam. China, which ranks third, meets 5.9% of world arms sales; its main customers include Pakistan, Bangladesh, and Myanmar. Approximately half of the arms sales of the UK are made to Saudi Arabia, while Turkey is an important customer for Spain and Italy as their third largest market.[57]

Table 1: Global Defense Expenditures by Country by Year (Million USD)

Countries	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
U.S.	849,867	839,803	793,157	732,148	687,112	671,509	669,448	662,550	682,491	718,689
China	143,932	155,169	168,514	184,209	200,023	213,526	225,558	238,476	253,492	266,449
India	51,671	52,171	51,986	51,603	54,276	54,292	59,833	64,572	66,258	70,794
Russia	49,198	52,506	60,836	63,800	68,378	73,694	79,007	63,652	61,388	64,144
Saudi Arabia	54,713	55,456	62,761	71,925	84,772	90,409	64,698	72,136	74,400	62,525
France	50,482	48,981	48,229	47,916	48,750	50,084	52,026	52,710	51,410	52,229
Germany	44,468	43,275	43,646	41,980	41,032	40,888	43,784	45,340	46,512	51,190
UK	58,962	56,813	54,524	52,355	50,996	49,838	49,912	49,412	49,892	49,916
Japan	45,629	46,243	45,686	45,492	45,978	46,788	46,505	46,542	46,618	46,562
South Korea	33,957	34,422	35,298	36,368	37,798	39,267	40,251	40,991	43,070	46,281
Brazil	26,424	25,595	26,087	26,229	26,754	26,134	24,807	26,424	28,177	28,030
Italy	31,377	30,727	28,403	27,315	25,216	24,146	27,353	28,139	27,808	28,037
Australia	22,289	21,981	21,210	21,026	22,820	25,155	27,546	27,496	26,840	27,395
Canada	17,583	18,177	17,284	15,977	16,238	18,656	18,904	22,835	22,729	22,279
Israel	15,500	15,669	15,986	16,476	17,725	17,971	18,911	19,739	19,759	20,102
Turkey	11,184	11,280	11,556	11,868	11,955	12,302	14,423	15,480	19,649	20,796

Source: SIPRI Military Expenditure Database 2019

Conclusion

Turkey's geographical position—especially the location of the Turkish Straits, which allow passage from the Black Sea to the Mediterranean—and its links with the Balkans, Caucasus and Middle East, are the most important factors that influence its defense strategy. Due to its deep-rooted historical, socio-political and economic relations with the countries of its neighboring regions, it is appropriate for Turkey to possess a multidirectional foreign policy and defense concept.

Since the early years of the Republic, the efforts made by Turkey's military factories have been crucial for the development of its defense industry's infrastructure. The airplane factories, shipyards and arms factories founded in Turkey could be regarded as the country's most important early investments in this area. Since 1980, the year when the first foundations of Turkey's transition into the modern defense industry were laid, initiatives launched at both the national and international level have brought about impressive results in a relatively short time. This progress has led to the development of a new national defense industry strategy and policy, which forms the foundations of Turkey's current defense concept.

Since the foundation of the Republic, Turkish governments have launched significant initiatives in the field of defense industry, although these efforts have hit occasional roadblocks due to the national and international problems experienced in some periods. Since the start of the 21st century, Turkey's defense industry has developed rapidly. Over the past decade alone, Turkish-made UAVs have become quite remarkable. Turkey is now closely following global technological developments and undertaking notable work in this sphere, producing swarm drones, quantum radars, pocket submarines and laser weapons. In addition, significant developments in electronic, information, communication and material technologies have enabled Turkey to make breakthroughs in the military field in recent years.

Endnotes

1 Suat İlhan, *Jeopolitik Duyarlılık*, İstanbul: Ötüken, 2003, p. 76.

2 Ibid, p. 146.

3 Murat Aslan, "Türkiye: Bölgesel Yükselen Oyuncu," in Murat Yeşiltaş & Rıfat Öncel (eds.), *Ortadoğu'da Güvenlik, Savunma ve Silahlanma*, Ankara: SETA, 2020, p. 72.

4 Richard L. Armitage & Joseph Nye, "CSIS Commission on Smart Power," *Carnegie Endowment for International Peacet*, 2007, https://carnegieendowment.org/files/csissmartpowerreport.pdf.

5 Nejat Eslen, *Tarih Boyu Savaş ve Strateji*, İstanbul: IQ Kültür Sanat, 2003, p. 50.

6 *Beyaz Kitap*, Ankara: MSB, 2000, p. 30.

7 Aslan, "Türkiye: Bölgesel Yükselen Oyuncu," p. 75.

8 *Beyaz Kitap*, p. 52.

9 Carl von Clausewitz, *Savaş Üzerine*, İstanbul: Alfa, 2018, p. 163.

10 Murat Yeşiltaş & Rıfat Öncel, "Ortadoğu'da Savunma, Güvenlik ve Silahlanma: Temel Kavramlar, Stratejik Eğilimler ve Oyuncular," in Murat Yeşiltaş & Rıfat Öncel (eds.), *Ortadoğu'da Güvenlik, Savunma ve Silahlanma*, Ankara: SETA, 2020, p. 24.

11 Şener Aktürk, "Turkey's Grand Strategy as the Third Power: A Realist Proposal," *Perceptions: Journal of International Affairs*, Vol. 25, No. 2 (2020), p. 154.

12 Hüsnü Özlü, "Atatürk Döneminde Türk Savunma Sanayii," *Atatürk Ansiklopedisi*, Ankara: Atatürk Araştırma Merkezi, 2021.

13 Metin Ünver, "Teknolojik Gelişmeler Işığında Osmanlı-Amerikan Silah Ticaretinin İlk Dönemi," *Tarih Araştırmaları Dergisi*, Vol. 32, No. 54 (2013), pp. 195–220.

14 Başbakanlık Cumhuriyet Arşivi (BCA), Bakanlar Kurulu Kataloğu 030.18 / 01-02 / 83-60-5, Karar No: 2-9141.

15 BCA, 030.18/ 01-02 / 90-32-12, Karar No: 2-13212.

16 BCA, 030.10/ 49-319-2 / M-15493.

17 Özlü, "Atatürk Döneminde Türk Savunma Sanayii."

18 Göksen Şimşek, "Savunma Sanayii Politikası ve Stratejisi," *Savunma Sanayiindeki Teknolojik Gelişmeler Sempozyumu*, Ankara, June 5–6, 1997, p. 14.

19 Yeşiltaş & Öncel, "Ortadoğu'da Savunma, Güvenlik ve Silahlanma," pp. 30–31.

20 Mustafa Aydın, "Grand Strategizing in and for Turkish Foreign Policy: Lessons Learned from History, Geography and Practice," *Perceptions: Journal of International Affairs*, Vol 25, No. 2 (2020), p. 207.

21 *Savunma Sanayii ve Tedarik*, Ankara: TÜBİTAK, 1998, p. 39.

22 Bülent Karan, "Türk Savunma Sanayiinin Mevcut Durumu ve Geleceğe Yönelik İhtiyaçları," *Savunma Sanayiindeki Teknolojik Gelişmeler Sempozyumu*, Ankara, June 5–6, 1997, p. 20.

23 M. Levent Şenel & Şaduman Doğrusöz, "Dünyada ve Türkiye'de Savunma Sanayii Politikaları ve Çok Uluslu Ortak Tasarım, Geliştirme ve Üretim Programları," *Savunma Sanayiinde Stratejik İlişkiler Sempozyumu*, Ankara, December 10–11, 2002, p. 271.

24 Aytekin Ziylan, *Savunma Sanayii Üzerine*, Unknown Publisher: Ankara, 1999, p. 15.

25 Ekrem Kadıoğlu, "Geçmişte ve Gelecekte Türk Savunma Sanayiinin Geliştirilmesi İçin Hedeflenmesi Gereken Politikalar II," *Savunma ve Havacılık*, Vol. 14, No. 81 (2000), p. 63.

26 *Savunma Sanayii El Kitabı*, pp. 14–28.

27 Ziylan, *Savunma Sanayii Üzerine*, p. 93.

28 Oktay Alnıak, "Savunma Endüstrilerinde Teknolojik Gelişme Stratejileri," *Savunma Sanayiinde Stratejik İlişkiler Sempozyumu*, Ankara, December 10–11, 2002, p. 3.

29 Ziylan, *Savunma Sanayii Üzerine*, p. 102.

30 Aslan, "Türkiye: Bölgesel Yükselen Oyuncu," p. 82.

[31] Muammer Şimşek, *Üçüncü Dünya Ülkelerinde ve Türkiye'de Savunma Sanayii,* Ankara: SAGEB, 1989, p. 17.

[32] Ibid, p. 19.

[33] Serkan Altuntaş & Türkay Dereli, "Savunma Sanayiinde Teknoloji Gelişimi: Mühimmat ve Tahrip Teknolojileri Üzerine Bir Uygulama," *Girişimcilik ve İnovasyon Yönetimi Dergisi*, Vol. 5, No. 2 (2016), p. 107.

[34] Dilek Temiz, "Ekonominin Önemli Bir Parçası: Savunma Sanayii," *Dumlupınar Üniversitesi Sosyal Bilimler Dergisi*, No. 33 (2012), p. 2.

[35] *15'inci Yıldönümünde Savunma Sanayiinin Dünü, Bugünü ve Yarını*, Ankara: SSM, 2001, p. 35.

[36] *Türk Savunma Sanayiinin Ana Sorunları ve Bu Sorunlara İlişkin Çözüm Önerileri*, Ankara: TOBB, 2002, p. 81.

[37] Ibid, p. 25.

[38] "2020 Yılı Performansı," *SSB*, https://www.ssb.gov.tr/Website/contentList.aspx?PageID=1040&LangID=1.

[39] Kutluk Kağan Sümer, "Savunma Harcamalarının Ekonomik Büyüme Üzerine Etkisinin İncelenmesi," *Güvenlik ve Stratejileri Dergisi*, Vol. 1, No. 1 (2005), p. 87.

[40] Ibid, p. 84.

[41] Şimşek, *Üçüncü Dünya Ülkelerinde ve Türkiye'de Savunma Sanayii*, p. 11.

[42] *Beyaz Kitap*, p. 125.

[43] Ibid, p. 117.

[44] Selami Sezgin, "Türkiye'de Savunma Harcamaları," *Türk Savunma Sanayiinin Dünü, Bugünü, Yarını, Savunma Sanayii Sempozyumu*, Ankara, November 7–8 , 2000, p . 476.

[45] Şerif Canbay & Derya Mercan, "Savunma Harcamalarının Ekonomik Büyüme ve Cari İşlemler Dengesine Etkisi: Türkiye Örneği," *Journal of Emerging Economies and Policy*, Vol. 2, No. 2 (2017), p. 88.

[46] Selami Sezgin & Şennur Sezgin, "Dünya'da ve Türkiye'de Savunma Sanayi: Genel Bir Bakış," *Avrasya Sosyal ve Ekonomi Araştırmaları Dergisi*, Vol. 5, No. 12 (2018), pp. 1–19.

[47] Sezgin, "Türkiye'de Savunma Harcamaları," p. 478.

[48] *Savunma Sanayii Sektör Meclisi 2017 Yıllık Raporu*, TOBB: Ankara, 2017.

[49] "Trends in World Military Expenditure 2019," *SIPRI*, April 2020, https://www.sipri.org/publications/2020/sipri-fact-sheets/trends-world-military-expenditure-2019.

[50] Ibid.

[51] "Tarihçe," *SSB*, https://www.ssb.gov.tr/WebSite/contentlist.aspx?PageID=47&LangID=1.

[52] "Türk Savunma Sanayii, 14 Yılda Proje Sayısını 10'a Katladı," *Akşam*, April 17, 2018, https://www.aksam.com.tr/ekonomi/turk-savunma-sanayi-14-yilda-proje-sayisini-10a-katladi/haber-726981.

[53] *Beyaz Kitap*, p. 117.

[54] Deniz Şişman, "Küreselleşme, Kriz ve Savunma Sanayi," *Marmara Üniversitesi İktisadi ve İdari Bilimler Dergisi*, Vol. 39, No. 1 (2017), p. 226.

[55] "Türk Savunma Şirketleri 'Defense News Top 100' Listesine Damga Vurdu! Savunmanın 7 Devi," *Hürriyet*, August 18, 2020, https://www.hurriyet.com.tr/ekonomi/turk-savunma-sirketleri-defense-news-top-100-listesine-damga-vurdu-savunmanin-7-devi-41589429,18.08.2020.

[56] Şişman, "Küresellşme, Kriz ve Savunma Sanayi," p. 229.

[57] Ibid, p. 231.

ARTICLE

Understanding Defense Industry: A Systems Thinking Perspective

Mehmet Hilmi ÖZDEMİR [*] & Gökhan ÖZKAN [**]

Abstract

The defense industry can be thought of as a complex system of intense interactions between humans and high-tech machines, platforms and data systems with a large number of dynamically interacting variables. Within the defense industry, many complex decision-making processes take place, in which even very intelligent and highly educated people often make poor decisions due to failure to grasp this complex system as a whole, and/or by using linear or deterministic methods. The present study is structured to offer decision-makers, researchers and practitioners dealing with defense industry subjects new perspectives. The development of new mental models requires new perceptions and even confrontations between different perceptions. The most distinctive developments begin with creative ideas that are the outcomes of particular mental models. The defense industry is among those that continuously seek innovative approaches, creative ideas and new solutions. A systems thinking approach, together with Viable Systems Model (VSM) and system dynamics methodologies is one such innovative approach. One successful application of systems thinking—NATO's Aggregated Resilience Model—can be considered a benchmark in the development of new mental models and creative solutions. The inevitable decision support needed by policy- and decision-makers who pursue innovation in the defense industry can be met by the "systems thinking" approach discussed in this article.

[*] PhD, STM Savunma Teknolojileri Mühendislik ve Ticaret A.Ş., Ankara, Turkey.
E-mail: mozdemir@stm.com.tr. ORCID: 0000-0003-1567-8044.

[**] PhD, STM Savunma Teknolojileri Mühendislik ve Ticaret A.Ş., Ankara, Turkey.
E-mail: gokhanozkan@stm.com.tr. ORCID: 0000-0003-3476-5661.

Received on: 12.05.2021
Accepted on: 17.10.2021

Keywords

Defense industry, systems thinking, complexity, system dynamics, viable systems model, mental models, modeling and simulation.

Introduction

Defense and security are among the paramount areas of global concern today. Looking at the big picture, defense and security issues are so far-reaching that almost all of humanity feels the effects of the concerns, as well as the outcomes produced in this area. This expansive area is addressed by a unique and complex industry—the defense industry—that incorporates boundlessly interconnected agents. The profile of these agents varies from ordinary citizens to superpowers and global stakeholders. Beyond this, the defense industry is a perpetual cornerstone industry in many nations, pioneering different domains such as technology, economics, education and training, standardization, modeling and simulation. Its pioneering role increases the attractiveness of the defense industry. Countries allocate considerable amounts of money to this sector and try to equip their armed forces with up-to-date capabilities, first to maintain their existence, and second to provide and sustain the appropriate conditions to protect their interests by reducing risks in the future in line with their policies and strategies. The multi-domain feature of the sector and the number and variety of the stakeholders seeking new business opportunities and potential investment areas within it add to the defense industry's complexity.

The management of a highly complex and attractive industry deserves exclusive attention. And given its complexity, a holistic understanding must be the starting point for studying and analyzing the industry; the results of fragmented efforts focusing on different parts of the industry, and even the synthesis of disconnected efforts, may not lead us to value-added inferences. Without a holistic perspective, decisionmakers and other authorities might face the risk of making faulty judgments when determining defense industry-related investment decisions in various dimensions such as research and development, training and education, personnel, technology, platforms and systems, infrastructure, etc.

The multi-domain feature of the sector and the number and variety of the stakeholders seeking new business opportunities and potential investment areas within it add to the defense industry's complexity.

Having framed the defense industry from a broad perspective, then, we aim to take a closer look in order to offer an innovative approach in this article. This study has been structured to contribute to a process whereby decision-makers, researchers and practitioners dealing with defense industry subjects can gain new perceptions. The development of new mental models requires new perceptions and even the confrontation of different perceptions. The most distinctive developments begin with creative ideas that are the outcomes of particular mental models. The defense industry is among those that continuously seek for creative ideas and solutions.

Given the ever-changing, dynamic conditions of the defense industry, traditional techniques and tools are insufficient. Therefore, we need to take a holistic approach that takes into account an understanding of those dynamic conditions and domains interactively and concurrently. Within the context of the defense industry, holism, meaning a comprehension of the interconnectedness and interrelatedness among all the parts that make up the whole, is a critical concept.[1] In this article, systems thinking, viable systems model (VSM) and system dynamics are discussed and recommended as an innovative and holistic approach and methodology. Systems thinking focuses on revealing the parts of complex structures and their relationships, examining different perspectives toward complex structures, and addressing power relations and potential conflicts of interest among related agents.[2] System dynamics methodology facilitates the policy determination process in the management of complex system behavior over time, as well as the policy application process for adapting to a complex environment.[3] System dynamics models provide foresight about situational behavior changes in a system over time. Importantly, the what-if scenario capacity of the model discussed in this study enables creation of alternative decisions for the policy makers.

Unique Features of the Defense Industry

The key outcomes of the defense industry are the generation and sustainment of "readiness" and "operational availability." The production of these critical outcomes requires addressing various dimensions and their interactions within the defense industry. This unique industry, consisting of intense interactions between humans and machines (high-tech platforms and systems) shall be taken as a complex system.

The complexity of the defense industry mainly stems from two challenges: (1) to educate and sustain highly skilled personnel and (2) to manage cost, schedule and risk factors during the development, acquisition and operation of integrated military systems. Moreover, the defense industry differs from other industries due to its unique features:

- High stakes, since the payoff of the defense industry's outcomes consists mainly of people's lives;
- The constant need for sustainable, strategic guidance;
- The involvement of high-tech systems, most of which are developed solely for their unique purpose within the industry and are not commercially available;
- The need for highly qualified personnel, who are indispensable yet expensive to employ;
- Time-lag; there is always a delay between taking an action and seeing its results (i.e., the outcomes of R&D or an acquisition may take several years);
- High standards; the defense industry sustains its viability only by adhering to strict international and military standards;
- High-level expectations and ever-changing requirements on the part of end users;
- Strict quality-control, testing and acceptance processes and procedures;
- Scarce resources, the use of which is always disputable;
- The demand that stakeholders produce the most from the least;
- Unique rules in the areas of economy, acquisition and competition.

As a highly complex system, the defense industry inherently involves many complex decision-making processes through which even very intelligent and highly educated people often make poor decisions by failing to see the whole picture, and using linear and/or deterministic methods.[4] Linear and deterministic approaches assume that managers live within a stable environment and are able to make reasonably good decisions about the future.[5] Most of the people dealing with the defense industry have a propensity to focus on tactical-level quantitative data and miss the strategic-level qualitative factors. Moreover, there are times when the problems managers are experiencing are themselves a consequence of flawed mental models. In these situations, managers rely on the wrong set of assumptions and inferences to make decisions that do not solve problems and often make matters worse.[6] So, as the defense environment becomes more complex, the defense industry by its unique structure and features has no other choice to but adapt to this environment.

As a highly complex system, the defense industry inherently involves many complex decision-making processes through which even very intelligent and highly educated people often make poor decisions by failing to see the whole picture, and using linear and/or deterministic methods.

The management of these challenges requires good conceptualization and contextualization practices, as traditional engineering and management implementations may fall short.[7] In the defense industry, decision- and policy-makers require innovative approaches to deal with the complex systems for which they are responsible. Hence the need to adopt a holistic approach considering different defense industry domains interactively and concurrently. At this point, among other views, the systems thinking approach and the system dynamics methodology take the stage as a modeling means for understanding strategic and complex phenomena and providing coherent world views[8] and thus policies for defense industry decisionmakers through scenario-based models (what-if analysis). This simulation method is based on calculus, and models of real-world dynamic processes are constructed using integral equations.[9] These simulation models use highly precise values and generate numerically accurate results; this functionality can be used by decisionmakers as "answer generators" for their area of interest.[10]

The first applications of systems thinking started to mature during and after World War II, and basic ideas were put forward in this period. The theorists of these approaches worked independently of each other in different disciplines; consequently, they focused on different problems, and various approaches emerged around systems thinking. The common point between them is that they focus on mutual relations rather than linear cause-effect relationships in scientific studies, and on the process of change rather than static situation assessments.[11]

Evolution of the Defense Industry via a Systems Thinking Approach

Systems may be understood as "coherent wholes" that consist of interrelated sub-systems and parts.[12] The interrelations (feedback loops) within a system, by virtue of their dynamic features, add complexity to that system. While the parts keep their individual importance within a system, the focus in systems thinking shifts to studying the whole system and the systemic behaviors of its various parts.[13] Complex systems with feedback loops and non-linear interrelations can be best understood via the systems thinking approach—and systems dynamics methodology—rather than deterministic techniques.[14] Deterministic methods have inadequacies when it comes to coping with complex systems such as social systems and defense systems. In contrast, systems thinking as a broad approach has the potential to tackle complexity. The systems thinking perception guides us to not break up a complex phenomenon into parts to fully understand it, but to deal with the phenomenon with a global vision to understand how it functions.[15] The core of the systems thinking approach is more about gaining the capacity to see the big picture[16] and creating new mental models—namely strategic planning itself—rather than making forecasts and projections. Systems thinking offers a robust perspective, a specialized terminology and a set of tools that has been proving its capacity with various successful implementations in different areas—including military and defense systems.[17]

The main difference between systems and traditional thinking is the dominance of reductionist and dogmatic approaches in traditional thinking, whereas relations, ecosystems and creative solutions are prioritized in systems thinking.[18] While traditional thinking techniques are analytic, system thinking techniques are synthetic.[19] However, it would not be wise to reduce one of these complementary approaches to the other.[20] For instance, the cybernetic approach falling in the system thinking context proposes a framework in which both analysis and synthesis are done concurrently.[21]

Rosnay states that the analytic approach foresees that making a change in one variable helps us understand the whole system, but this prediction can only be true for homogeneous systems. The most important weakness of the analytic approach is that the interrelations among parts are discounted,[22] and the system is not discussed as a whole. Rosnay emphasizes that the analytic approach might be weak when it comes to understanding complex systems.[23] A system is broken into sub-parts and is focused on differences among these parts in the analytic approach, while system thinking focuses on the commonality of parts and investigates patterns or models.[24] Thus, time-based changes in real world cases can be translated into models, and real-time intuitive forecasts can be developed by the adaptation of these models with the real world.[25]

In order to understand problems and find solutions, linear modelling may be sufficient for systems that have simple relations among parts, whereas system thinking and evolutionary modelling techniques are appropriate for more complex systems.[26] Table 1 summarizes some of the salient differences between traditional thinking (i.e., linear, classic or deterministic thinking) and systems thinking.[27]

Table 1: Differences between Traditional Thinking and Systems Thinking

Traditional Thinking	Systems Thinking
Isolates the system, disassembles it and focuses on it.	Takes the system as a whole and focuses on interaction among the parts.
Examines the nature of interactions among parts.	Investigates the effects of interactions among parts on the system.
Focuses on the accuracy of the details of system components.	Takes a holistic view of the system.
Predicts a change in a variable at a given moment.	Simultaneously predicts a change in a group of variables.
Uses time and events in a reversible way.	Uses time and events realistically, i.e., irreversibly.
Tries to verify the facts experimentally within the theoretical framework.	Tries to verify the facts by comparing the created model to reality.
Uses detailed, rigid models that are difficult to implement in real life.	Uses general, soft models that can be implemented easily.
It is effective when interactions among parts are linear and weak.	It is effective when interactions among parts are dynamic and strong.
Directs to individual discipline-oriented education.	Directs to multidisciplinary education.
Foresees application of detailed plans/programs.	Foresees goal-driven applications.
With the knowledge of the details, there are targets that are not fully defined.	Fuzzy details are available with the knowledge of goals.

Source: Joel de Rosnay, *The Macroscope: A New World Scientific System*, New York: Harper & Row, 1979, p. 74.

Among the methodologies employed to understand and define complex systems, the use of Viable Systems Model (VSM) and System Dynamics (SD) has expanded through many applications in various areas and industries. VSM is a functional tool that is very powerful in defining and developing the generic structure of complex systems, whereas SD is very useful in understanding the complex relationships and behaviors of components of a whole system.

VSM, developed by Beer, can be defined as a tool for modeling an organizational structure by taking the human nervous system as a base model. The model consists of Operational Units, Meta System and Environment. System 1 (Opera-

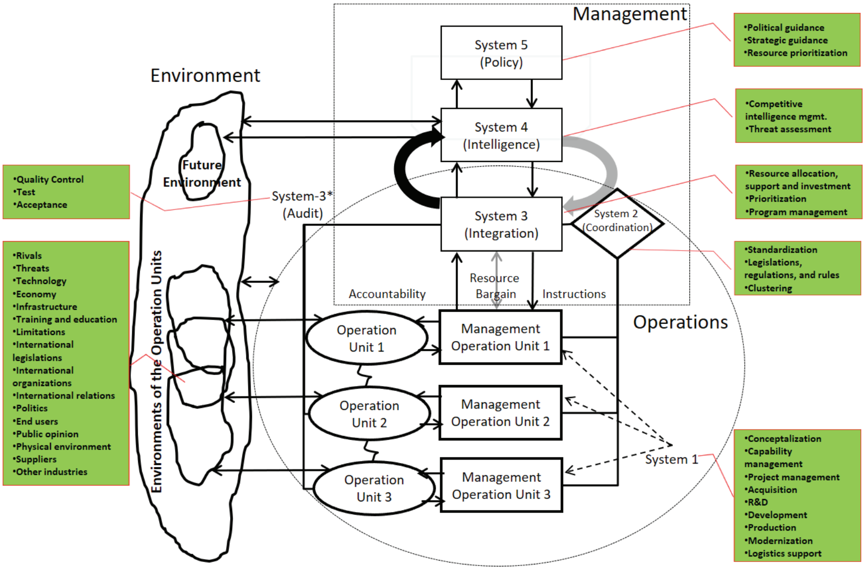
VSM is a functional tool that is very powerful in defining and developing the generic structure of complex systems, whereas SD is very useful in understanding the complex relationships and behaviors of components of a whole system.

tion) consists of autonomous units that execute main functions and processes to produce outcomes. System 1 can also be called 'system-in-focus.' System 2 (Coordination) are regulatory mechanisms that facilitate the coordination and integration of all the autonomous units' work and reduce possible conflicts among these units (i.e., information systems, production plans, programming tools, processes, procedures, etc.). System 3 (Integration) helps System 1 produce outcomes in coherence with the defined policies and strategies. System 3 allocates resources and creates synergy. System 3 also controls and evaluates effectiveness and efficiency by collecting data via its sub audit system, System 3*. System 4 (Intelligence) consists of mechanisms that observe and analyze the current situation and all possible future states, and making operational and strategic projections in order to adapt to the external environment. System 5 (Policy) is the highest level mechanism where policies and strategies are defined, interactions are managed between System 3 and 4, and an indirect relationship is established with System 1.[28]

VSM considers that all systems resemble each other because of the recursiveness feature. The capacity to understand and analyze complex systems and discuss those complex systems as analyzable and manageable recursive systems make VSM a robust analysis tool.[29]

Figure 1 illustrates the generic structure of the defense industry from a systems thinking perspective. This structure focuses on the essential dimensions and factors that must be considered to define a seamless and viable defense industry. Regardless of its area of activity, a viable defense industry can be constructed, reconstructed or evaluated via its environment and the five main systems provided by VSM, such as policy, intelligence, integration (and audit), coordination and operation.

Figure 1: Defense Industry Generic Structure



Source: Jose M. Perez Rios, *Design and Diagnosis for Sustainable Organizations*, Berlin: Springer-Verlag, 2012.

The defense industry operates in an open environment in which a plethora of factors and agents interact dynamically. These dynamic variables include rivals, threats, technology, economic factors, training and education, limitations, international legislation, international organizations, international relations, politics, end users, public opinion, physical environment, suppliers, other industries, etc. Strategic direction and guidance, in which political, strategic and resource-related priorities are clearly delineated, are needed as the starting point for a viable defense industry. In accordance with this guidance, a robust mechanism should continuously observe the operating environment (including the variables noted above) to execute intelligent threat assessment and management. Having made the necessary assessments, an integration function should be in place, wherein resource allocation, support, investments and prioritizations are made through a program management discipline. At the operation level of the defense industry, relevant stakeholders such as requirement authorities, acquisition bodies, main contractors and sub-contractors implement the primary processes (conceptualization, capability management,

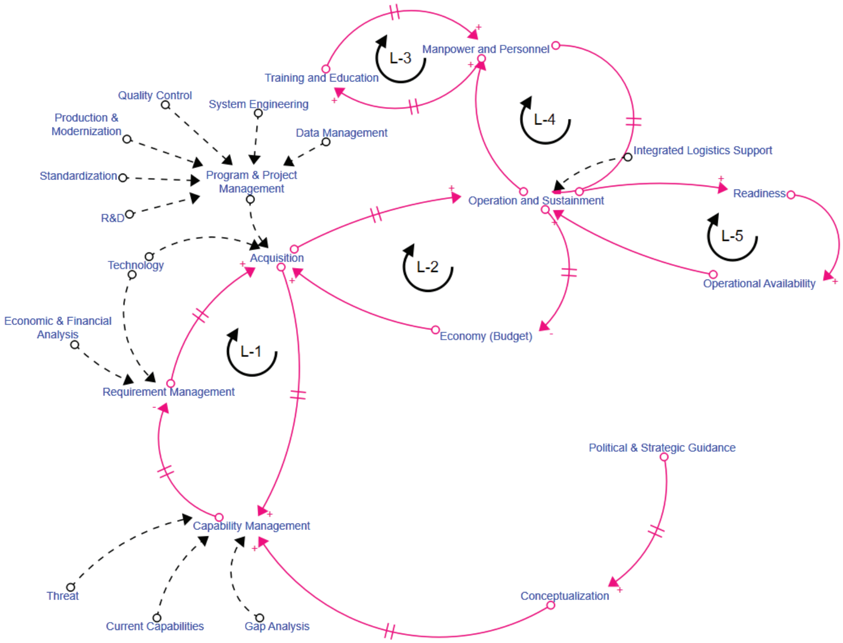
The defense industry operates in an open environment in which a plethora of factors and agents interact dynamically.

project management, acquisition, research and development, system development, system production, modernization and logistics support) that produce outcomes of the industry. These outcomes shall be controlled, tested and accepted by accountable authorities. The relationship between integration and operation is constructed via a coordination domain where standardization, legislation and clustering functions are executed.

System dynamics, developed by Jay Forrester in the 1960s, is a powerful methodology that may be used to understand and model complex systemic behavior, including the behavior of system components, and express those behaviors by means of differential equations. System dynamics methodology can be used successfully during the policy development process in complex system management for adapting to a complex environment. Comprehensive, simple and adaptive models can be created by the help of system dynamics.[30] System dynamics models provide foresight into behavior changes in a system over time. One of the strengths of system dynamics is its capability to capture feedback loops that inherently exist in complex systems, either in the form of positive (reinforcing) or negative (balancing) polarity.[31] Causal Loop Diagrams (CLD) are used for this purpose. These diagrams help us focus on the important feedback that is responsible for the complexity in the system.[32] Positive loops express a causal relation wherein a change in one variable causes a change in another variable in the same direction. Conversely, we see a change in the opposite direction within the negative loops. The polarities of the loops are denoted with "+" and "-" on the diagrams. Delays, as the most salient factors that create dynamics, are denoted with double stripes on the links. Feedback loops represent interactions among the parts of a system and enable better understanding of complex systems.

Figure 2 depicts a generic causal loop diagram for the defense industry. The casual flow starts with political and strategic guidance and continues through main nodes/variables (conceptualization, capability management, requirement management, acquisition, operation and sustainment, readiness and operational availability) that continuously provide feedback to each other.

Figure 2: Generic Causal Loop Diagram for the Defense Industry



The red lines in Figure 2 express direct connections, whereas dotted lines depict information flows within the above CLD that consists of five main loops. Loop-1 (reinforcing) covers the management of capabilities, requirements and acquisition, wherein a positive causality relationships exists, such that as the capability gap increases or decreases, the requirement increases or decreases; the rise or fall in requirement causes a corresponding increase or decrease in acquisition, and (positive) feedback flows to the capability variable. Loop-2 (balancing) depicts the relationships among acquisition, operation & sustainment and economy. In this loop, acquisition has an effect on operation & sustainment in the same direction; and operation & sustainment will affect economy in the opposite direction (i.e., an increase in operation & sustainment causes a decrease in economy), whereas economy and acquisition behave in the same direction (i.e., as the economy rises, acquisition rises too). Loop-3 (reinforcing) deals with the training and education of human resources, where both variables affect each other in the same direction (for instance; an increase in the number of personnel will increase the need for education and training and vice versa). A similar feedback flow exists in Loop-4 (reinforcing), in which operation & sustainment and human resources affect each other in the same direction. Loop-5 (reinforcing) is the last loop in the CLD, where any increase or decrease in operation & sustainment will cause affect the readiness and operational availability variables accordingly.

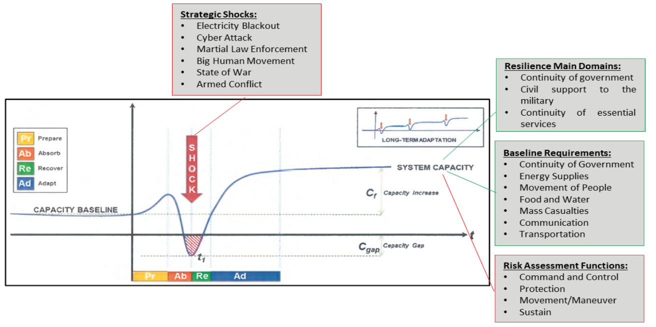
The basic CLD depicted in Figure 2gives an idea about the structure of the defense industry as a complex system. In other words, it clearly models what would happen within the overall system if any change in one of the variables were to occur. The CLD thus provides a picture of a mental model of the defense industry. Through the CLD structure, the behaviors of this complex system can be understood and modeled with the help of stocks and flows. Stocks and flows give an idea about the actual states of the complex systems by showing how the variables actually behave (in a non-linear way) in the event of specific decisions and actions within the defined structure.

An example of a defense industry application of the systems thinking approach and system dynamics methodology may be illuminative to show how a complex system or problem can be considered, conceptualized, structured and modeled. The "NATO Aggregated Resilience Model" developed by STM ThinkTech (Future Technology Institute) is an exemplary model. The subject of the model is 'resilience,' a complex and vague phenomenon that NATO has been in search of an innovative approach to deal with. Because of its complexity, NATO adopted systems thinking as an innovative approach to be used for the model development.

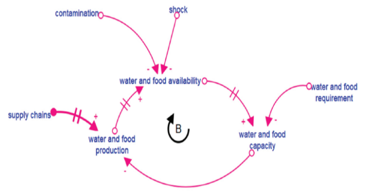
Figure 3 depicts the modelling process starting from articulating the complex system, modeling the structure and behavior of the system, and presenting the outcomes of the model via a strategic dashboard. In the model, the NATO's strategic resilience concept is addressed as a complex system. Strategic resilience is an adaptive process in which resilience performance is measured by absorbing strategic shocks (electricity blackout, cyber-attack, large-scale human movement etc.) with minimal risk effects (command and control, protection, movement, sustainability) while maintaining essential functions (continuity of government, civil support to the military, continuity of essential services) at an acceptable level, then recovering functionality within a reasonable time and at a reasonable cost. This complex system is understood and modeled via CLDs and stock and flow diagrams in which a considerable number of variables are interconnected. Then, a simulation model was developed with which users can create what-if scenarios and see the outcomes through various dashboards. The resilience model is capable of quantitatively representing the resilience-related factors of countries in a complex operational environment in a dynamic way.[33]

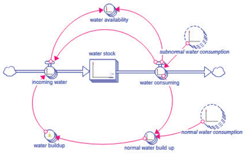
Figure 3: Generic Modelling Flow of Resilience

Articulation of complex system (Resilience)

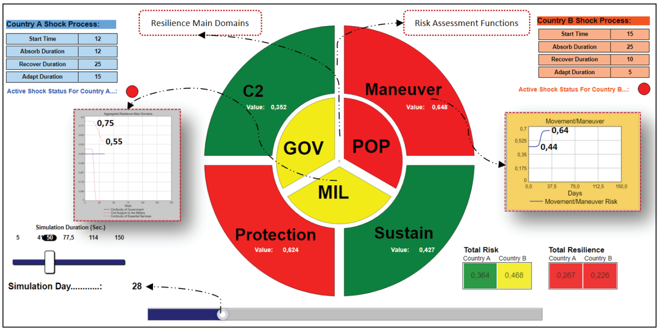


Understanding and modeling the structure (CLD) and behavior (stocks and flows) of the complex system


contamination
shock
water and food availability
supply chains
water and food production
B
water and food capacity
water and food requirement



Scenario-based strategic dashboard of the resilience model



Country A Shock Process:

Start Time	12
Absorb Duration	12
Recover Duration	25
Adapt Duration	15

Active Shock Status For Country A...:

Country B Shock Process:

Start Time	15
Absorb Duration	25
Recover Duration	10
Adapt Duration	5

Active Shock Status For Country B...:

Source: Jan Hodicky et al, "Dynamic Modeling for Resilience Measurement: NATO Resilience Decision Support Model," *Applied Science*, Vol. 10, No. 2639 (2020), pp. 1–10.

One of the critical outcomes of this aggregated model is its capacity to provide views on the future behavior of both the overall system itself and its sub-systems. Meadow et al. discuss such outcomes by providing a valuable threefold classification:[34]

- *Absolute, precise predictions*. The model provides realistic foresight about the consequences of one or more simultaneous, strategic shocks on baseline requirements by representing the impacts of those shocks with their behavioral shape, depth and length along the simulation period.

- *Conditional, precise predictions.* The model also synthesizes multi-domain dynamism; if there is a strategic shock(s), the model depicts its effect on a baseline requirement, as well as the impact that the affected baseline requirement will have on others.
- *Conditional, imprecise projections of dynamic behavior.* The model has the capacity to project the dynamic behavioral pattern of demands. For instance, users can review the communication demand patterns through ordinary states where everything is normal (steady-state pattern) and through extraordinary situations where a cyber-attack shock takes place (increasing inclination pattern).[35]

System dynamics models were inspired by and stem from the practical world of normal managerial domains such as economics, politics and defense and security. It does not begin with abstract theory, nor is it restricted to the limited information available in numerical form. Instead, system dynamics uses the descriptive knowledge of the operating arena about structure, along with available experience about decision-making as inputs. Such inputs are augmented where possible by written description, theory and numerical data. For example, feedback theory is one of the prominent theories used as a guide for selecting and filtering information to yield the structure and numerical values for a dynamic simulation model. These dynamic models are good for tackling complex intuitive or mathematical problems, as their advanced features are capable of simulating an almost infinite number of parts of a system to determine how they will interact with one another to produce changing patterns of behavior.

System dynamics models were inspired by and stem from the practical world of normal managerial domains such as economics, politics and defense and security.

Conclusion

The ever-increasing volume of complexity aggravates the challenges for the decision support processes within the defense industry.[36] Therefore, the defense industry, with its dynamically interconnected agents (environmental factors, stakeholders, legislation, standards, operations, etc.), should be addressed and studied by means of innovative approaches and methodologies. A systems thinking approach, together with VSM and system dynamics methodologies can be deemed among those innovative approaches. Many successful applications in various areas such as the NATO aggregated resilience model mentioned above can be benchmarked in the development of new mental models and creative solutions.

A Systems Thinking approach and System Dynamics methodology can be used for structuring complex defense phenomenon, formulating the interrelationships among defense industry actors, and developing dynamic models. Although generic processes have already been mentioned, some of the high-level modelling points can be touched as: (1) Relevant mental and written information, experience, and judgements shall be gathered from the defense industry ecosystem with participatory techniques such as a community-based modeling approach; (2) A specific subject or problem shall be identified; (3) The identified subject or problem shall be framed in terms of pattern of behavior over time via scientific thinking; (4) Closed-Loop thinking shall be implemented by viewing and quantifying causality as an ongoing process, not a one-time event; (5) The behavior of the defense industry shall be evaluated via the interactions of its components.

The proposed approach and methodology for the conceptualization and contextualization of the defense industry provides the following potential benefits:

- Unique and applicable approaches for both theorists and practitioners in the defense sector so that they could be able to possess a comprehensive look
- A powerful methodology to translate and reflect tacit knowledge and mental models about defense and security into usable models and tools;
- A clean lens through which to see the complex interconnectedness among various agents in the sector;
- A functional tool to understand and evaluate dynamic behavioral relations among those agents (i.e., which causes create which effects, and how);
- A supportive means for approaching political and strategic level decision-making processes and procedures by providing:
    - Understanding of the interdependencies among defense industry agents (different domains, stakeholders, different aspects, etc.);
    - Use of all available related datasets as inputs in various formats, including graphical behavior inputs;
    - Ability to analyze alternative options and evaluate courses of action across different domains;
    - A realistic multi-domain picture (i.e., of the defense industry itself);
    - A model where almost limitless what-if scenarios can be created and tested within that multi-domain picture;
    - Understanding of the potential intended and unintended effects of decisions;

- Mitigating biased decision-making probability
- Superior situational awareness that includes interdependencies and trends;
- A risk-free and cheap environment to make all the necessary tests before executing the decisions in the real operational arena;
- State-of-the-art and lean visualization of analysis and synthesis results.

The inevitable decision support needed by policy- and decisionmakers who seek innovative means in the defense industry can be met by the systems thinking approach and system dynamics methodology discussed in this article. In the future, the most likely applications for this approach and methodology will be in the areas of: (1) defense planning and programming, (2) defense acquisition, (3) defense investment and (4) the operation and maintenance of defense platforms.

Last but not least, the discussion presented in this article should help to increase situational awareness about the existence of new paradigms (systems thinking and system dynamics) that could be gainfully utilized within the defense industry. The application of these paradigms will add value to the defense industry as a whole ecosystem.

Endnotes

1 John E. Thomas, Daniel A. Eisenberg & Thomas P. Seager, "Holistic Infrastructure Resilience Research Requires Multiple Perspectives, Not Just Multiple Disciplines," *Infrastructures*, Vol. 3, No. 3 (2018), pp. 1–18.

2 Martin Reynolds & Sue Holwell (eds.), *Systems Approaches to Managing Change: A Practical Guide*, London: Springer, 2010.

3 Sergio Gallego-García, Jan Reschke & Manuel García-García, "Design and Simulation of a Capacity Management Model Using a Digital Twin Approach Based on the Viable System Model: Case Study of an Automotive Plant," *Applied Sciences*, Vol. 9, No. 24 (2019), pp. 1–15.

4 Daniel Lafond et al., "Training Systems Thinking and Adaptability for Complex Decision Making in Defence and Security," *IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support*, New Orleans, 2012.

5 Reynolds & Holwell, *Systems Approaches to Managing Change*.

6 Dietrich Dorner, *The Logic of Failure: Recognizing and Avoiding Error in Complex Situations*, New York, NY: Basic Books, 1997); Peter M. Senge, *The Fifth Discipline*, New York, NY: Currency Doubleday, 1990.

7 Pin Chen & Mark Unewisse, "A Systems Thinking Approach to Engineering Challenges of Military Systems-of-Systems," *Joint & Operations Analysis Division Defence Science and Technology Group*, Canberra, 2016.

8 Ibid.

9 Jim Duggan, *System Dynamics Modeling with R*, Switzerland: Springer, 2016.

10 B. Richmond, *An Introduction to System Thinking*, Isee Systems Inc., 2004.

11 Michael C. Jackson, "Fifty Years of Systems Thinking for Management," *Journal of the Operational Research Society*, No. 60 (2009), pp. 24–32.

12 Irene CL Ng, Roger Maull & Nick Yip, "Outcome-based Contracts as a Driver for Systems Thinking and Service-dominant Logic in Service Science: Evidence from the Defence Industry," *European Management Journal*, Vol. 27, No. 6 (2009), pp. 377–387.

13 Hans Daellenbach & Donald McNickle, *Management Science: Decision-making through Systems Thinking*, New York: Palgrave Macmillan, 2005.

14 Ng, Yip & Maull, "Outcome-based contracts as a Driver for Systems Thinking."

15 Christina Mele, Jacqueline Pels & Francesco Polese, "A Brief Review of Systems Theories and Their Managerial Applications," *Service Science*, Vol. 2, No. 1–2 (2010), pp. 126–135.

16 Reynolds & Holwell, *Systems Approaches to Managing Change*.

17 Chen & Unewisse, "A Systems Thinking Approach to Engineering."

18 Reynolds & Holwell, *Systems Approaches to Managing Change*.

19 Gary Bartlett, "Systemic Thinking: A Simple Thinking Technique for Gaining Systemic (Situation-Wide) Focus," in *Breakthroughs 2001: Ninth International Conference on Thinking*, Auckland, 2001.

20 Joel de Rosnay, *The Macroscope: A New World Scientific System*, New York: Harper & Row, 1979.

21 Heiki Hyötniemi, "Information and Entropy in Cybernetic Systems," 2005, http://neocybernetics.com/publications/pdf/step6.pdf.

22 Bartlett, "Systemic Thinking."

23 Rosnay, *The Macroscope*.

24 Bartlett, "Systemic Thinking."

25 John Stewart, *Evolutions Arrow*, Canberra: The Chapman Press, 2000.

26 Yavuz Ercil, *Systems and Systems Thinking*, Canada: Trafford Publishing, 2020.

[27] Ibid.

[28] Rios, *Design and Diagnosis for Sustainable Organizations*.

[29] Jon Walker, "The Viable Systems Model: A Guide for Co-operatives and Federations," 2001, http://www.greybox.uklinux.net/vsmg_2 2.

[30] Daellenbach & McNickle, *Management Science Decision-making through Systems Thinking*.

[31] John Sterman, *Business Dynamics: Systems Thinking and Modeling for a Complex World*, Boston, MA: McGraw-Hill, 2000.

[32] Ibid.

[33] Jan Hodicky et al., "Dynamic Modeling for Resilience Measurement: NATO Resilience Decision Support Model," *Applied Science*, Vol. 10, No. 2639 (2020), pp. 1–10; Jan Hodicky et al., "Analytic Hierarchy Process (AHP)-Based Aggregation Mechanism for Resilience Measurement: NATO Aggregated Resilience Decision Support Model," *Entropy*, Vol. 22, No. 1037 (2020), pp. 1–13.

[34] Dennis L. Meadows et al., *Dynamics of Growth in a Finite World*, Cambridge, MA: Wright-Allen Press, 1974.

[35] Duggan, *System Dynamics Modeling with R*.

[36] Ercil, *Systems and Systems Thinking*.

ARTICLE

National Security 2.0: The Cyber Security of Critical Infrastructure

A. Burak DARICILI [*] & Soner ÇELİK [**]

Abstract

Thanks to technological advancements in recent years, critical infrastructure has become both irreplaceable for modern social life—and highly vulnerable. Safe, effective and efficient management of critical infrastructure is a sign of a state's social welfare and economic development. Ensuring the security of critical infrastructure is essential for national security, and is becoming ever more dependent on network technology. Indeed, providing for the cybersecurity of critical infrastructure, i.e., protecting it from cyber attack, is the chief goal of modern states' cybersecurity strategy. The present study aims to reveal the importance of ensuring the cybersecurity of critical infrastructure within the scope of national security. First, the relationship between the concept of national security and cyber threats is scrutinized from a realist perspective. The interaction of the critical infrastructure concept and cybersecurity is then analyzed from a theoretical and technical point of view. In addition to official documents published by the United States, which has the world's most advanced cybersecurity infrastructure, the study includes definitions of related concepts published by Turkey, a country that has made significant progress in recent years in terms of the cybersecurity of its critical infrastructure.

Keywords

Critical infrastructure, cybersecurity, cyber attack, national security, realism.

[*] Associate Professor, Bursa Technical University, Department of International Relations, Bursa, Turkey. E-mail: ali.daricili@btu.edu.tr. ORCID: 0000-0002-3499-1645.

[**] PhD, Süleyman Demirel University, Department of International Relations, Isparta, Turkey, E-mail: sonercelik85@gmail.com. ORCID: 0000-0001-7554-5628.

Received on: 08.06.2021
Accepted on: 18.10.2021

Introduction

Critical infrastructure refers to the physical and virtual systems that underlie modern societies, and are vital for their survival. Providing for the security of these systems is an essential part of the national security strategies of modern states. The safe and effective management of critical infrastructure is an indicator of a state's social welfare and economic development. Today, the security of critical infrastructure is heavily dependent on network technologies; accordingly, providing for the cybersecurity of a state's critical infrastructure is synonymous with national security. Protecting critical infrastructure against cyber attacks is thus crucial for maintaining daily life, as it ensures the provision of essential public services and reliable commercial and financial transactions.[1]

The process of managing critical infrastructure by means of network technologies, which are mainly operated by mechanical systems under human supervision, has accelerated since 1990, with the rapid commercialization and demilitarization of the internet under the leadership of the U.S. As a result, in the same period, cybersecurity strategies began to be developed at the national and international level. Many countries in the international system now have cyber defense and attack capacities commensurate with their developmental level and economic potential. Since the 2000s, states have endeavored to improve their cyber-attack capacities in various ways, e.g., through space espionage and counter espionage, the spread of disinformation using web-based platforms, the development of electronic warfare skills, perception management and the dissemination of propaganda. In addition to states, many international organizations and companies have developed cybersecurity plans within their fields of activity in tandem with their goals.

The importance of critical infrastructure was first emphasized in U.S. Presidential Policy Directive 63 (PPD-63), accepted by President Bill Clinton in 1998. Since that time, many countries, notably the U.S., have addressed the security of critical infrastructure in their codes, official plans and strategy papers.[2] Many measures, evaluations and recommendations with titles related to the cybersecurity of critical infrastructure have been and continue to be circulated in the realm of legal regulations, and in states' plans and strategy documents, as a result of the ongoing emergence, proliferation and diversification of cyberspace-based threats.

There have been many concrete instances of cyber attacks targeting states' critical infrastructure. Many of these occurred in the 2000s, before awareness had developed as to the nature of this kind of threat. To provide an example, at the end of the Cold War, the tension between Russia and Estonia that had begun in response to Estonia's rapprochement with the North Atlantic Treaty Organization (NATO) alliance became heightened due to Estonia's decision to remove a Soviet-era statue from Tallinn Square. Immediately after this decision, a large-scale Distributed Denial of Service (DDoS) attack was launched against Estonia's critical infrastructure. The cyber attacks aimed to collapse the country's internet infrastructure by targeting the websites of Estonia's political parties, its state institutions, parliament, media organizations, banking and financial systems. The internet sector of Estonia's critical infrastructure became unserviceable for a week as a result of the attacks. Estonia recovered with the help of NATO, and the decision to close access to Estonia's national web from abroad.[3]

There have been many concrete instances of cyber attacks targeting states' critical infrastructure. Many of these occurred in the 2000s, before awareness had developed as to the nature of this kind of threat.

In another instance, a cyber attack involving the Stuxnet Virus was launched against Iran's nuclear installation in Natanz in June 2010; the installation was physically damaged and the development of its nuclear energy capacity was delayed as a result. Although Iran blamed the U.S. and Israel as the backers of the attack, no one has claimed responsibility to date.[4]

Other examples of cyber attacks targeting critical infrastructure were observed during Russia's intervention in Ukraine, which began in 2014. The use of mobile phones in Crimea in the first days of close combat in March 2014 was prevented by destroying the infrastructure of Ukrtelecom, Ukraine's official mobile phone company. Another cyber attack was carried out against a power plant in the Prykarpattyaoblenergo Region of Ukraine on December 23, 2015, causing a power outage there. According to Ukraine's allegations, these cyber attacks were conducted by Russian intelligence services and affiliated hacker groups.[5]

Another example of cyber attacks targeting a state took place in Turkey. On November 24, 2015, Turkish F-16s shot down a Russian Su-24 fighter jet for violating Turkish airspace—an incident that created significant political tension between Turkey and Russia. The tension increased in December 2015 when "DDoS" cyber attacks aimed to erode Turkey's critical infrastructure, including its banking and finance systems, public institutions and e-state, by targeting the bandwidth used by the system where ".tr" extension names are kept. The attacks had the potential to affect 400,000 websites in Turkey. Russia is alleged to have been behind those attacks, but has not recognized such claims.[6]

As these concrete cases indicate, organized cyber attacks can target the virtual/ technological systems used in managing critical infrastructure. National intelligence services and/or various hacker groups may be associated with these attacks, which can be almost impossible to trace. And there are many more such examples. The remarkable point here is that today, states can organize cyber attacks against rival or adversary states by targeting critical infrastructure, rather than purely military targets. Indeed, critical infrastructure is now seen *as* a military target against which a state can organize cyber attacks. This situation is a development arising from the use of systems based on network technologies with cyber space-based technological developments to manage critical infrastructure.

It is a logical development within this context that states have begun to provide for the security of critical infrastructure as a crucial component of their national security strategies. States aim to protect their critical infrastructure by means of various plans, institutional structuring, legal regulations and strategy papers. And in addition to providing cybersecurity for their own critical infrastructure, several states have developed the capacity to carry out cyber attacks that can damage the critical infrastructure of adversary states as an important target.

Relations between the concept of national security and cyber threats will be discussed in this context from a Realist perspective in this study. Subsequently, the interaction of the critical infrastructure concept and cybersecurity will be analyzed from a technical and theoretical perspective, drawing upon definitions of these and related concepts found in official documents published by the U.S. and Turkey.

National Security and Cyber Threats in terms of the Realist Paradigm

Although the national security concept emerged as the result of the political conditions of the 20th century, the intellectual foundations of this concept date back much farther, specifically to the era of the establishment of modern nation-states. The national security concept was first recorded in U.S.-based official documents and academic studies after WWII; U.S. national security in the period after 1950 focused on coordinating between government agencies to address the nation’s threats and interests. The national security concept, as a key component of ensuring the collective security of NATO member states during the Cold War years, was fundamentally defined within the context of the struggle against Communism.[7] In studies conducted during this period, national security was defined mainly from a historical, military perspective.

Over time, it developed into a reference that countries use to determine their domestic and foreign policies. The national security concept, in its current form, includes both domestic and foreign policy elements.

In the post-Cold War era, the national security concept was redefined in the literature in light of the disintegration of the bipolar political system and ideological point of view, along with the emergence of new-generation threats, and the desire to promote liberal values and develop free trade.

In the post-Cold War era, the national security concept was redefined in the literature in light of the disintegration of the bipolar political system and ideological point of view, along with the emergence of new-generation threats, and the desire to promote liberal values and develop free trade. Because the national security concept developed in different states with different perspectives, it became more controversial in the post-Cold War era. Across decades, many different schools analyzed whether security is/should be individual, national or international. The modern approach tends to be critical of any security mentality that discusses national security solely from a military perspective, and a more human-centered national security mentality has come into prominence.[8] The national security concept, after moving away from its military debut, has been discussed from points of emphasis such as economic security, health safety, individual safety, food security, societal security, environmental safety and cyber safety. This new theoretical point of view has vastly extended the scope of the security concept. To provide an example, Buzan highlights the need to analyze the political, economic, social, environmental and military dimensions of security.[9]

The intellectual foundations of Realist national security policies were built on the premise that people act with motives such as interest, greed and power, contrary to Idealist approaches. Realists argue, in contrast to what the Idealists claim, that it is almost impossible to change human nature at the point of ensuring security. Instead of changing human nature, then, it should be accepted that humans are human, and the negative sides of human nature should be acknowledged and addressed by politics. Only then, we can talk about ensuring security of the people.[10]

Intellectuals such as Thomas Hobbes, Niccolò Machiavelli and Jean-Jacques Rousseau had a pessimistic perspective that can be applied to the ways in which national security needs to be understood. Those intellectuals accepted the international system as an area where states continuously fight with each other to pursue their own selfish interests. For this reason, it is impossible to establish universal peace, as the Idealists desire. This line of reasoning is accepted by Realists such as Carr and Hans Morgenthau; in their view, the only way to prevent a state from becoming a hegemon in the international system, where there is a constant conflict of interests among states, is for states to balance each other's power.[11] The pessimistic viewpoint of classical Realists is accepted by neo-realists such as Kenneth Waltz and John Mearsheimer, according to whom security or insecurity is a result of the anarchic nature of the international system on a large scale. Therefore, international policy will continuously sustain a tendency to violence.[12]

The Realist political approach accepts states as the main actors of the international system; since the interests of each country differ from each other, there is always the possibility of war, and some kind of conflict or fighting is inevitable. The Realist approach defines the international system as anarchic, and characterizes international policy as a power struggle in which security is the main agenda item in the realm of international relations. In this respect, the security concept for Realist theoreticians is discussed through "insecurity" in general terms, and this theoretic approach is explained via themes of power, threat and insecurity.

Cyberspace-based developments, today, propose new approaches to states' threat, security and deterrence agendas. Some states have even begun to see cyber attack and cyber conflict as important methods of engaging in strategic defense and inflicting damage on their opponents. Developments in cyberspace bring along new security risks; the importance of removing these risks has thus also increased, compelling states to develop strategies to address this issue. For Realist theorists, this makes the international system even more uncertain and anarchic than before, especially given that cyber attacks can be caused not merely by states but by individuals.[13]

In Realist terms, the diversification of risks to cyberspace resources, and the inability to determine the source of these risks, deepens the anarchic structure of the international system. A cyberspace attacker can hide his or her identity by using various forms of crypto software and programs. The attacker can even conduct a "false flag"[14] operation, making it appear that the source of the cyber attack is another state or a state-sponsored hacker group by using similar software. All of these circumstances deepen the insecurity of the international system and reinforce the mutual distrust between states.

Power struggle and competition in the international system have expanded into a new dimension thanks to internet-based developments. Many states have used these technologies as an opportunity to develop their hard power. Improving military power with the help of cyber-based technology and skill has become an important goal for these states. Allocating budgets, making investments, training experts and establishing cyber military commands in tandem with conventional army development are now essential for states in order to reach a powerful attack and defense capacity in cyberspace.[15]

All of these developments contribute to what Realists call the "security dilemma," a phenomenon whereby "many of the instruments that are used by a state to increase its security decrease the security of others."[16] And it is ongoing. When one state makes a military investment or takes a military measure, this is taken as a threat by another state, which then applies similar measures, which in turn are interpreted by other states as a threat. The threat perceptions of states vis-à-vis one another escalate, in some cases leading to an armament race with mutual measures taken back and forth.[17]

Based on the security dilemma concept, states evaluate international relations as a zero-sum game, and plan their behavior patterns in the international system based on the assumption of relative earnings. They also avoid cooperation by asking the question, "who will benefit more?" instead of, "how can we both profit?" As indicated above, the Realist approach adopts a competitive and confrontational security perspective on the axis of anarchy. Given the rigidity of this perspective, the limitations and difficulties of cooperation in the Realist paradigm come into prominence. Because the structure of the international system is anarchic, according to this approach, this insecure environment prevents states from cooperating in the long term,[18] a situation exacerbated by the anonymous structure of cyberspace and its accompanying uncertainties, which diversify and deepen risks.

Concerning all these evaluations, the mentality that has started to gain credence recently is that critical infrastructure is an inseparable part of a state's cybersecurity and thus its cybersecurity strategies. This perspective is clearly emphasized in the national cybersecurity documents of many states. For example, Turkey's National Cyber Security Strategy (2020–2023) Document states, "*Cybersecurity is an inseparable part of national security. Providing national security in an absolute manner depends on achieving [our] goals in the cybersecurity field.*"[19] As mentioned above, the security of critical infrastructure and information systems that are mostly managed by internet technologies has become vital to the security of any state. States, now, are aware that cyber attacks targeting critical structures can be a serious threat, and that such attacks can negatively affect their political, economic and military security.

The Relationship between Critical Infrastructure and Cyber Security

Critical infrastructure has two dimensions in terms of cybersecurity: defense and attack. Let us look first at the cyber defense and security dimension. Rapid development in network technologies has led to decisions to manage the critical infrastructure vital to a state's national security and public functioning by means of operating systems that rely heavily on internet technologies. Therefore, states that are in a power struggle within the international system may inflict damage on sectors of each other's critical infrastructure, accepting them as military targets. It is now a necessity for a state to protect its critical infrastructure against cyber attacks by investing in the defense capacity of these systems and endeavoring to provide security for them.

The other dimension is cyber attack capacity. A state may wish to completely or partly damage the critical infrastructure of an adversary state by seeking opportunities and improving skills in this capacity and organizing covert operations. A state may prefer this mode of attack due to the anonymous structure of cyberspace; it is almost impossible to prove allegations or to find concrete evidence of a cyberspace attack in terms of international law.

As noted above, a state's critical infrastructure might be exposed to various civil and military threats in terms of both its cyber defense and cyber attack capacity. Since critical infrastructure sectors are now evaluated within the scope of strategic systems that need to be protected at the national level, they are accepted as sensitive targets. To provide an example, Turkey's National Cyber Security Strategy (2020–2023) goals include "implementing regulations for the protection of critical infrastructure sectors; developing cyber risk management and emergency plans; ensuring that internet traffic, whose source and target is domestic, remains in the country; and discussing cybersecurity within the scope of national security."[20] Even collective security organizations, such as NATO and the European Union (EU), take measures to protect critical infrastructure against cyber risks and attacks.

Critical infrastructure is defined differently in various approaches; the common trait of all the approaches identify it as consisting of vital systems in terms of the functioning of the state.

Critical infrastructure is defined differently in various approaches; the common trait of all the approaches identify it as consisting of vital systems in terms of the functioning of the state. Regarding cybersecurity, each critical infrastructure system that is managed by internet technologies is a potential target of cyber attack. Critical infrastructure is defined in

Turkey's National Cyber Security Strategy and 2013–2014 Action Plan as "Infrastructures with information systems that may cause loss of life, large-scale economic damage, national security gaps or disruption of public order when the confidentiality, integrity or accessibility of the information it processes is impaired."[21] Turkey's 2016–2019 National Cyber Security Strategy specified the sectors that comprise critical infrastructure as follows: "electronic communications, energy, water management, critical public services, transportation, banking and finance sectors."[22]

Critical infrastructure as defined in terms of U.S. legislation are sectors that would result in a weakening of the country's national defense and economic security if they were to fail or collapse. An official document prepared for the U.S. in 1997 identifies these sectors as (1) telecommunication; (2) electrical power supplies and gas and oil storage and production units; (3) banking and financial institutions; (4) transport units and components; (5) units from which water is supplied; (6) emergency service units including emergency medical response units, general law enforcement, fire and search and rescue units; (7) government services and institutions.[23]

The U.S. Patriot Act, which entered into force in 2001, defines critical infrastructure as "*Vitally important physical or virtual systems and assets that can create a detrimental effect on security, national economic security, national public health, or any combination of these in case of being inadequate or destroyed.*"[24] The U.S. Presidential Policy Directive—Critical Infrastructure Security and Resilience, accepted in 2013, specifies the sectors of critical infrastructure as "chemistry, commercial activities, communication, critical production, dams, the defense industry, emergency services, energy, finance, food and agriculture, public institutions, health, information technologies, nuclear reactors, materials and waste, transportation systems, water and wastewater."[25]

The U.S. defines its current critical infrastructure sectors as "*chemical industry, trading areas, communication, critical production facilities, dams, defense industry and production areas, financial services, emergency services, energy, food and agriculture, public health and maintenance, information technologies, nuclear reactor materials and waste, public buildings and areas, transportation systems, water and wastewater systems.*"[26]

Almost all of these critical infrastructure sectors—notably energy, telecommunications, transportation and water systems—are currently managed by utilizing internet technology infrastructure. These systems can be perceived as military targets when we consider that they are strategically important for a country. It is now possible to damage the critical infrastructure of an adversary state, causing chaos or turning its economy upside-down via cyber attacks.[27]

It is possible, in cyberspace, in which all these systems are interconnected, to collapse a state's critical infrastructure, i.e., to make a system based on mutual dependence unworkable, and thus start a cyber conflict. The general run of cyber attacks toward operational targets in cyberspace starts by perforating critical infrastructure systems that are managed by internet technologies,[28] as is evident in the cyber attacks against Estonia, Iran, Turkey and Ukraine.

Considering the risks above, protecting critical infrastructure and establishing cybersecurity entails the following considerations:[29]

- Providing security against physical and cyber threats that could destroy the operation of critical infrastructure.
- Being prepared for the environmental, social, economic and political effects that could emerge in the event of the disruption or failure of critical infrastructure arising from the system itself or from natural disasters; establishing coordination and work safety plans and action steps for this purpose.
- Evaluating the law enforcement personnel, fire stations, search and rescue and medical units that are involved in ensuring the security and functionality of critical infrastructure. Precautions should be taken to ensure continuance of function, and to maintain the mobility and preparedness of units that can intervene in the event of a critical infrastructure emergency.

Cyber Security of Critical Infrastructure

Conducting quality checks on the precautions that are taken to ensure the cyber and physical security of critical infrastructure is important, as is keeping the effectiveness of these measures up to date. Private companies and/or public enterprises apply penetration tests to specify the required measures. These tests model and simulate possible attacks against the system.

The effect of a "third eye," i.e., having an independent contractor company assess the safety measures, is essential in providing the security of critical infrastructure. The scope and currency of these measures is even more critical when it is considered that hackers' attack methods change day by day.

The effect of a "third eye," i.e., having an independent contractor company assess the safety measures, is essential in providing the security of critical infrastructure.

It is worth going into greater detail in regard to information systems, as these may require addition measures of protection. Information systems can be divided into two categories: data systems and communication systems. Some critical infrastructure sectors use publicly available information systems for service, while other aspects of their functioning are managed by private information systems called Industrial Control Systems (ICS). ICSs are used in critical infrastructure sectors such as electricity transmission/generation and distribution businesses, power and nuclear power plants, chemical factories, refineries, water and treatment plants and larger industrial complexes. Providing cybersecurity to industrial companies, rather than physical security alone, has grown in importance because of the digitalization trend and increasing demand for productivity. ICSs themselves are divided into two groups based on their topology and components; Supervisory Control and Data Acquisition (SCADA) systems and Distributed Control Systems (DCS).

Critical infrastructure information systems fall into four categories:

- Information Systems: Computer systems serving an institution and its stakeholders.
- Communication Systems: Systems that provide communication services to many institutions and organizations, consisting of components geographically spread over a very wide area.
- SCADA Systems: Systems that are used to centrally monitor and control the components of a geographically dispersed system.
- Distributed Control Systems (DCS); Systems with control components spread throughout the plant to monitor and control an industrial process limited to a specific facility and location. [30]

SCADA systems have been used for many years in the management and tracking of critical infrastructure installations such as dams, steam power plants and energy distribution units. SCADA systems had no connection with other networks in the 1970s and 1980s. There were no known information and communication technologies in SCADAs in those years—only technologies developed specifically for infrastructure. In the decades that followed, SCADA systems began to include standard software, hardware, operating systems and network protocols that are widely known and used today. Currently, many SCADA systems that manage and monitor critical infrastructure systems are associated with enterprise networks and the internet. SCADA systems have thus become open to cyber attacks, and the security of those systems is seriously questioned.

Industrial infrastructure information systems generally consist of a large number of different processes that are interrelated with and mutually reliant upon each other. This is because they are topologies that include multitier rather than flat network architecture; each layer is in communication with different layers associated with it, and each layer may vary in terms of mechanisms because of different security criteria. Therefore, a defense-in-depth mentality should be applied for multilayered topologies such as ICS. This mentality was developed based on the idea that all measures taken against cyber attacks will somehow be circumvented.

The defense-in-depth approach aims to minimize the success rate of a potential attacker by taking measures based on the requirements of each layer and its assets at the same time. The use of modern technologies in industrial infrastructure makes these systems more skillful, while the same technologies increase the potential for cyber threats by proliferating the possible attack surfaces of the systems. The "Purdue Model" layered network architecture was developed by Purdue University, Indiana, and was adapted to ICSs by the International Society of Automation (ISA)[31] both to keep the attack surfaces to a minimum and to make the management of control systems for each layer safer. There are private network security architectures for different ICS and SCADA systems, and various, modified versions of the Purdue model. The Purdue Model consists of 5 or 6 layers, depending on the reference source and notation. These layers are the Enterprise Demilitarized Zone (DMZ), Local Corporate Network, Supervisory, Control DMZ, Logical, Field and Instruments. Four main problems may be encountered in the field for each layer:

- Access Control
- Log Management
- Network Security
- Remote Access

Purdue Model layered architecture is based on the principle of separating Information Technology (IT) and Operational Technology (OT) networks into subnets. The goal is to provide controlled access (through INTER-VLAN routing or by establishing an Access Control List (ACL) or by creating isolated networks using other technologies) to subnets and restrict unnecessary access that could become a threat.[32]

With such systems, there is a need to continuously monitor and work to correct technical imperfections and deliver the required solutions. Implementing necessary precautions in a faultless manner is crucial for the security of critical infrastructure within the ongoing digitalization processes of modern life. Taking precautions that provide for the security of critical infrastructure must be seen as essential steps to be taken from the moment an organization is established, as cybersecurity precautions and applications are not components that can be added to systems later. Protecting critical infrastructure by means of software that is specially designed for SCADA systems is all-important to keeping crucial services functioning. Research and development (R&D) activities regarding the security of critical infrastructure must be supported in order to develop national software to prevent cyber attacks from adversary states and non-state actors. Conducting and financing R&D activities to ensure cybersecurity should be basic government policy. As a result of R&D activities, cybersecurity guidelines that can be used jointly by various sectors, and that contain consistent information should be prepared for critical infrastructure; standards should be established and good practices should be specified.

Moreover, the critical infrastructure sector itself needs to be expanded, as systems based on internet technologies have become more common in recent years, and have expanded to almost all areas of life. In this regard, the critical infrastructure sectors that need to be protected for a country with a developed internet infrastructure should include all systems pertaining to the defense industry, including "all communication systems, information systems and logistics systems; air defense and command control systems; cryptosystems; navigation, approach, landing, positioning and direction-finding systems; satellite and ground systems; space systems; manned and unmanned aerial vehicle systems,"[33] as well as critical systems pertaining to the functioning of society, such as:

banks, shopping malls, education and training campuses, public buildings and enterprises, hospitals, factories, refineries, oil pipelines, natural gas lines, drinking water pipelines, treatment facilities, fixed facilities installed on pipelines, liquefied natural gas facilities and warehouses, oil wells, large pump stations, weapon and military equipment factories and facilities, railways, highways, important bridges and crossings, large ports, marinas, airfields, navigation auxiliary stations, radar stations, national monitoring, information processing system centers, radio, radio link centers, dams, power plants, transformer centers, strategic mine treatment, and operation factories.[34]

Inflicting economic damage, tarnishing the reputation of the target state by making it appear weak, creating panic and fear in society and establishing an unsafe environment are the reasons such facilities may be selected as targets by a government or government-sponsored hacker group. Critical infrastructure facilities should not only be thought of as cyber attack targets, but as the priority targets of a conventional war that could be selected to affect the will and tenacity of the adversary state—or destroy it.

Cyber threats of the asymmetric type are on the rise; 79,790 information security violation incidents and 2,122 data leaks were reported by 70 organizations from 61 countries.

Cyber threats of the asymmetric type are on the rise; 79,790 information security violation incidents and 2,122 data leaks were reported by 70 organizations from 61 countries. Two-thirds of cyber attacks were concentrated on the critical infrastructure of G-7 member states, especially the U.S. The sectors most affected by the cyber attacks were public institutions, and private or public companies engaged in technology and financial activities. [35]

Cyber threat sources may be grouped into three categories: external attackers, in-house attackers and business partners. External attackers play a role in 80% of violations, and in 60% of such attacks, the attackers seize the target systems within minutes. However, determining 75% of the attacks within a few days is impossible.[36] And the scope of cyber attack risk is much greater when we consider that the statistical information given above includes only data that can be detected and reported.

Cyber attacks on critical infrastructure can cause vitally destructive/disruptive results. Those results directly affect end users, and threaten the strategic targets and national security of the countries in which they occur. It is thus essential to reduce the number of attacks on critical infrastructure and to implement and sustain effective protection methods. Moreover, it is now essential for states to create an integrated security strategy to protect critical infrastructure and to determine both cybersecurity and physical security measures, along with their requisite audit needs and methodologies.

States should adopt a comprehensive, integrated approach, in which risks and threats are evaluated from all angles and the roles of all relevant actors are defined for the periods before, during and after an attack. Such an approach should include international actors and all public and private sector stakeholders. Thinking like a hacker or a terrorist, the weakest and most sensitive points ought to be identified, the worst scenarios should be anticipated and prepared for, and the requisite practices to prevent and respond to these scenarios should be determined.

After establishing a structure that can organize all these elements, a model system is required. It must be decided who will react when and in what way, in the event of an attack. It is of great importance to consider and address these issues in detail. Priorities within this context include the determination of the steps necessary for prevention, protection and recovery.

Conclusion

The first hacking events were performed for personal interest in the 1990s; today, the activities of government-sponsored or individual hackers have spawned a new generation of threats on a global scale. It has become very important to provide for the physical and cybersecurity of critical infrastructure sectors that render essential services for living and working within the scope of evolving security paradigms. Cyberspace is now understood as a new field of struggle on the state level.

International security approaches will continue to evolve as new technological advancements emerge. Cyber security-centered developments will play a significant role within this process. Investments in cyber defense and attack capacities will increase in the ongoing competition and power struggle within the international system, which will in turn affect states' mutual threat perceptions. Generating cybersecurity strategies and practicing them will continue to increase in importance as states develop their cyber security-oriented political approaches.

Attacks by governments, government-sponsored hacker groups and independent hackers on digital systems are becoming more complex and sophisticated day by day.

Attacks by governments, government-sponsored hacker groups and independent hackers on digital systems are becoming more complex and sophisticated day by day. Hackers who infiltrate and damage critical infrastructure by benefiting from system gaps have started to act like cyber warriors, receiving state support for their efforts. The scope of the threats they pose has expanded, as modern societies are much more dependent than ever before on complex and widely used internet-based technologies.

States and international organizations today focus on precautions against cyber attacks much more intensely than in the past. As a matter of course, it is hard for critical infrastructure sectors to always be prepared for asymmetric cyber attack threats. It goes without saying that there is a need for close cooperation between the government and private companies to effectively guarantee the cybersecurity of the critical infrastructure systems of the public and private sectors.

The confidentiality of the measures a state develops to ensure the cybersecurity of its critical infrastructure can be accepted as the fundamental principle. However, there is also a need for international cybersecurity alliance and cooperation based on the principle of mutual dependence when the universality of cyberspace is considered. Thus, the cybersecurity of shared, critical infrastructure is not only a national issue—it requires international cooperation.

Most cyberspace threats consist of more than one variable; the multidimensionality of the new generation of threats arising due to technological developments obliges a new and wide range of approaches in countries' national security strategies. Providing for the cybersecurity of critical infrastructure sectors that are now seen as military targets is crucial for governments to survive. Especially in the last 20 years, critical infrastructure has relied more heavily on processes dependent on network technologies; this circumstance has made the provision of cybersecurity for critical infrastructure a very important goal of states' national security strategies. Developing cyber defense and attack capacity in determining states' national defense strategies is now more necessary than ever.

Many states prepare strategies, make plans, establish special institutional structures and reform their armed forces to improve their cyber defense and attack capacity regardless of their economic size, military capacity or level of technological development. The main reason for following cyberspace-based developments so closely and trying to get involved in these processes is the power struggle and military competition among states within the scope of the Realist paradigm. States, and even collective security organizations such as NATO, have accelerated their plans to develop an effective cyber attack and defense capacity by utilizing network technology-oriented developments.

This study researched why providing security for critical infrastructure is vital for ensuring national security. We revealed that the security of critical infrastructure has become increasingly dependent on network technologies. In light of the above analysis and evaluations, the conclusion is that providing the cybersecurity of a state's critical infrastructures is of vital importance in ensuring its national security, as states have begun to accept each other's critical infrastructure as a military target within the scope of their power struggle in the international system. Thus, states are now increasing their investments in cyber defense and attack capacities. It is clear that ensuring the cybersecurity of critical infrastructure will continue to increase in importance in terms of state security as network technology-centered developments continue to evolve.

Endnotes

1 Tarık Ak, "İç Güvenlik Yönetimi Açısından Kritik Altyapıların Korunması," *ASSAM Journal*, Vol. 7, Special Issue (2019), pp. 42–45.

2 "Presidential Decision Directive / NSC-63," *Federation of American Scientists*, 1998, https://fas.org/irp/offdocs/pdd/pdd-63.htm.

3 Ali Burak Darıcılı, "Rusya Federasyonu Kaynaklı Olduğu İddia Edilen Siber Saldırıların Analizi," *Uludağ Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, Vol. 7, No 2 (May 2014), pp. 5–7.

4 Ali Burak Darıcılı, *Siber Uzay ve Siber Güvenlik: ABD ve Rusya Federasyonu'nun Siber Güvenlik Stratejilerinin Karşılaştırmalı Analizi*, Bursa: Dora, 2017, pp. 104–105.

5 Ibid, pp. 222–223.

6 Ibid, pp. 225–228.

7 Fikret Birdişli, "Ulusal Güvenlik Kavramının Tarihsel ve Düşünsel Temelleri," *Sosyal Bilimler Enstitüsü Dergisi*, No. 31 (2011/2), p. 150.

8 Ibid, p. 152.

9 Barry Buzan, *People, States and Fear: The National Security Problem in International Relations*, Chapel Hill: University of North Carolina Press, 1983, pp. 214–242.

10 Laurie M. Johnson*, Political Thought: A Guide to the Classics*, Belmont: Wadsworth/Thomson Learning, 2002, p. 49.

11 John Baylis, "Security Concept in International Relations," *International Relations*, Vol. 5, No. 18 (Summer 2008), p. 71.

12 Ibid, p. 72.

13 Darıcılı, *Siber Uzay ve Siber Güvenlik*, pp. 40–41.

14 A false flag operation is an act committed with the intent of disguising the actual source of responsibility and pinning blame on a second party. The term "false flag" originated in the 16th century as a purely figurative expression meaning "a deliberate misrepresentation of someone's affiliation or motives." It was later used to describe a ruse in naval warfare whereby a vessel flew the flag of a neutral or enemy country in order to hide its true identity. The term today extends to include countries that organize attacks on themselves and make the attacks appear to be perpetrated by enemy nations or terrorists, thus giving the nation that was supposedly attacked a pretext for domestic repression and foreign military aggression.

15 Anthony Craig & Brandon Valeriano, "Realism and Cyber Conflict: Security in the Digital Age," *E-IR*, February 3, 2018, https://www.e-ir.info/2018/02/03/realism-and-cyber-conflict-security-in-the-digital-age/.

16 Robert Jervis, "Cooperation under the Security Dilemma," *World Politics*, Vol. 30, No. 2 (1978), p. 168.

17 Charles L. Glaser, "When are Arms Races Dangerous? Rational versus Suboptimal Arming," *International Security*, Vol. 28, No. 4 (2004), p. 44.

18 Kenneth Waltz & George H. Quester, *Uluslararası İlişkiler Kuramı ve Dünya Siyasal Sistemi*, Ankara: A.Ü. Siyasal Bilgiler Fakültesi, 1982, pp. 44–47.

19 *Ulusal Siber Güvenlik Stratejisi ve Eylem Planı* 2020–2023, Ankara: T.C. Ulaştırma ve Altyapı Bakanlığı, 2020, p. 22.

20 Ibid, p. 10.

21 "Ulusal Siber Güvenlik Stratejisi ve 2013–2014 Eylem Planı," *Haberleşme Genel Müdürlüğü*, https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/some-2013-2014-eylemplani.pdf, p. 9.

22 *Ulusal Siber Güvenik Stratejisi 2016-2019*, Ankara: T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, 2016, p. 8.

23 "The Report of the President's Commission on Critical Infrastructure Protection," *Federation of American Scientists*, October 1998, https://fas.org/sgp/library/pccip.pdf.

24 "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act," *US Congress*, 2001, https://www.congress.gov/bill/107th-congress/house-bill/3162

25 "Presidential Decision Directive / PPD 21, 2003," *Obama White House*, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

26 "Critical Infrastructure Sectors of the USA," *CISA*, 2021, https://www.cisa.gov/critical-infrastructure-sectors.

27 Seda Yılmaz & Şeref Sağıroğlu, "Siber Saldırı Hedefleri ve Türkiye'de Siber Güvenlik Stratejisi," *6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı*, Ankara, 2013, pp. 323–326.

28 Kris Hemme, "Critical Infrastructure Protection: Maintenance is National Security," *Journal of Strategic Security*, Vol. 5, No. 8 (2015), p. 25.

29 "Critical Foundations Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection," *Federation of American Scientists*, 1997, p. B-1, https://sgp.fas.org/library/pccip.pdf.

30 "TÜBİTAK Kritik Bilgi Sistem Altyapıları için Asgari Güvenlik Önlemleri Dokümanı," *Haberleşme Genel Müdürlüğü*, https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/kritik-bilgi-sistem-altyapilari-i-c-in-asgari-gu-venlik-o-nlemleri-6445b90e-b2ad-4e5e-9c13-6ae19ba10e37.pdf.

31 The ISA is an institution that makes improvements in areas such as engineering and technology, and also sets standards for industrial automation and control systems.

32 See http://www.pera.net.

33 Hülya Kınık & Vahit Güntay, "Siber Güvenlik Temelinde Kritik Altyapılar ve Hazar Havzası," *Journal of International Social Research*, Vol. 9, No. 47 (December 2016), p. 254.

34 Ibid.

35 "Data Breach Investigations Report," *Idaho Cybersecurity Awareness*, 2015, https://cybersecurity.idaho.gov/wp-content/uploads/sites/87/2019/04/data-breach-investigation-report_2015.pdf.

36 Ibid.

ARTICLE

Ensuring Turkey's Border Security and Defense Industry: Current Evaluations

Özden ÖZBEN [*]

Abstract

In this article, the concept of "homeland security" is divided into two components according to the situations that damage physical, social and cultural assets and values, as well as the form of force to be employed in response. The article interprets border security as a sub-element of homeland security, while redefining integrated border management (IBM), which is used by the European Union, in the context of the Turkish defense industry. In addition to this new and more local definition, current evaluations reveal that boundaries are no longer just physical, and contemporary threats are multidimensional, multistage and multifaceted. The final part seeks to define and structure a more proactive defense industry that is ready for these changes with new wider assessments.

Keywords

Turkey, homeland security, border security, integrated border management, defense industry.

[*] Project Manager, Presidency of Defense Industries, Department of Cyber Security and IT Systems, Ankara, Turkey. E-mail: ozdenozben@outlook.com. ORCID: 0000-0002-2468-2259.

Received on: 20.04.2021
Accepted on: 14.09.2021

Introduction

When the concept of border security is considered in its narrow sense in terms of only physical border protection, up-to-date analyses are mostly made in the sphere of technological components. Especially in Turkey, it would seem that no other possible threats are included beyond the factors that have been troubling the country in the physical sense for years such as terrorism and migration. This narrow definition, however, addresses only a small part of the higher-level understanding of security implied by the terms "national security" and "homeland security."

In order to provide national security or homeland security at an effective level, it is necessary to reinterpret the concept of the border, re-analyze where borders begin and end, and re-evaluate the concept of border protection within this broader framework. Upon doing so, conclusions as to how adaptable technological developments are to these new border definitions can be interpreted separately.

Changes in both the quality and quantity of effective border security measures in line with current developments are not necessitated only by events occurring in the physical dimension. A national defense industry that is more prepared for these changes is defined in this article as one that is more proactive on the level of industrial quality and addresses the fact that borders are no longer merely physical and that threats are now multidimensional, multistage and multifaceted. The term "proactive" refers here to a competent level of industry in terms of national product and technology development, together with the design and production capabilities to analyze potential threats before they occur. In Turkey today, the interpretation of what industrial proactivity means at different operational, strategic, and tactical levels, and decisions about the direction of this sector in this context are currently being made and carried out through intense interaction with end users under the authority of the Presidency of Defense Industries (*Savunma Sanayii Başkanlığı*, SSB).

This article discusses the qualitative and quantitative changes that are considered to be necessary in reviewing Turkey's border security, and analyzes the situation of the Turkish defense industry within the scope of integrated border management (IBM). To this end, the first part of the article seeks to address the identification and classification issue regarding border security, while the second part focuses on current evaluations of Turkey's border security. Finally, the third part elaborates on Turkey's defense industry within the framework of IBM.

Identification and Classification

Border security, in the narrow sense, means the protection of the physical structure of a country's borders. Even if we begin with this conservative definition, however, it is necessary to consider questions such as where and in what scope the border begins and ends, and how and at what level the borders should be protected. In this article, the basic definitions of border security (green homeland, blue homeland, sky homeland, cyber homeland) and possible alternatives to those definitions are not given on the basis of international security theories. Instead, the classification and definitions are more specific with the aim of explaining the approach and the viewpoint of the article.

Dealing with border security only in terms of its physical dimension, or trying to produce security solutions while defining borders as merely physical structures will lead to a narrow and thus inadequate analysis of today's problems and needs in the realm of border security.[1] Therefore, border security should be defined as comprising different main elements and sub-elements in terms of quality and quantity. Separate analyses and solution components should be developed for each of those elements, and focus should be placed on the development of domestic and national solutions to ensure that those solutions can be implemented individually or together. The competence of the national defense industry in this field should be measured by its ability to provide solutions within this broad framework and by the proactivity of its approach to responding needs. In this article, threat is defined as the sum of the past, present and potential risks that have the potential to adversely affect any component of homeland security at any level. The components of an effective homeland security regime are detailed below based on this definition.

Dealing with border security only in terms of its physical dimension, or trying to produce security solutions while defining borders as merely physical structures will lead to a narrow and thus inadequate analysis of today's problems and needs in the realm of border security.

Homeland Security

It is possible to discuss two different levels of homeland security, according to the type of threat and the type of response the threats.

Hard Components

The threat is the possibility of immediate damage to physical, social or cultural assets and values; or the situation requires hard power response. For example:

- Military security
- Political security
- Border security
- Critical infrastructure security
- Citizen security
- Cyber security
- Disaster management
- Migration management

Soft Components

Threats that entail the possibility of damage to physical, social or cultural assets and values, yet which unfold slowly over a period of time, or in which the situation does not primarily require the use of hard power, fall into this soft category. In their initial stage, such threats do not necessarily require the use of hard power. The search for a solution may of course include any use of force when necessary, but this classification refers to situations in which hard power is not preferred. Classification is made on the basis of what is being protected. If we are to protect nuclear power plants, for example, the situation would be considered under the heading of critical infrastructure security. If we are protecting against the possibility of nuclear fallout, it should be evaluated under the heading of chemical, biological, radiological, and nuclear (CBRN) safety. This is why nuclear safety is not included among the following components:

- Food and water security
- Economic security
- Energy security
- Health security
- CBRN safety
- Environmental safety

- Industrial security
- Trade security
- Communication security
- Transportation security
- Education security
- Social and cultural security (race, language, religion, etc.)

Naturally, the method of reacting to threats to sectors in these two broad categories might differ, depending on the circumstances. For example, hard power measures might be taken against threats occurring in any of the areas typically considered soft. However, since this article does not aim to evaluate all possible action and intervention styles, these possible alternative models are not considered in the above classification.

It should be apparent to the reader that different definitions are required for the use of hard and soft power in the preservation of homeland security. For example, is the adoption of an aggressive method as a response to a cyber-threat within the scope of hard power necessary? Should it be categorized as soft power when the response to a cyberattack on critical infrastructure is not at the military level? In an effort to provide more accurate answers to questions such as these, the distinctions between definitions should be emphasized in a clearer way. Also it is possible for a threat to emerge involving more than one component, or, in other words, for a threat to affect more than one component when it occurs.

Terrorism poses a threat to any and all of these hard and soft components. For this reason, terrorism is not considered to belong to any one category. Instead, it is assumed that all kinds of threats can occur on the basis of terrorism, or, in other words, terrorism can be a threat for every component (such as cyberterrorism, political terrorism, health terrorism, etc.).

Another alternative classification may be related to the dimension or level of the potential threat to the homeland. The threat's dimension refers to the sectors the threat affects. The threat's level refers to whether it is physical, social/cultural or economic. Basic approaches will also be defined for the dimensions or levels at which precautions or reactions should be taken.[2]

From a state-centered perspective, almost all interpretations of homeland security are made on the basis of border security.[3] As mentioned above, however, border security should be considered as only one sub-element of homeland security.

Some threats are multifaceted, targeting multiple sectors and requiring a multi-pronged approach to address. A threat can also be interpreted as a combination of different types of threats.[4] For example, both the physical and cyber protection of energy facilities is necessary in ensuring the safety of critical infrastructure,[5] and the possible social and economic problems caused by disruptions in energy supply and distribution should also be considered. In addition to the physical protection of critical infrastructure, the need to protect them in cyberspace has become evident, thanks to the recent rise in the number of cyberattacks. When threats are considered as a whole (that is, the sector they target, the type of threat, its dimension/level, depth, intensity, impact area, etc.), it is clear that physical protection alone will not be sufficient.

Although border security and management are often included in security studies as critical concepts, efforts to consider homeland security as a whole and to put the idea in operation with a broader perspective also directly or indirectly affects border security-oriented activities. Doing so provides an opportunity to add components with different weights to the equation to ensure safety. Every single component of homeland security has effects of different weights, and within the general concept of homeland security, the evaluation of all affected components as a whole will make the measures to be taken or the possible intervention activities more meaningful. When security is approached together by all relevant stakeholders, a multidimensional and multicomponent (integrated) perspective can be gained, instead of a one-dimensional and single-component conceptualization of border security. Moreover, by considering every effective and relevant subcomponent of homeland security, effective measures can be taken for border security with relatively less but more focused and intensive effort.

Although border security and management are often included in security studies as critical concepts, efforts to consider homeland security as a whole and to put the idea in operation with a broader perspective also directly or indirectly affects border security-oriented activities.

In this respect, the concept of homeland security can be evaluated as a nation's efforts to protect itself, i.e., all units of the state, including every institution and individual, and to minimize possible damage from threats and dangers that may adversely affect its existence, security, resources, health, social and cultural structures, etc., by whatever methods it deems necessary. In other words, the concept of homeland security, which can be defined as all national efforts to try to make the homeland safe and resilient against possible threats and dangers, should be considered from a higher-level perspective that includes border security.

Border Security

As mentioned above, threats may occur in a variety of different mixtures, affecting multiple sectors at once. Within the context of homeland security, a threat for example arising on a cyber platform should not be interpreted merely as a cybersecurity threat but as a threat to the nation's digital borders, what we might call the cyber homeland. Otherwise, we are drawn back into the narrow definition, by which border security is only explained with elements of physical security. When border security is interpreted based on both what is within the borders and what is beyond them, it is possible to determine to what extent reactions, measures, infrastructure, technology and industry should be analyzed in this context.

There are two different action models of border security, which can be described as models for "preventing" and "allowing." Each one requires different technological infrastructures:

Preventing

As we have seen, border protection and external threat prevention have to do not only with physical elements. Protecting the nation from the inside out can be considered as any kind of precaution that can be taken for any kind of threat that is defined and understood to be outside the borders, based on the fact that we are located within many kinds of borders. Inside-out protection can be considered as a virtual, physical, social, cultural, etc. walls. Each such application will enjoy a high level of efficiency when it is planned in detail and its infrastructure is appropriately built. For example, when only physical security is being pursued, it is recommended to work on the following points to establish the appropriate infrastructure before planning the operational model. However, these recommendations will naturally vary from institution to institution:

- Services for defining institutional reforms and establishing inter-institutional interoperability requirements and plans;

- Identification of systems, physical infrastructure and equipment required to implement the border management strategy;
- Analysis of what kind of security/control system can be applied according to the relevant physical and geographical needs;
- Creation of a multilayered, comprehensive technological architectural structure for ensuring the security of land, air and sea (port security, coastal security, etc.) borders;
- For each region, risk analyses and threat assessments should be conducted, with infrastructural needs determined according to those analyses, considering the geographical structure of the land, climatic conditions, social structure, population density, land-use criteria, economic status of the people of the region, propensity to crime, neighboring countries, crime routes, records of past years, political developments in the region, terrorism, etc.;
- Identification of detailed documentation and technical requirements in the definition of required systems (requirements management);
- Monitoring, project management, efficiency analysis and reporting of the implementation processes of each border management and border security project;
- Establishment of distance and local, online and offline education infrastructures that include the relevant institutions;
- Design and planning of the institutional requirements for the integration of information and communication subsystems, communication network environments, information technologies infrastructures and various basic systems, which are key parts of a national border management system;
- Converting all these requirements into projects, dividing the projects into sub-segments and phases for each geographical region, and making the technical setups traceable;
- Design and monitoring of all planning, budgeting, construction, operationalization, provision of functionality, and execution processes that will enable preventive and protective measures to be taken by dividing physical security into subcomponents such as "physical prevention," "observation and control," "intervention systems and equipment" and "protection systems."

Allowing

For example, customs practices, transportation and migration management fall within the rubric of *allowing*. The entry of consumable products such as food, medicine and water, is also included here. The management of the entry and exit of digital data, which is likely to be used as a soft power tool from a broader perspective, should also be interpreted within the scope of protection for outside-in flows. In this context, who and what can enter the borders, how they do so and what methods of entry will be allowed should be evaluated. This represents the management of how much of the allowable types of movements (entry, transmission, communication, etc.) will be permitted, and which are considered to be beyond any kind of border.

The generally accepted concept of IBM as used by the European Union should be interpreted, revised, and redefined as the concept of "National Integrated Border Management" (NIBM), not as it is currently presented, but rather according to national requirements, expectations, capacities, and possible threats.

The generally accepted concept of IBM as used by the European Union should be interpreted, revised, and redefined as the concept of "National Integrated Border Management" (NIBM), not as it is currently presented, but rather according to national requirements, expectations, capacities, and possible threats.

As many different researchers have noted, current problems in globalization, such as organized crime, terrorism and migration, highlight the concept of border management. States relying on economic power use the concept of IBM, in which security and trade are considered together. In this article, IBM is considered as the formula for the execution of a free market economy without compromising security.[6] Thus, IBM can be expressed as the ability to achieve security and trade together in order to eliminate possible threats and ensure the continuity of a level of welfare built on economic power. This means that while economic activities are carried out effectively, security management in line with new border security understandings is emphasized.[7] To give a concrete example, the EU's IBM includes three basic elements: (1) regional and wide-ranging efforts to support mutual trade and transportation and reduce insecurity, smuggling, etc.; (2) interagency cooperation; and (3) cooperation in joint border management.[8] However, there is no definition of border security systems in the documents created by the EU, and there is no strategy document that presents the concept of IBM in a wide scope.[9] The EU's internal and external borders are being reinterpreted in line with enlargement policies and new security approaches. This new view is defined as IBM as part of a new border security system.[10]

Yet, boundaries must truly integrate different actors, functions, and processes for safe development. The concept summarized as IBM should restructure traditional border protection and management processes in a way that facilitates the passage of goods, services, and people, and it should be redesigned in a way to present them all in a secure manner.[11] Border management should be carried out in line with modern economic strategies, not by slow bureaucratic institutions.

The term "IBM" was first used by the EU in 2004 in a document entitled "IBM Guidelines in the Western Balkans." The definition in this guide refers to a holistic management style that emphasizes cooperation at national and international levels while providing good border security and being open to people, goods, and trade. "IBM" is used in North America with a slightly different definition: it is a strategy that requires the pooling of resources of various institutions and the participation of both individuals and institutions.[12] Boriboonrat, for instance, uses the concept of collaborative border management (CBM); similar to the definition of IBM, CBM refers to the management of the activities of border-related institutions, ensuring the safe passage of people and goods and meeting national needs while keeping the borders secure. [13]

As mentioned earlier, IBM is interpreted in North America rather as a strategy for institutions to work together in line with common goals.[14] This cooperation model requires the inclusion of both public and private institutions.[15] This definition could be restructured accordingly as follows:

For all national assets and values (physical, social, cultural etc.):

- To ensure the establishment of all inter-institutional interactions and action plans in order to protect the borders;
- To be ready on individual, institutional and national scales against all possible elements that may pose a threat to all types of our borders; and
- To take all necessary preventative/protective measures.

As can be seen, the term "integrated" refers to the ability to prevent and react to the existence of a wide-scale threat portfolio in a unified manner. The term "national" emphasizes the power of all institutions and individuals to work together and be ready within the framework of ensuring integrated border security.

A narrow view of Turkey's border security will only allow us to establish adequate physical security elements in line with current technological developments. However, when border security is approached in line with the definition given above, it is necessary to perform evaluations at many different levels, from the preventative measures to be taken to the forms of intervention that may be required if a threat materializes. When all related concepts are considered together, such as the establishment of inter-institutional interoperability for ensuring border security, social and cultural readiness, technological positioning and industrial competencies; and measures are taken by analyzing the threat across all dimensions and levels, it will then be possible to talk about "Integrated" border management. Any approach to NIBM should be implemented and managed in this context.

It must also be kept in mind that, while borders are now more permeable to people, goods and services, this permeability makes the areas inside the borders more vulnerable to unwanted elements.[16]

For this reason, based on this seesaw effect, border management should include but must not be limited to:

- Policy development processes for concepts such as immigration and trade management[17]
- Resource optimization and continuous technological modernization to provide physical security management.

In summary, it is recommended that all institutions in Turkey that participate in interactions on a national and/or international level should be involved/included in the nation's integrated approach to border security, which is interpreted as a hard component of homeland security, and should establish principles of interoperability in line with the points given below. Naturally, while this approach is particularly relevant to border security and management, it can be similarly applicable to all other components of homeland security.[18]

Once the foundation for interoperability is established according to the ideal model, other components will also be operable in the same way. The following components of the interoperability model between institutions are not offered under the assumption that the model is in-complete; rather, they are proposed to advance the debate that existing interactions in the context of homeland security could be improved:

- Consensus on the structure and details of the common working area where representatives of all relevant institutions will work together;
- Determining the level of required information technology/managerial integration between institutions and the principles of data sharing to build a standard information and risk assessment/management platform, discussing and determining the basic structures for the creation of a common data collection and analysis system that can evaluate national and international information on IBM and make it available to relevant institutions when necessary;
- Determination of the data-sharing model and its limits within interactions among national institutions for border management-related national and international cooperation;
- Negotiations on the expectations for and sharing among national institutions, with consensus on a model that all will be able to apply in cooperation;
- Designing of the software model required for common use among the institutions and structuring of data to be shared among institutions;
- Determination of the fundamental elements of a command and control center under border management control and supervision, including risk analyses and crime intelligence-sharing modules;
- In coordination with all authorized institutions, discussions on capabilities on hand and capabilities that need to be further developed for crime detection both outside and inside the borders;
- Discussion of models and alternatives for a common risk analysis mechanism among institutions;
- Construction of a national risk database and discussion of the operational usage of this database;
- Discussions on the creation of relevant legislation and review of related regulations;
- Development of the fundamentals of NIBM information acquisition and management;
- Establishment of models for data gathering from inside institutions

and data sharing between institutions to enable preventive measures to be taken effectively and instantaneously;

- Creation of an interaction map and the design of the main features of the interaction platform needed to produce reports and outputs subject to emergency management;
- Discussions of what institutions can contribute to the process, both in terms of assets and expertise, with the aim of developing the necessary information and decision support infrastructure for decisions about initial and secondary-level preventive measures;
- Discussions on eliminating administrative/technical obstacles to the establishment of a common model where the information infrastructures of institutions are not affected, but can be used in line with national/international security objectives;
- Design of infrastructure, based on consensus, for a central and integrated education center that can meet the inter-institutional and intra-institutional managerial and operational education requirements;
- Building a data infrastructure that generates and records critical data with the aid of traceability and effectivity analysis;
- Ensuring that institutions interact with each other in real time and have common decision-making systematics allowing for rapid intervention;
- Design of an infrastructure for instantaneous detection of the affecting and affected factors according to the type of the threat;
- Establishment of infrastructures, hierarchies and administrative functions to be ready for use at any time,
- Maintenance of alternative policy development processes based on relevant scenarios to be ready at all times and stages together with the maintenance of the resources for those needs.

Current Evaluations of Turkey's Border Security

Various projects have been developed and implemented, and will continue to be implemented, for the physical protection of Turkey's homeland borders. In addition, in line with the Integrated Border Management Action Plan approved in 2006, a group of projects carried out with EU funding have also been implemented.[19] With the latest projects, in which high technology is used intensively, more and more effective solutions have been offered and serious advances have been made to ensure more effective border security. Unmanned systems have now replaced manned systems, and a wider area has been brought under control more quickly with systems offering more advanced observation capabilities. As Ankara's security discourse has evolved recently from an emphasis on the integrity of Turkey's physical land borders to encompass its territorial waters, undersea resources and airspace, as evident in the current prominence of the "Blue Homeland" and "Sky Homeland" concepts, the understanding of border security has expanded well beyond a line in the sand. At the same time, developments in the realm of cybersecurity have increased global awareness of the digital dimensions of border security.

In line with these developments and advances in technology, the scope of ensuring Turkey's physical border security has been expanded toward a three-dimensional model rather than a two-dimensional one. To summarize briefly, when border protection is considered in the context of physical security as simply protecting a line, that protection remains rather primitive when there is no analysis of previous or future movements. When we consider how movements, violations, and possible threats will affect situations both inside and outside borders, the concept of line protection turns into the concept of protecting a surface. When depth is added, as the idea of "Blue Homeland" and "Green Homeland" (underground resources) implies, and when height is added, as in the concept of "Sky Homeland" (without an upper limit), a three-dimensional concept of protection evolves. Although "Cyber Homeland" does not have any physical or visible borders, any type of national data or data that may have value for national benefits and rights (including the protection, storage, sharing and transmission of the data) are the elements defining this invisible border. The violation of these rights and benefits and attempts to access such data should also be interpreted as a violation of the Cyber Homeland.

In line with these developments and advances in technology, the scope of ensuring Turkey's physical border security has been expanded toward a three-dimensional model rather than a two-dimensional one.

Turkey's Defense Industry and IBM

In this section, industrial-scale evaluations of the integrated/consolidated/holistic approach will be made, where the application area is border security. Border security, as the focal point for these evaluations, has been interpreted here as a hard component of homeland security. It is addressed in terms of Turkey's land, air, sea and digital (cyber) borders and is evaluated considering the aforementioned models of prevention and allowance.

Every security-oriented capability may also have a countermeasure or a relevant countermeasure may be developed. Therefore, one should not fail to notice the possibility that those who violate the border could be informed about the products we possess or could acquire or develop different products and solutions.

In this context, if both sides are utilizing the same solutions and products, the solutions themselves may become potential security problems. These solutions may be, for example, systems, tools, components or software. It must be kept in mind that external actors can easily obtain non-national or non-native elements and that measures against such products and systems can be easily taken. Although attempts to violate borders are also made by those who do not use technology, maintaining national systems and solutions at the highest levels possible, regardless of the nature of the threats, will allow us to be ready for threats and take preventive measures.

At this stage, it is necessary to interpret the concepts of "domestic" and "national" specifically within the considered scope. "Domestic" refers to a nation's internal production using local assets and capabilities. "National" refers to products and technologies that are controlled by the state at every stage from design to final production. Control of a product means the ownership of the proprietary rights, or the design or the production process. The fact that a product is domestic does not necessarily mean that it is national, and it is likewise not always possible to say that a national product is totally domestic. In summary, nationally controlled products or technologies should not contain components or stages that are domestically uncontrollable, even though domestic production may not always be provided. More detailed definitions of these concepts may be given as follows:

Domestic: A product, service, or competence being domestic means that all or a part of that product, service, or competence is produced locally, using domestic industry competencies, domestic raw materials, domestic labor forces, etc.

National: A national product emerges from, is produced by, and is used in the interest of the state, i.e., to meet the state's expectations, needs and capabilities, from its design to its production and from the intellectual dimension to the usage stage. No international commercial concerns or limits should interfere in a product's being national. The design, production and development of a national product, system or subsystem cannot be changed or blocked by non-national parties for any reason.

To summarize, based on these definitions, the national quality of a product, system or subsystem means that all the rights, powers and capabilities of that product are within the scope of national industrial competencies.

Observing international examples of advanced technology development and production, it may be seen that there is a focus on consumer electronics and the automotive and aerospace industries. Countries producing advanced technology products in these sectors strategize to be the best in the technological areas in which they enjoy leadership. This competition is sometimes purely driven by consumer markets, and sometimes occurs in line with national, strategic goals. In the latter case, the process of choosing a national commercial model with broad participation and adopting specific "technological distinction and superiority areas" are guided by the central authorities. The main such authority in Turkey, the SSB, has developed many projects to shift the geopolitical balance in Turkey's favor with increasing momentum in recent years, and has been carrying out this process in a highly qualified way to achieve technological superiority. Especially in the last few years, there has been a significant increase in the number of projects carried out under the authority of the SSB; important steps have been taken in the fields of localization and industrialization, dominance over the relevant sectors and technology has increased, the development of Turkish technologies and the production of original products have been ensured through successful R&D projects.

The administrative requirements for selecting and focusing on specific areas of technology in terms of border security, regardless of which institution is managing the process, should be considered as follows:

1) In which areas should investments in advanced technology be made, and which areas need to be domesticized;

2) Which national, domestic or industrial strategies should be used in choosing these areas and how these areas are to be chosen;
3) Which of these areas should be owned, expanded, operated and marketed by which institutions and establishments (corporate ownership);
4) How industrial and technological separation should occur (which companies should invest and improve themselves in which areas), preventing the duplication of investments;
5) What kinds of purchase guarantee models can be applied to support or defend these investments and improvements;
6) How to evaluate long-term national border security strategies on a geopolitical basis in a technological context and discuss them as deep, long-term industrial strategies rather than short-term approaches;
7) How to ensure superiority in the market and overall technology by developing the basic technologies at the basis of the need, in addition to analysis of the extent to which the purchased, acquired, or developed technology and competencies can meet the need.

Although each of the above items may be worked on by national institutions individually and with focus, it is critical for the IBM approach to integrate and generalize these efforts, advance them on a talent-based basis, and adopt them as national strategic technology areas. Caudle divides the capability-based risk management framework into four dimensions: force management (the ability to manage threat readiness), operational management (the ability to use military capabilities against sudden developments), potential challenges (foresight, readiness, acquisition of new capabilities) and corporate management (the ability to use resources efficiently and establish the effective functioning of the defense ecosystem).[20]

We can expand the term "industrial proactivity" in border security to include the analysis of possible threats and the need for managing threats before they occur, and, to this end, reach a more successful industrial level with the development, design, and production of national products and technologies. In other words, emphasis is placed on predicting a threat before it becomes real, on the development of all types of industry-oriented policies in advance, and on all types of efforts carried out in advance and in a pioneering fashion on the basis of technology and product ownership. These efforts to predict threats should be so deep and so broad that both operational proactivity (event-, scenario-, and field-oriented) and strategic proactivity (industrial policies- and industry development-oriented) are ensured.

When the studies carried out by the SSB in recent years are evaluated in terms of border security, it is seen that activities are implemented under the following main headings, as described above, with a focus on industrial proactivity:

- Creating a consolidated list of products/technology in areas that can be domestic, in light of data obtained from companies, key contractors and relevant institutions/organizations;
- Identifying potential investment areas that are considered critical for advanced technology production;
- Classifying the technological development capabilities needed in these fields with the assignment and categorization of relevant academic platforms;
- Performing general analysis of which companies, academic institutions or industrial clusters can work in which technological fields;
- Generating a general competence and technology matrix that can be used in determining national and international strategic technological areas;
- Creating a technology development database of elements that do not require reinvestment, allowing recommendations for the consolidation of such investments.

Conclusion

Considering that a border has two sides, the fact that a secured border is expected to bring multiple international actors closer to each other with common security concerns —and that the opposite case can also occur— naturally requires the weights of factors for international interactions based on border security to be analyzed individually and repeatedly. Domestic/national industrial dominance, levels of advancement, technology development and production capacities, and integrated defense industry-oriented policies and practices, all of which are independent of international interactions, are all crucial parts of such analyses. Naturally, borders have two sides, and both sides must protect themselves according to their own threat and risk levels.

Homeland security cannot be provided through border security alone, just as the establishment of physical border security does not mean that the homeland is safe. Of course, it is difficult and expensive to take all possible measures against every possible threat, but effective homeland security management must be established with a holistic perspective, considering an adaptive and active infrastructure for inter-institutional interactions, responses, precautions and notifications. This integrated approach should primarily be carried out on an industrial axis, and administrative and technical policies should be developed on that basis.

This article has sought to reinterpret the concept of borders to allow the provision of national security or homeland security at an effective level, to analyze where borders begin and end regarding the technical dimension that concerns the industrial approach, and to offer a broad framework of the concepts of border protection that can be considered in this context.

Homeland security cannot be provided through border security alone, just as the establishment of physical border security does not mean that the homeland is safe.

As the discussion above indicates, changes in the quality and quantity of the needs for effective border security in line with current developments are not only occurring in the physical dimension. Security concerns and needs may change depending on where and how the boundaries are drawn, in addition to their dimensions. It has been emphasized that a national defense industry that is more ready for these changes should be prepared for the fact that borders are now more than physical and threats are now multidimensional, multistage and multipronged. The national defense industry should also be more proactive, reaching a higher level of industrial competence, capable of analyzing threats and needs before they occur, and possessing all relevant national product and technology development, design, and production capabilities.

In a broader sense, approaches to establishing border security require evaluations at many different levels, from the measures to be taken to the forms of intervention. When all relevant aspects are considered as a whole, such as establishing interagency interoperability for border security, social and cultural readiness, technological positioning and industrial competencies, and when threats can be analyzed in all dimensions with proper precautions taken, only then will it be possible to talk about "integrated" border management in the fullest sense.

Endnotes

1 Cemhan Kocabaş, *Border Security with Hegemony: Evaluation of EU Neighborhood Policy's Mediterranean Basin Applications in Terms of Critical Theory's Concept of Hegemony*, unpublished PhD dissertation, Karadeniz Technical University, 2016, p. 228. Border security is no longer considered merely physical; it involves the comprehensive protection of a country's cultural heritage and welfare.

2 Nihat Akçay, *Turkey's Threat Perceptions and Security Approaches in the 21st Century*, unpublished PhD dissertation, Uludağ University, 2008, p. 17. The author classifies threats as vital (to existence, national sovereignty and territorial integrity) and national (political, economic and natural disturbances that can disrupt internal stability). He also addresses two other types of threats: primary (regional instability, democratic negativity, mafiaization, increased crime rates, etc.) and secondary (situations that may be fundamental or national threats in the long run). In addition, he discusses internal threats (economic, sociological, etc.) that cause danger to national integrity and national welfare, which may be internally or externally triggered; and external threats (those originating from a country or terrorist organization), giving the definition of asymmetric threat as follows: "Aiming to be effective by using low-level force and technology, with the potential to cause instability in political, social, and economic structures, which may have a high impact due to [the targeted individual or site] not being ready for the threats."

3 Kocabaş, *Border Security*, p. 5. Threats to domestic security can have both material and moral qualities.

4 Bilal Karabulut, *Rethinking Security in the Globalization Process*, unpublished PhD dissertation, Gazi University, 2009, pp. 12–14. In this study, the author defines threats as phenomena that may adversely affect the existence and values of a state, society, or individual, explaining three different types of risks: the risk of losing what one has, the risk of not obtaining what one does not have, and risk that is independent of the actor and of a global nature. He also emphasizes that threats can constitute combinations of these different forms. According to the author, regardless of the type of threat, actors establish security systems comprising three different rings: an innermost ring for internal dangers, an immediate-periphery security ring that includes border neighbors and an outermost ring for global threats.

5 National Research Council, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, Washington DC: The National Academies Press, 2002, p. 313. The challenges in protecting critical infrastructure against terrorism include, for example, the integration of information infrastructures into national and international data networks and information systems. A cyberattack will be able to produce results similar in scope to physical attacks.

6 Arif Köktaş & Ömer Yılmaz, "Integrated Border Management Model in the European Union: From Schengen Convention to the Stockholm Programme," *Turkish Journal of Police Studies*, Vol. 12, No. 2 (2010), p. 3.

7 Kocabaş, *Border Security*, p. 32.

8 Ibid, p. 33.

9 Radko Hokovský, "The Concept of Border Security in the Schengen Area," *Central European Journal of International and Security Studies*, Vol. 10, No. 2 (2016), p. 76.

10 Ahmet Türköz, "The Integrated Border Management Model of the European Union," *Turkish Administrative Journal*, No. 487 (December 2018), p. 716.

11 Martijn Pluim & Martin Hofmann, "Integrated Border Management and Development," *ICMPD Working Paper*, No. 8, 2015, p. 11, https://www.icmpd.org/fileadmin/ICMPD-Website/ICMPD_General/Working_Papers /Working_Paper_BMdevelopment_final.pdf.

12 Köktaş & Yılmaz, "Integrated Border Management," p. 4.

13 Pimupsorn Boriboonrat, "Collaborative Border Management in Thailand and Neighboring Countries: Needs, Challenges and Issues," *International Journal of Criminal Justice Sciences*, Vol. 8, No. 1 (January–June 2013), pp. 1–12.

14 Peter Hobbing, "Integrated Border Management at the EU Level," *CEPS*, August 2009, https://www.ceps.eu/download/publication/?id=5181&pdf=1254.pdf.

15 Nathan E. Busch & Austen D. Givens, "Public-Private Partnerships in Homeland Security: Opportunities and Challenges," *Homeland Security Affairs*, Vol. 8, No. 18 (October 2012), p. 16.

16 James Anderson & Liam O'Dowd, "Border, Border Regions and Territoriality: Contradictory Meanings, Changing Significance," *Regional Studies*, Vol. 37, No. 7 (1999), p. 602.

17 Robert Bach, "Transforming Border Security: Prevention First," *Homeland Security Affairs*, Vol. 1, No. 1, (Summer 2005), p. 10.

18 Sharon Caudle, "Basic Practices Aiding High-Performance Homeland Security Regional Partnerships," *Homeland Security Affairs*, Vol. 2, No. 3 (October 2006), p. 5. High-performing cooperation and inter-institutional integration should be interpreted in a broad framework that includes a common evaluation infrastructure, common resources, political influence and organizational capabilities and capacities.

19 *Türkiye'nin Entegre Sınır Yönetimi Stratejisinin Uygulanmasına Yönelik Ulusal Eylem Planı*, 2006, https://docplayer.biz.tr/2573591-Turkgye-ngn-entegre-sinir-yonetgmg-stratejgsgngn-uygulamasi-na-yonelgk-eylem-plani-gelggtgrglmesgne-destek-projesg.html. This document presents an overview of Turkey's current border management and IBM strategy, highlighting the areas for improvement within the context of the EU acquis and detailing the investments and financing model after classifying the goals. The document includes an evaluation of Turkey's interagency coordination and cooperation. The action plan addresses infrastructure needs in two different categories: border surveillance and control. The document was approved by the Prime Ministry on March 27, 2006.

20 Sharon L. Caudle, "Homeland Security Capabilities-Based Planning: Lessons from the Defense Community," *Homeland Security Affairs*, Vol. 1, No. 2 (2005), p. 9.

ARTICLE

UAV Autonomy in Turkey and Around the World: The "Terminator" Debate

Ufuk SÖZÜBİR [*]

Abstract

Autonomous systems, particularly unmanned aerial vehicles (UAVs), present both opportunities and challenges for modern warfare. Although they lack the moral compass and flexibility of the human mind, they nonetheless provide great advantages in terms of range, precision, coordination and speed in land, naval and air warfare. The advantages of their relative autonomy removes certain limitations, particularly in the sphere of UAVs, both in Turkey elsewhere, while the same autonomy gives rise to the "Terminator" debate with regard to lethal autonomous weapon systems (LAWS)—often called "killer robots"—theoretically capable of targeting and firing without human supervision or interference. The purpose of this article is to help elucidate the challenges posed by the autonomy of the UAVs, and to discuss the advantages and disadvantages of UAV systems, particularly the debates, reservations and criticisms about handing over authority to unmanned systems, especially given that Turkey has been eagerly and successfully working to develop this technology. As the technology continues to evolve, becoming more efficient and expanding into new areas of application, the challenges in determining the level of autonomy that LAWS should have are likely to increase. Although it is not easy to articulate the balance between the hu-

[*] UAV Mission Commander / Lieutenant Colonel, Turkish Gendarmerie General Command & PhD Candidate, Ankara Yıldırım Beyazıt University, Department of International Relations, Ankara, Turkey.
E-mail: ufuksozubir@gmail.com. ORCID: 0000-0002-9514-4036.

Received on: 17.05.2021
Accepted on: 03.10.2021

man and the machine in the division of authority, the best solution might be an efficient collaboration between the human mind and artificial intelligence (AI). Also, the law of armed conflict (LOAC) should be developed sufficiently and flexibly to regulate this kind of weaponry, particularly since, unlike nuclear arsenals that are kept under the strict control of states, it is easier to access and develop autonomous weapon systems (AWS). Therefore, permanent measures are needed in order to ensure that development in this field is consistent and ethical with respect to international humanitarian law.

Keywords

Unmanned aerial vehicles, Terminator debate, defense industry, Turkey, lethal autonomous weapon systems.

Introduction

With recent developments in electronics and computer technology, the usage of unmanned aerial vehicle (UAV) systems in the battlefield has become more common and visible around the world. In Southwestern Asia, Syria and Iraq in particular, the extensive usage of drones by various countries (e.g., Turkey, the U.S. and Russia) has necessitated the development of new doctrines and concepts of operations (CONOP-S).[1]

Although UAV systems are relatively new, a considerable body of academic literature has emerged around the world to discuss this field. In Turkey, however, the number of studies on lethal autonomous weapon systems (LAWS), particularly UAVs, remains relatively small and is mostly limited to the publications of the production companies themselves. In this regard, the literature is divided into two main branches: One of these focuses on the capabilities of AWS, while the other addresses the usage of these systems and their position in international humanitarian law (IHL).[2] Both of these dimensions will be elaborated upon here, although it should be noted that it is beyond the scope of this article to try to cover all of the related concepts in detail.

To begin, some basic terminology will be helpful. A UAV, commonly known as a "drone," [3] is basically an aerial vehicle able to convey the necessary payloads to execute different missions without a human pilot on the vehicle itself.[4] Without the need to carry a crew, and thus without the weight of the crew's accompanying life-support systems, UAVs have greater design permissiveness, and are efficient and safe, capable of greater range and endurance than manned vehicles.[5] Depending on the type of the UAV, there is usually a ground control unit with a controller, a communication system linking the drone with the ground control unit and a payload set up for a variety of tasks. The vehicle itself and its support units form the basic components of any type of UAV system. As there is no risk of human loss, since they carry no pilot, UAVs provide low-risk operations with mission flexibility, design flexibility, endurance and continuity. They are mostly cost-effective and personnel effective, because there is no need for personnel to be stationed inside the air vehicle. UAVs have the additional benefit of being able to conduct instant data transfers and stealth patrols. On the other hand, because UAV technology has been developed relatively recently, there are certain disadvantages, such as relying integration for the airspace, data link vulnerabilities (UAVs are sensitive to electronic warfare and electronic counter warfare), limited survivability, limited meteorology effectiveness and limited situational awareness.[6] In addition to these practical concerns, drones raise significant moral concerns by their very nature: some UAVs are automated weapons and some have already started to become autonomous in certain tasks. The difference between automated and autonomous systems will be discussed in more detail later in the article.

Although the usage and development of UAVs started before the 1960s, the main milestones in their history began after the 1980s with the development of the Israeli mini-scout drone.[7] Later, UAV development continued with rapid progress, from unarmed piston-engine scout drones to unmanned combat vehicles with turbojet engines like the U.S. Nortrop Grumman X-47B unmanned combat aerial vehicle (UCAV).[8] By 2018, 65 countries had become UAV producers of various types, hosting 702 different military/civilian firms producing approximately 3,121 various types of UAVs. Today, at least 24 countries are currently developing military unmanned aircraft.[9] In the U.S., the MQ-1 Predator and MQ-9 Reaper UAVs became manually controlled in 2005; requiring licensed pilots only for take-off and landing. Eight years later, the X-47B turbojet engine UCAV prototype successfully made an autonomous landing on an aircraft carrier. And in 2015, another X-47B succeeded in its first air-to-air refueling mission using specially developed software—dispensing with the need to land in order to refuel provides a considerable increase in the UAV's level of autonomy.[10]

In the case of Turkey, even a relatively cost-effective drone like the Bayraktar TB-2 now has the capability for autonomous take-off from and landing on an airbase.[11] This shows the level of progress Turkey has achieved in developing UAV systems. Moreover, these systems have proven to be advantageous in combat theatres. Even though they are mostly used for intelligence, surveillance and reconnaissance (ISR) missions and assassination tasks, UAVs were utilized by the Turkish Armed Forces (TAF) to assist in air superiority in an innovative manner for the first time in Syria. Although UAVs are relatively slow-moving and do not possess air-to-air capabilities, the TAF has overcome these disadvantages through intensive use of electronic warfare and F-16 AMRAAM Beyond Visual Range Missiles in the scanning range of airborne early warning and control aircraft.[12] Thus, while the capacity and autonomy of unmanned vehicles has improved in many ways, the auxiliary systems supporting UAV technology have also advanced; it is clear that, in the future, UAVs will play a crucial role in effective military networks, cooperating with other unmanned systems in a whole new area of conflict that includes land and sea, as well as space and cyberspace. Such developments will necessitate a new set of Rules of Engagement—which has already become the subject of debate.

Limitations and Capabilities

UAVs may carry many different loads, but they all function with two fundamental components. The first is hardware, which includes the body, engine, payloads and other attachments. Depending on the purpose of the UAV in question, there are a number of possible classifications regarding its hardware, including the size of the flying component (micro, mini, small, tactical, operational, strategic), the type of payload (UAVs and UCAVs), the type of fuel used (internal combustion, turbojet, turbofan, electric, solar), the type of flight process (fixed-wing, rotary wing), the type of command system (autonomous, remote-controlled), the UAV’s purpose (target detection/decoy; intelligence, ISR, logistics support), its desired take-off/landing procedures (launch from ramp, direct launch, take-off from runway, dropped from plane, thrown with hand, land on wheels, land on fuselage, land with parachute), its flight range and altitude (nano, micro, mini, close range, short range, medium range, medium range endurance, low altitude deep penetration, low altitude long endurance, medium altitude long endurance, high altitude long endurance) and special mission (combat, offensive, defensive, stratospheric, exo-stratospheric, space).[13] For military unmanned aircrafts, NATO made its classifications simply according to the weight of the UAV.[14] These classifications mostly have to do with the “limitations” of the drone and whether it has the ability to complete a specific task according to the feasibility of the vehicle itself. In this sense, the analogy of a sports car and a scooter could be used, as the former is much faster and reliable, while it consumes more fuel and is much more expensive.

The second fundamental component is the “software” of the system, which enables the drone to perform the operations necessary to accomplish its tasked objective by using the “hardware” that has the functionality to complete the mission. Software is also a must for performing maintenance tasks for the vehicle while it is in flight; software is responsible for executing commands and applications automatically or in response to a ground command.[15] Software may be categorized in two main branches in terms of its utilization in a UAV. The first branch is mainly reserved for the abilities that enable the UAV to perform its duties by using the hardware it possesses. For example, a Bayraktar TB-2 drone can automatically draw a circle around a specific target for hours without much interference from meteorological changes in its vicinity; a heavier and bigger (Class 3) UCAV Akıncı can perform take-off and landing even though there is no Ground Control Station in the area,[16] which is something that cannot be automatically executed by the smaller, older TB2 model.

Unlike a manned aerial vehicle, which includes all the constituents inside the vehicle, an unmanned system is a complex unit with support units, datalinks, control unit and human operator or monitor dispersed across a wide area. The first category of the software, then, is the main responsible linking element that provides communication and connection among all these components. Software also supports the unit in determining a safe and stable flight route, and provides flight stability during the fire-on mode.

The second category for the software is the vehicle's autonomy. UAV systems depend on a certain level of automation to execute given tasks. Machine involvement means machine speed in the decision-making process, although how to achieve optimum speed and precision while remaining under the control of a human mind is a serious question that remains to be answered.

From Automation to Autonomy: Opening Pandora's Box

The difference between "automation" and "autonomy" needs to be described before evaluating what might constitute a "solid" decision on the levels at which a UAV operates. Automation is the ability of a system to operate under well-defined rules and algorithms predetermined by humans, and to achieve better, faster and more precise outcomes by relying on these preconditions without AI support. Therefore, automation refers to a certain standard operating procedure (SOP) that is conducted in a pre-planned manner and carried out in the command line of a machine. In terms of the unmanned military craft concept, automation does not exclude the human element; it only decreases the complexity of the specific tasks executed by the operator and prevents possible mistakes due to human nature.[17]

Autonomy, on the other hand, specifically refers to a machine's ability to make decisions and perform specific tasks without, or only under the supervision of, a human operator. Autonomy refers either to operating in predefined conditions with or without human assistance, or acting with totally independent decision-making processes with full awareness of the environment and conditions in the operation area. Autonomy not only means acting after observation, orientation and decision steps, but making autonomous decisions after having a full awareness of the situation.[18]

In politics and philosophy, issues about autonomy have been widely discussed; most of the literature about unmanned systems is based on these discussions. According to Mackenzie, individual or personal autonomy has three different but causally interdependent dimensions:

self-determination, self-governance and self-authorization. Self-determination includes the freedom to set preferences and the capability and propensity to choose values about the future of one's life. Self-governance, on the other hand, implies having the necessary background for making self-determined choices. Self-authorization refers to the behavior and attitude of a person in determining their decisions and actions.[19] When these three dimensions are reinterpreted for military systems, three distinct concepts emerge: the sort of task the machine/AI is designed to execute, the human-machine relationship while the task is being performed and the level of sophistication of the machine when executing the task. Just like a human being in sociology, a machine can increase its autonomy simply by increasing its level of autonomy in any of these three dimensions.

In terms of UAV autonomy, the sort of task being performed mostly serves a military or security-oriented purpose. The human/machine relationship is closely related with the first dimension and places a human being in the process of sensing the situation, deciding upon the necessary response to the situation and acting accordingly. In accordance with the place of a human in this process, machines can be called semi-autonomous or fully autonomous. Semi-autonomous systems are further divided into two categories; in one, humans are involved in the decision-making process as deciders and in the other, humans are involved in the decision-making process as supervisors.

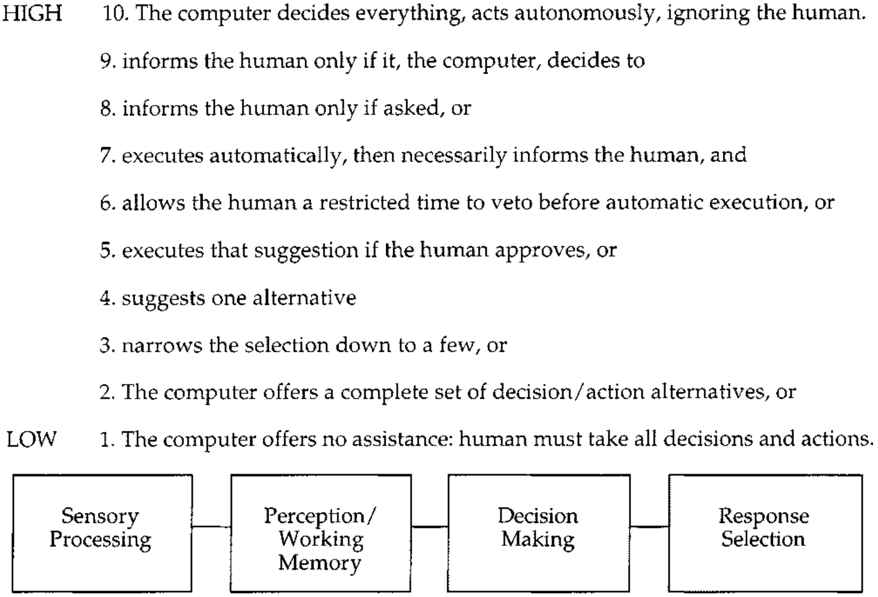
In semi-autonomous operations in which a human is the initiator, the machine (UAV/drone) performs a task and then waits for the operator's approval to continue or stop executing the operation. Such systems are limited to the specifics of a given task and cannot operate without the consent and direction of the operator. In contrast, in supervised autonomous operations, when the machine is activated, it continues performing the task until the human intervenes to halt the operation. Here, a human is in the role of a supervisor. In this kind of autonomy, human-machine communication as well as detailed information implementation is of crucial importance. With supervision, possible negative outcomes can be corrected and the behavior of the vehicle can be adjusted as a safety measure. In other words, in supervised semi-autonomous systems, a human observes the project and has the authority to interrupt if something goes wrong.

Lastly, “fully autonomous” refers to a task-performing machine that operates without human intervention. In this kind of automation, the machine starts to operate and the human does not have the authority to make decisions or even supervise the process and action.[20] For example, according to the U.S. Department of Defense, an AWS is “a weapon system that, once activated, can select and engage targets without further intervention by a human operator. This includes human-supervised autonomous weapon systems that are designed to allow human operators to override operation of the weapon system, but can select and engage targets without further human input after activation.”[21]

In unmanned systems, autonomy is related to the ability to choose the best option from a set of possible decisions and perform a logical action accordingly. A truly autonomous system can perceive the environment around itself, make logical decisions based on the recognized environment and take an action or perform a manipulation that makes a distinct change in the environment in which it operates.[22] Therefore, autonomy includes a solid decision-making process with the help of advanced recognition of the conditions in the current environment and highly advanced Identifying Friend or Foe (IFF) procedures.

In the military sphere, certain references are used for evaluating degree of autonomy, and determining whether it is high, medium or low. According to Parasuraman, Sheridan and Wickens, one of the sources of evaluating the autonomy of a device or vehicle is the partial or full replacement of the control or function that had previously been executed by humans. This classification is provided in the figure below:

Figure 1: Levels of Automation of Decision and Action Selection



HIGH 10. The computer decides everything, acts autonomously, ignoring the human.

9. informs the human only if it, the computer, decides to

8. informs the human only if asked, or

7. executes automatically, then necessarily informs the human, and

6. allows the human a restricted time to veto before automatic execution, or

5. executes that suggestion if the human approves, or

4. suggests one alternative

3. narrows the selection down to a few, or

2. The computer offers a complete set of decision/action alternatives, or

LOW 1. The computer offers no assistance: human must take all decisions and actions.

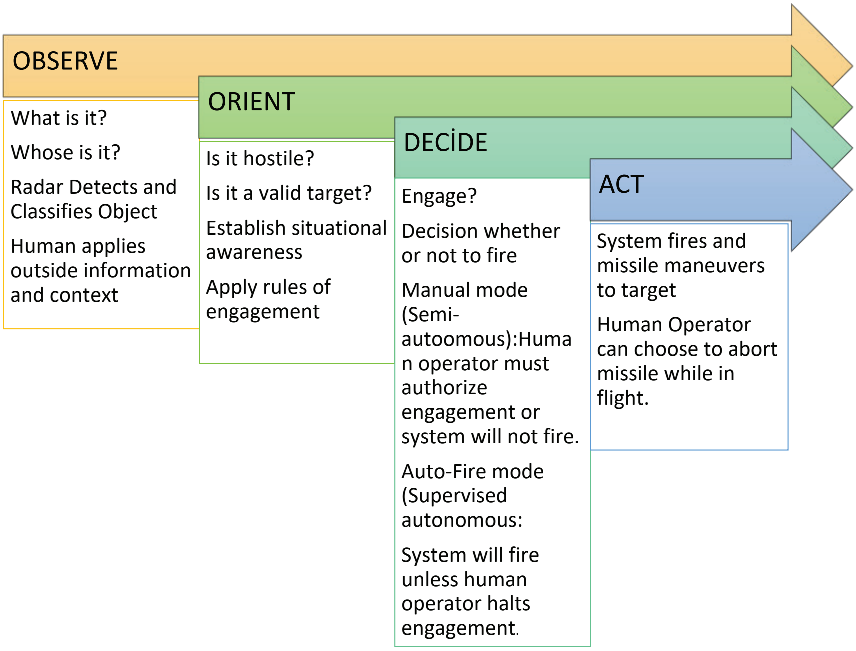
Source: Raja Parasuraman, Thomas B. Sheridan, and Christopher D. Wickens, "A Model for Types and Levels of Human Interaction with Automation," *IEEE Transactions on Systems, Man, and Cybernetics-Part A:Systems and Humans*, Vol. 30, No. 3 (2000), p. 287.

In the "Sense, Decide and Act" loop paradigm, the authors focus on the automation of determining the course of action mainly based on the output functions of the system. Therefore, the figure reflects a lower-level autonomy definition. Yet, when the input functions are put into use, we will likely witness automations so advanced that they have the ability to change their code and adapt to the new situation in accordance with their goals. This means that the automation will evolve at a speed with which the human mind cannot compete. Therefore, even though the figure above is accurate and consistent, it does not fully explain the benefits and challenges posed by the automation process.

A second model the military literature offers is the "Observe, Orient, Decide, Act" (OODA) loop paradigm of combat. This concept is introduced by Boyd.[23] Usually, victory on the battlefield belongs to the side that is able to complete this cycle faster and more effectively. In any case, the presence of AI in this loop brings the ultimate advantage in accelerating and fulfilling the cycle. According to the U.S. Air

Force Flight Plan 2009–2047, computing speeds and the capacity of non-organic intelligence agents will permanently change the OODA loop from supporting to fully participating in all aspects of the process. Therefore, the cycle will be reduced to micro or nanoseconds, and the "perceive and act" vector will depend on the AI capabilities that are used by the opposing sides. Humans will no longer be "in the loop."[24]

Figure 2: OOAD Cycle in a Patriot Air-Defense Autonomous System


OBSERVE
What is it?
Whose is it?
Radar Detects and Classifies Object
Human applies outside information and context
ORIENT
Is it hostile?
Is it a valid target?
Establish situational awareness
Apply rules of engagement
DECİDE
Engage?
Decision whether or not to fire
Manual mode (Semi-autoomous):Human operator must authorize engagement or system will not fire.
Auto-Fire mode (Supervised autonomous:
System will fire unless human operator halts engagement.
ACT
System fires and missile maneuvers to target
Human Operator can choose to abort missile while in flight.

Source: Paul Scharre, *Army of None: Autonomous Weapons and the Future of War*, New York: WW Norton & Company, 2018, p. 191.

In these models, predetermination raises two main issues regarding human/AI participation and control override preferences. The first issue is the degree of repetitiveness and uniformity of a task given to AI: The more repetitive a task is, the more successful automation becomes. In civilian air transportation, for example, all planes have Automatic Flight Control (AFC) systems installed on their computer system. Mostly these systems operate far more precisely and effectively than the human mind, because a large portion of the work is completed without human clumsiness and hesitation. But in extraordinary situations for which the automatic pilot has not been programmed, the human intervenes uses his/her own decision-making process to solve the problem.

The second issue is about the nature of the task given to the AI system and the capacity of a human to intervene and control the process. Although today almost every weapon with automation technology has semi-autonomous and fully autonomous modes, some tasks, like air and land defense missions, require a speed of engagement that overwhelms human operators. These systems include the U.S. Naval Aegis and Phalanx Close-in Weapon System, the land-based Israeli "Iron Dome" and U.S. "Patriot" air defense systems, counter-artillery and counter-mortar systems such as the German "Mantis" and active protection systems for tanks and other land vehicles such as the Aselsan "AKKOR" and Israeli "Trophy" systems.[25] Therefore, determining the type and level of automation depends on an evaluation that examines the effect of the human operator on the results. In the future, fully autonomous weapons may be developed that completely remove the human mind from the OODA loop and even forge their own codes, depending on the environment of the battlefield or arena.

The "Terminator" Debate: What are the Dangers of an AWS?

The "Terminator" debate originates from the eponymous cult film starring Arnold Schwarzenegger, who plays the role of a killer robot fully independent of human control that aims to destroy the human race with directions received from a fully autonomous AI "Skynet" that determines the human race is a "danger" to its own existence.[26] Although achieving that kind of autonomy in AWSs does not seem possible in the short term, the speed and extent of technological advances should be a warning of possible risks. Moreover, although giant leaps have been made in the development of AI systems, there are still a lot of uncertainties regarding the natural environment in which they operate. And there are certain risks and dangers directly related to AWS in their current form. These include the "expandability" of an AWS, the human-AI relationship and the incredible machine speed of autonomous systems which in certain situations makes it impossible for humans to even supervise the actions committed by the AI.

AWSs are human-free systems; therefore, any country with autonomous technology has the ultimate advantage of managing human-free conflicts. This means that a leader who desires and plans to start an unlawful war, but hesitates because of the morally and politically negative implications of military casualties, will no longer fear because there will be fewer casualties and the aggressor will gain the ultimate upper hand. AWSs could thus make war more prevalent. Relatedly, AWSs have the capacity to start an uncontrolled arms race, which may even take place between nation-states and transnational/international terrorist organizations that could have access to sophisticated weaponry once AWSs are easily produced and accessed. The latter could also target civilians.[27]

The second risk is related to the precision and clarity of the machine's decision-making process. Automation complicates control over a task or mission because of the increased complexity of the overall mechanism, and nullifies the operator's supervision because the checks that need to be executed exceed the capacity of human reflexes in a limited time. This complexity leads to two other important problems: The first problem has to do with the complicacy of the system as the operator is indispensably reliant on the indicators. In today's most advanced systems, even the designers do not have the most complete knowledge and design structure of the system, which means there can be no direct inspection of any kind of advanced AI-based automations. The supervisor has the power to intervene, but this intervention can only be useful if the indicators successfully address the true nature of the problem. The second problem is the complexity of the computer codes that need to be written for a really sophisticated system. Considering that an F-22 fighter jet uses 1.7 million codes, and an F-35 fighter jet requires 24.7 million, this level of sophistication could bring inevitable errors. Codes can also make the system vulnerable to hacking and guided processing. Last but not least, the sophisticated logic and technology used in the coding system makes errors incomprehensible to and undetectable by the operators and engineers.[28]

NATO originally thought the UAV systems could be a solution to "conduct the dangerous, dull and dirty (D3) missions;" instead of asserting a certain limit of autonomy, they have preferred stringent control over the drones and have emphasized a reliable military communications network. Protti and Barzan argue that depending on the roles executed by the system, NATO plans to carry out a detailed analysis of the functionalities of a UAV to be autonomous, the level of autonomy required for these functionalities and the balance between the supervised human and AI machine. Dangerous missions mostly include ISR missions in the event of a high-level enemy Air Defense threat. Dull missions include surveillance missions that keep tabs on a target over a very long period of time (e.g., the house of a red category target). And dirty missions include ISR and operational missions in a CBRN dirty environment.[29]

Autonomy in any kind of device, whether robot or vehicle, becomes a topic of debate at the legal and ethical levels. In politics and social psychology, many thinkers have expressed reservations about using a device that is outside human control, even though it would be very useful in some cases. The image of the HK (Hunter-Killer) Aerial VTOL Drones armed with laser weapons searching for any kind of humanoid in the *Terminator* movie is still circulating in many people's consciousness.

For clear tasks, there is no doubt that any AI system with a certain amount of autonomy will be faster, more decisive and more precise than a human operator. But if an unconventional situation occurs, AI has a doubtful performance compared with a human being. The human mind's flexibility and capacity to operate under unexpected conditions is superior when dealing with new threats and circumstances. Based on this factor, governments and other potential clients of UAV systems prefer to depend on operators to control the drones, and the U.S. in particular—the world's leading manufacturer of drone technology—opposes the idea of increasing the autonomy of unmanned systems.[30] Therefore, considering the military loop as the basis for UAV systems, the question as to *where* the human should be placed in this cycle becomes the main subject of the debate.

One should also touch upon the concept of "meaningful human control," which was first used in the 2013 report of a non-governmental organization that focused on how the UK conceptualizes autonomous weapon systems.[31] Although there are different opinions about the concept, two schools elaborate on human control in autonomous systems. The minimalist school defends the free usage of any kind of LAWS that can obey the basic rules of IHL. For this school, if a weapon has the capability to comply with the rules of international law, it is unimportant whether a human delivers the lethal blow by pressing the button on an unmanned system, or whether s/he activates a LAWS that operates on its own while selecting and engaging with the targets. Conversely, the maximalist school argues that all kinds of autonomous systems should be considered like nuclear weapons and categorically banned.[32] As a major UAV producer, it is not surprising that Turkey's perspective regarding UAVs is closer to the minimalist school.

The place of the human mind in the decision-making loop is an important concept, one that raises debates regarding the relationship between IHL and armed conflict. Since some basic principles like military necessity, humanity, proportionality and distinction are generally understudied in the field of international law, UN bodies have shown a growing interest on this subject. For instance, the first official LAWS Group of Governmental Experts (GGE) came together in Geneva in November 2017. In 2019, the group accepted 11 guiding principles in the area of LAWS—particularly that human responsibility could not be transferred to LAWS and that countries should pledge to develop future LAWS in accordance with IHL. In addition, it agreed that there should be a certain balance between military necessity and humanitarian considerations. The group's report stated that the development and production of LAWS should be strictly tackled within the context of the IHL—even though the broad scope of IHL could sometimes blur certain limitations in LAWS.[33] Despite diplomatic initiatives like the Geneva meeting, however, the boundaries in this sphere remain vague, making it hard to create a practical legal background regarding meaningful human control over LAWS. In addition, it should be noted that these debates—like those over nuclear weapons—are dominated by major arms producers and militarily powerful states, rendering it difficult to reach an agreement to put limits on the production of such systems.[34]

In today's world, UAVs are used in many fields, from the observation of forest fires to the control of autonomous irrigation projects; however, in the much more complex environment of a battlefield, the consequences of failing performances and faulty decisions are very different and potentially even appalling. This is because the main objective of military UAVs and other unmanned systems is to neutralize a human target or some other weapon that could affect a human target. Taking these facts into consideration, excluding autonomous defense systems like the AEGIS naval defense system or the PATRIOT missile defense system, the human element becomes a crucial part of an information network and the decision-making process to avoid any irrecoverable flaw in the AI infrastructure. Currently, there are no machines with the consciousness or the ability to reevaluate a situation in the presence of uncertain variables. In other words, automation is not a black-and-white question and there are many debatable grey areas at every level.[35]

Turkey's UAVs and the Autonomy Debate

Although Turkey has not been a pioneer in the development of unmanned systems in general, or UAVs in particular, like the U.S. or Israel, it would not be an exaggeration to claim that it has achieved a certain level of expertise in a considerably short time and has become quite experienced in the production of Medium Altitude Long Endurance (MALE) class UAV systems, such as the TUSAS ANKA series or Baykar's Bayraktar TB2 UAV systems. ANKA UAVs belong to the MALE class; they have an operational altitude of 30,000 feet and a 24-hour flight capability with a 200 kg payload.[36] They have been used in numerous Turkish cross-border military operations and are regarded as one of the "combat proven" units of Turkey's unmanned fleet. With over 300,000 hours of operational flight capacity, Bayraktar UAVs have also been acquiring "combat proven" status. The latter has an operational altitude of between 18,000 and 27,000 feet and the capacity to carry 650 kg with up to 27 hours of endurance.[37]

It is remarkable that Turkey has designed, developed and produced its own unmanned systems, which have proven to be very efficient both in countering terrorism inside its borders and in conducting military operations outside its borders—especially in Iraq and Syria. For instance, as part of Operation Spring Shield launched in Syria in 2020, the Turkish military staff introduced a brand new unmanned air doctrine by operating UAVs as air-to-surface weapons in a non-air-superiority environment. In other operations in Syria, like Euphrates Shield, Olive Branch, Peace Spring and Spring Shield, Turkish UAVs proved to be precise and hard to counter: even Short-Range Air Defense Systems

(SRADS) were not considerably effective against the massive campaign of the Turkish unmanned systems.[38]

It should be noted that although Turkey has long been aware of the importance of unmanned systems, the indigenous development of these systems and Turkey's ascension as a "drone power" [39] is largely the result of the reluctance of the U.S. and Israeli governments to sell such systems (The MQ-1 Predator and MQ-9 Reaper for the U.S. and Heron Systems for Israel), which Turkey wanted to use in its counter-terrorism operations.[40] Today, with its self-developed UAV systems, Turkey has been working to enlarge its fleet with both larger (TUSAS Aksungur and Bayraktar Akıncı) and smaller (Alpagu, Kargu and Bayraktar Mini İHA) unmanned systems and is continuing to invest in more advanced systems, which will certainly enhance the autonomy level of its drones.

Turkey's currently operational UAVs and new prototypes should be analyzed in terms of automation. As indicated by Protti and Barzan, NATO defines four levels of autonomy: [41]

1. Remotely-controlled system: system reactions and behavior depend on operator input.
2. Automated system: reactions and behavior depend on fixed, built-in functionality (pre-programmed).
3. Autonomous non-learning system: behavior depends on built-in functionality or upon a fixed set of rules that dictates system behavior (goal-directed reaction and behavior).
4. Autonomous learning system: system with the ability to modify rule-defining behaviors (behavior depending upon a set of rules that can be modified for continuously improving goal-directed reactions and behaviors within an overarching set of inviolate rules/behaviors).

Turkey's two currently operational MALE UAVs, the Bayraktar TB2 and the ANKA, cannot be categorized into any one of these definitions, since they do not include a compact operational body. Instead, they are both built from various components, each with different automation capabilities. These two MALE models can best be defined as a harmonious combination of drone, payload and weapon with different automation levels in every piece of equipment. The Baykar firm's website states that the Bayraktar TB2 drone can be categorized as an autonomous, non-learning system with fully autonomous landing and take-off capability, fully automatic taxiing and parking, GPS-independent navigation, automatic navigation and route tracking capabilities.[42] In terms of the OODA loop, its operators occupy only the role of a supervisor or director; therefore the system can be considered semi-autonomous. In extreme conditions for which the UAV system is not designed, operators can manually take control of the joystick and throttle—although in many cases that kind of intervention has caused negative outcomes. The Bayraktar TB2 uses a Wescam MX-15D Electro-Optic Camera, a completely remote-controlled system, as its surveillance device. As payload, the camera has no initiative in the decisions made by the operator. The payload operator has total control over the optics, which seek the target in a designated area; after acquiring the target, it aims at it with a remote-control system. As for the weapon, the MAM-L and MAM-C smart micro-precision-guided munitions used by the TB2 can be categorized as an automated system with a semi-active laser seeker and optional inertial navigation/global positioning systems.[43] The smart munition, when fired, follows the track of the laser marker created by the optic system and the maneuverability is totally under autonomous control while following the laser tracker. The munition cannot be deactivated after firing, but it can be directed to a safer place if the decision of the human changes after hitting the fire button.

With additional supporting avionics and other systems, these three main components with different levels of autonomy have been combined to make a remarkable UAV weapon that has proven itself in real ISR and air-to-ground missions. Stringent human control over the firing mode places questions about the law of armed conflict (LOAC) (necessity, distinction of target, proportionality, accountability and liability, and other moral and ethical issues) squarely in the realm of the human operator. In Turkey's drones, targets are identified, surveilled and hit totally under the control of military authorities. Necessity is determined by the process of carefully selecting and identifying targets within hours (sometimes days) of ISR missions. The distinction and proportionality of the weapon in the military offensive is provided perfectly with precision-guided and limited-effect munitions. Bayraktar drones are impeccably reliable and accountable systems with autonomous functions that prevent them from causing harm to friend or foe even when command and control (C/C) is lost. And for moral and ethical issues, humans instead of machines press the button, which means that the hostile target is not eliminated by the machine, but by the operator who uses the system.

There are ongoing ethical debates about the autonomy of unmanned systems, which have no conscience or reasoning power; some argue that this makes it impossible for a target to surrender to an unmanned system on the rapidly changing battlefield. Under LOAC, an important principle is to "provide for and do not harm those who surrender, are detained or are otherwise under your control."[44] Yet it is indeed possible for a target to surrender to a Turkish drone, because it is operated by a human; there is even video footage of a terrorist surrendering to a Bayraktar TB2 UAV in the Afrin region in Syria.[45]

When it comes to the development of new prototypes and projects, it is almost certain that Turkey will pay special attention to AI utilization. On Baykar's website, many AI features, including visual posture detection without the help of GPS systems, basic object detection (with the use of deep learning technology), gimbal object detection and operation beyond the line of view and landmark recognition are mentioned as ongoing projects. The new prototype UCAV Akıncı, with a 20-meter wingspan, 40,000 feet operational altitude, 24-hour operational flight and a 1,350 kg payload capacity will be a much larger and stronger UAV than the Bayraktar TB2. In the future, the Akıncı will be equipped with air-to-air missiles, enabling it to be used in air superiority missions.[46] However, in the field of autonomous systems, this capability may cause some problems regarding the decision-making process. First, until now, UAVs have been designed to conduct ISR missions, which do not require a quick decision-making stage in the OODA loop. But in air-to-air combat, the air vehicle has to react instantly to its adversary, which is equipped with weapons of a similar sophistication level. Because the Akıncı has two propeller engines with limited speed, it will have a low probability of survival against turbojet-engine manned fighters. Therefore, it would be logical to think that the air-to-air capability of the Akıncı will be limited, like propeller-engine CAS manned crafts, helicopters and other UAVs.

After serial production, the Akıncı will be equipped with an indigenous AESA radar system, making it easier to detect and react to other manned/unmanned aircrafts with its Gökdoğan/Bozdoğan air-to-air missile arsenal. However, these "hardware" elements may still not be enough to deal with manned air targets. First of all, UAV sight over the battle scene is very limited compared to manned aircraft because the UAV operator has to rely on the remote camera system that must transfer visual data; there may be only a lag of milliseconds, but this small timelapse is enough for a manned aircraft pilot, who is using his/her eyes and other sensor avionics on board, to destroy the UAV system. The second problem with air-to-air engagements has to do with the possibility of losing connection between the UAV and the operator. This is an unacceptable risk for any kind of unmanned system, because it could ultimately lead to the loss of an expensive device. The Baykar website indicates that these challenges should be overcome by the extensive usage of AI components that can provide more autonomy to the aircraft in certain situations. For instance, in an air-to-air combat situation, the Akıncı will be equipped with full air-to-air internal and external payload, and will be autonomous in specific combat situations. This relative independence will likely raise many of the questions previously mentioned in this article. Indeed, the TUSAS Aksungur, a Medium Altitude Very Long Endurance (MAVLE) system that is regarded as the Akıncı's "brother," will probably be a subject of the ongoing "Terminator debate" in the very near future.

Turkey's leading UAV firms, Baykar and TUSAS, have both announced their objective of developing turbojet-engine UAVs (Baykar's MIUS and TUSAS' Göksungur) capable of conducting air-to-air warfare. In his conference, Baykar's technical manager Selçuk Bayraktar stated that the MIUS will be capable of strategic offense, CAS (close air support), SEAD/DEAD (Suppression Enemy Air Defenses/Destruction Enemy Air Defenses) and missile attack capabilities.[47] Although these projects are still in the design and planning stage, it is assumed that highly capable and autonomous AI will be installed in these advanced systems.

Conclusion

Today, the use of AI has become widespread all around the world, as it is an easy-to-use and rapidly evolving technology. And just like most cutting-edge technologies, automation and AI have found their first extensive usage in a military context. Modern low-level conflicts and battles are witnessing an increasing use of military drones in ISR as well as offensive and propaganda missions. The more tasks a military UAV/drone undertakes, the more intelligent and capable AI it has to use.

Turkey's military technology has been evolving constantly, like that of the rest of the world, and Turkish military designers have been working hard on the development of autonomous systems and ever more sophisticated AI technology. The lessons that have been learnt by the TAF in this field, particularly during their cross-border military operations in Iraq and Syria, indicate that the Turkish defense industry will continue to thrive in the development of new UAVs. In fact, negotiations are under way for the sale of Turkish-made UAVs to many other countries. Although the state still imposes strict control over weapon systems in Turkey, the achievements of Turkish military companies have been promising regarding the use of AI/automation systems. Turkey is becoming a leading UAV producer and user, developing new concepts and vehicles, in the context of a novel, evolving mode of warfare characterized by the use of military networks, AI collaboration between air-land-naval systems, unmanned offensives and other types of innovation.

To date, the usage of weaponry in UAV arsenals has been conducted under the strict supervision of a human mind, but the need for ever-increasing speed and precision is already revealing this supervision as a constraint to the true potential of machine speed. What we have to understand in this area is that there is no "conscience" or "mercy" in the AI architecture; therefore, even if the slightest autonomy is enabled in any kind of killer hardware, these machines will use this autonomy without hesitation or remorse to ensure victory for their side, since this is the main objective for which they are built. Both in Turkey and around the world, concept designers will have to decide where to stop the autonomy of killer machines—or, in the terms of the debate—at what point to terminate the Terminator.

Endnotes

1 Can Kasapoğlu, "Turkey's Drone Blitz Over Idlib," *Terrorism Monitor*, April 17, 2020, p. 7, https://jamestown.org/program/turkeys-drone-blitz-over-idlib/.

2 On the debate regarding LAWS and autonomy, see Paul Scharre, *Army of None: Autonomous Weapons and the Future of War*, New York: WW Norton & Company, 2018; Michael C. Horowitz & Paul Scharre, "Meaningful Human Control in Weapon Systems: A Primer," *CNAS Working Paper*, March 2015, https://www.files.ethz.ch/isn/189786/Ethical_Autonomy_Working_Paper_031315.pdf; Michael A. Goodrich & Alan C. Schultz, "Human-Robot Interaction: A Survey," *Foundations and Trends in Human-Computer Interaction*, Vol. 1, No. 3 (2007), pp. 203–275. For the same debate in Turkey, see Tarık Ak, *Günümüzün Değişen Savaş Koşullarında İnsansız Savaş Araçları ve Etik Tartışmalar*, Ankara: Sistem Ofset, 2017; Can Kasapoğlu & Barış Kırdemir "Yükselen İnsansız Sistemler Gücü: Askeri Atılımın Eşiğindeki Türkiye," *EDAM*, June 1, 2018, https://edam.org.tr/wp-content/uploads/2018/06/CAN-Yukselen-Insansiz-Sistemler.pdf.

3 In this article, the terms UAV and drone will be used interchangeably. Also see:*Strategic Concept of Employment for Unmanned Aircraft Systems in NATO*. Kalkar: Joint Air Power Competence Centre, 2010, p. 5.

4 Brendan Gogarty & Meredith Hagger, "The Laws of Man over Vehicles Unmanned: The Legal Response to Robotic Revolution on Sea, Land and Air," *Journal of Law, Information and Science*, No. 19 (2008), p. 73.

5 J. F. Guilmartin, "Unmanned Eerial Vehicle," *Encyclopedia Britannica*, July 15, 2020, https://www.britannica.com/technology/unmanned-aerial-vehicle.

6 Jean Paul Yaacoub et al., "Security Analysis of Drones Systems: Attacks, Limitations, and Recommendations," *Internet of Things*, No. 11 (2020): 100218.

7 John F. Kreis, "Unmanned Aircraft in Israeli Air Operations," *Air Power History*, Vol. 37, No. 4 (1990), p. 48.

8 See https://www.northropgrumman.com/what-we-do/air/x-47b-ucas.

9 *RPAS Yearbook 15th Edition*, Paris: Bryenbuerg Co., 2018, p. 123, https://rps-info.com/publications/rpas-yearbook-2018/#page/123; Dan Gettinger, *The Drone Databook*, New York: Center for the Study of the Drone, 2019, p. xv.

10 Paul D. Scharre, *İnsansız Ordular: Katil Robotlar, Otonom Silahlar ve Makine Savaşları*, İstanbul: Kronik, 2020, p. 94

11 See https://baykardefence.com/uav-15.html.

12 Kasapoğlu, "Turkey's Drone Blitz over Idlib," p. 8.

13 Salih Akyürek, *İnsansız Hava Araçları: Muharebe Alanında ve Terörle Mücadelede Devrimsel Dönüşüm*, İstanbul: Bilgesam, 2012, p. 2.

14 *Strategic Concept of Employment for Unmanned Aircraft Systems in NATO*, p. 6.

15 "Flight Software (FSW) Overview," *Arizona State University*, https://phxcubesat.asu.edu/subsystems/flight-software#:~:text=The%20Flight%20Software%20(FSW)%20is,%E2%80%9C-brain%E2%80%9D%20of%20the%20satellite.

16 "Bayraktar Akıncı Yer Kontrol İstasyonu Bulunmayan Uzak Meydana Tam Otonom İniş Kalkış Gerçekleştirdi," *Youtube*, November 5, 2020, https://www.youtube.com/watch?v=_yw_Q3Pdd1I.

17 Wei Xu, "From Automation to Autonomy and Autonomous Vehicles: Challenges and Opportunities for Human-Computer Interaction," *Interactions*, No. 28 (January 2021), p. 49.

18 Mica R. Endsley, "Situation Awareness, Automation & Free Flight," in *FAA/Eurocontrol Air Traffic Management R&D Seminar*, Saclay, France: SA Technologies, 1997, pp. 1–5.

19 Catriona Mackenzie, "Three Dimensions of Autonomy: A Relational Analysis," in Andrea Veltman & Mark Piper (eds.), *Autonomy, Oppression and Gender*, Oxford, New York: Oxford University Press, 2014, pp. 17–18.

20 Paul Scharre, *Autonomous Weapons and Operational Risk*, Washington DC: Center for a New American Security, 2016, pp. 9–10.

21 *Autonomy in Weapon Systems*, Washington DC: Department of Defense, November 21, 2012, p. 2.

22 Jason Walker, "What Are Autonomous Robots? 8 Applications for Today's AMRs," *Waypoint Robotics*, 2020, https://waypointrobotics.com/blog/what-autonomous-robots/.

23 John Boyd, *Patterns of Conflict*, 1976, p. 128, http://www.ausairpower.net/JRB/poc.pdf.

24 *United States Air Force Unmanned Aircraft System Flight Plan 2009–2047*, Washington DC: Headquarters, United States Air Force, 2009, p. 44.

25 Ibid, p. 76.

26 James Cameron & Gale Anne Hurd, *The Terminator*, Los Angeles: Hemdale, 1984.

27 Thomas B. Payne, "Lethal Autonomy: What it Tells us about Modern Warfare," *Air & Space Power Journal* Vol. 31, No. 4 (Winter 2017), pp 20–22.

28 Scharre, *İnsansız Ordular: Katil Robotlar*, pp. 185–210

29 Marco Protti & Riccardo Barzan, "UAV Autonomy: Which Level is Desirable? Which Level is Acceptable?" *NATO Alenia Aeronautica Viewpoint*, November 2007, pp. 12-2;12-4,https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/RTO-MP-AVT-146/MP-AVT-146-12.pdf.

30 Directive no. 3000.09 of the Department of Defense is perfectly clear about how to use autonomy in weapons. See "Autonomy in Weapon Systems."

31 "Killer Robots: UK Government Policy on Fully Autonomous Weapons," *Article 36*, April 2013, https://article36.org/wp-content/uploads/2013/04/Policy_Paper1.pdf.

32 Horowitz & Scharre, "Meaningful Human Control in Weapon System," p. 7.

33 "Meeting of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects," *United Nations*, December 13, 2019, https://undocs.org/CCW/MSP/2019/9.

34 Daniele Amoroso & Guglielmo Tamburrini, "Autonomous Weapons Systems and Meaningful Human Control: Ethical and Legal Issues," *Current Robotics Reports*, No. 1 (2020), pp. 187–194.

35 Raja Parasuraman, Thomas B. Sheridan & Christopher D. Wickens, "A Model for Types and Levels of Human Interaction with Automation," *IEEE Transactions on Systems, Man, and Cybernetics*, Vol. 30, No. 3 (May 2000), p. 289.

36 See https://www.ssb.gov.tr/WebSite/contentlist.aspx?PageID=364&LangID=2.

37 See https://baykardefence.com/uav-15.html.

38 Ali Bakeer, "The Fight for Syria's Skies: Turkey Challenges Russia with New Drone Doctrine," *MEI*, March 26, 2020, https://www.mei.edu/publications/fight-syrias-skies-turkey-challenges-russia-new-drone-doctrine.

39 Samuel Brownsword, "Turkey's Unprecedented Ascent to Drone Superpower Status," *Drone Wars*, June 15, 2020, pp. 1–9, https://dronewars.net/2020/06/15/turkeys-unprecedented-ascent-to-drone-superpower-status/.

40 Özge Özdemir, "İHA ve SİHA Üretiminde Türkiye Dünyada Yükselen Bir Güç Mü?" *BBC Türkçe*, October 14, 2020, https://www.bbc.com/turkce/haberler-turkiye-54533620.

41 Protti & Barzan, "UAV Autonomy," pp. 12–7.

42 https://baykardefence.com/uav-15.html.

43 https://www.roketsan.com.tr/en/product/mam-l-smart-micro-munition/.

44 "Introduction to the Law of Armed Conflict (LOAC)," *Geneva Call*, 2013, p. 27, http://www.genevacall.org/wp-content/uploads/dlm_uploads/2013/11/The-Law-of-Armed-Conflict.pdf.

45 See https://twitter.com/i/status/1368917622436335621.

46 https://www.baykarsavunma.com/iha-14.html.

47 "Selçuk Bayraktar Milli Teknoloji Hamlesi MEB Sunumu," *Youtube*, June 25, 2020, https://www.youtube.com/watch?v=tsQezdIh2CA.

ARTICLE

Israel's Renewable Energy Strategy: A Review of its Stated Goals, Current Status, and Future Prospects

Sujata ASHWARYA [*]

Abstract

Israel's commitment to renewable energy development stems from a desire to reduce its reliance on imported fossil fuels while also meeting environmental goals. The Israeli government has aided the development and expansion of the renewable energy sector through a series of favorable regulatory decisions. Solar energy has established itself as the primary driver of the country's renewable energy development. Wind energy development, on the other hand, is hampered by a slew of political and administrative squabbles, and biomass technology, which is not considered profitable due to its inability to generate grid-level electricity, is investment-constrained. While wind and biomass renewable technologies would benefit overall renewable energy development, they currently offer only marginal growth opportunities. As intermittent renewable energy sources become more common in the electric grid, Israel's expanding hydropower capacity will help to maintain grid stability and reliability by stepping in during unplanned outages. The country's 2030 goal is to phase out coal, oil and diesel, and renewable energy will be critical to achieving that goal. Solar photovoltaic tariffs have dropped significantly in recent years, putting this energy resource in direct competition with natural gas, which Israel has in abundance due to its Eastern Mediterranean reserves. Although renewables do not threaten the dominance of natural gas in the electricity market, Israel's goal of 30 percent renewable energy in the country's energy mix by 2030, achieved through increased capacity addition across technologies, will help the country meet its climate change mitigation goals.

Keywords

Israel, renewable energy, fossil fuels, hydropower, smart meter.

[*] Associate Professor, Centre for West Asian Studies, Jamia Millia Islamia, New Delhi, India.
E-mail: scheema@jmi.ac.in. ORCID: 0000-0001-6700-619X.

Received on: 05.05.2021
Accepted on: 11.10.2021

Introduction

Israel's energy system is extremely vulnerable, as the country is an electricity "island" with no interconnections to the grids of its neighbors—a result of its unique history in the conflict-ridden region. Approximately one-third of its electricity generation is currently derived from imported coal, and the transportation sector is entirely reliant on imported crude oil. Coal and oil imports account for a sizable 63 percent of Israel's total primary energy supply (TPES). Although natural gas from indigenous fields—discovered in 1999–2000 in Israeli economic waters in the Eastern Mediterranean and in significant quantities ten years later—has become the country's "fuel of choice" for power generation, significantly improving its energy security, reliance on imported fossil fuels entails economic and security risks associated with the need to maintain energy supplies. These risks, however, can be significantly mitigated by integrating renewable energy into Israel's energy system, given the country's substantial solar, wind and hydropower resources. While the government authorized the incorporation of renewable energy into Israel's energy supply chain in 2002 by inviting independent power producers (IPPs) to construct and operate solar energy facilities, renewable energy's share of total electricity generation has remained relatively low.[1] In addition, the country's renewable energy portfolio is not particularly diverse, with solar energy accounting for the lion's share of supply.

Despite a 17 percent year-on-year increase in 2018–2019, Israel's solar energy penetration rate remains among the lowest in the world, especially when compared to OECD countries, particularly Europe, which receive significantly less sunlight. Despite having one of the highest irradiance rates in the world and an abundance of sunlight throughout the year,[2] a number of factors have slowed Israel's development of solar energy and other renewable energy sources. The most significant barriers have been bureaucratic red tape, onerous regulations and difficulty in acquiring land for renewable energy farms. For years, Israeli inventors have been developing cutting-edge solar energy technologies, but due to the difficulty of bringing their inventions to market in Israel, they have primarily exported their expertise.

Despite these obstacles, non-fossil fuel electricity generation gained traction after the Israeli government enacted a regulatory mandate in 2011 requiring the optimization of renewable energy in power generation through grid-connected quotas for each renewable energy technology. A slew of financial incentives, including feed-in tariffs (FIT), the elimination of taxes on residential solar and wind energy generation and the net-metering system, have all contributed to the growth and diversification of Israel's renewable energy market.[3] When the Public Utilities Authority (PUA) for Electricity (colloquially called the Electricity Authority) launched a solar tendering round in 2017, it ushered in a new era of market-driven renewable development by removing the red tape associated with licensing, eliminating long lines and mountains of paperwork for renewable energy entrepreneurs.[4]

In addition, the Israeli government has funded renewable energy research in order to advance the field's development. In 2019, the Office of Chief Scientists of the Ministry of Industry, Trade and Labor allocated $1.45 billion USD, equivalent to 5 billion Israeli New Shekel (NIS), to clean technology research and development projects, including renewable energy.[5] The 2018 electricity market reforms, which separated the electricity generation and transmission segments of the public utility Israel Electric Corporation (IEC), significantly increased opportunities for local and international IPPs to build and operate renewable energy plants. By 2025, private electricity generation facilities are expected to account for 60 percent of Israel's total capacity.[6]

This article examines the various renewable energy technologies currently in use in Israel, as well as the government's efforts to accelerate their development in light of the Paris Climate Agreement's quantitative pledges to improve air quality and reduce emissions. It contends that in the coming years, the solar energy sector will be the primary driver of Israel's renewable energy expansion, owing to governmental support, the presence of excellent natural solar resources, declining technology costs and political and administrative disputes over wind energy development. Hydroelectricity, for which Israel has set a separate development quota, will serve as a backup source to compensate for the intermittent nature of renewable energy sources, which are increasingly being integrated into the country's power grid.

Hydroelectricity, for which Israel has set a separate development quota, will serve as a backup source to compensate for the intermittent nature of renewable energy sources, which are increasingly being integrated into the country's power grid.

Renewable Portfolio Standard: Evolution and Implementation

Israel is proud of its renewable energy pioneering history. Following the country's establishment in 1948, Prime Minister David Ben Gurion made the visionary decision to establish an Israel Research Council to promote research and development that would apply scientific knowledge to the task of developing a new nation with almost no natural resources. In the Research Council's Physics and Engineering division, Harry Tabor, a British scientist hired by Ben-Gurion, developed the Tabor Selective Surface—thermal panels capable of absorbing and storing solar energy. Tabor then incorporated this technology into the water boiler, yielding what many Israelis affectionately refer to as a "dude shemesh" or sun boiler: solar-heated water tanks that have been a fixture on Israeli rooftops since the 1960s.

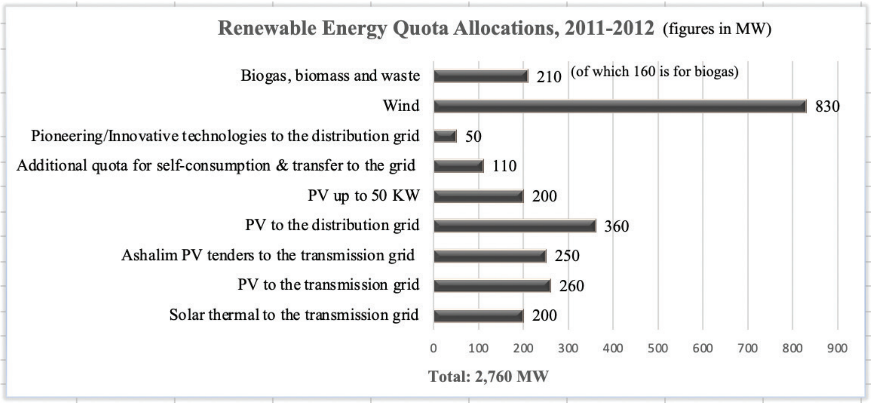
By 1967, 50,000 sun boiler systems were being sold each year,[7] and this technology was widely adopted locally following a 1980 law requiring the installation of solar water heating systems on all new residential buildings up to 27 meters in height.[8] With this national building code in place, Israel achieved one of the highest penetration rates of solar water heaters in the world, contributing to a 3 percent reduction in electricity consumption over time. Israel is now the world leader in solar water heating systems, with 85 percent of households heating their water using rooftop solar collectors.[9] However, from 1948 until the early twentieth century, there was a strong bias in Israeli policymaking circles in favor of fossil fuels, which were viewed as a more reliable source of energy. There were few takers in the energy ministry for a proposal to implement renewable energy technology on a national scale.

Nonetheless, Israel's 1992 accession to the United Nations Framework Convention on Climate Change sparked internal debate about climate change mitigation, prompting the IEC to integrate natural gas into electricity generation and the energy ministry to consider using renewable energy to clean up the country's power grid. This shift in thinking resulted in the development of a Renewable Portfolio Standard (RPS). The RPS is a collection of regulatory provisions aimed at increasing the use of non-fossil fuel alternatives for electricity generation through the allocation of developmental quotas for each type of renewable technology. Its objective is to diversify a country's energy sources, reduce reliance on expensive fossil fuel imports, promote domestic energy research and reduce polluting emissions. The RPS establishes progressive targets or requires utilities to sell a certain percentage of electricity generated by renewable sources.[10] Global advancements in renewable energy generation are fueled by national commitments to renewable energy.

The first step in the evolution of the RPS in Israel was taken in November 2002, when Government Decision (henceforth, Decision) 2664 mandated the integration of renewable energy into the electricity sector with a minimum 2 percent share by 2007 (above domestic solar water heaters) increasing to 5 percent by 2016.[11] In accordance with Decision 2664, the government implemented policy measures, such as a tariff review and renewable energy technology quotas, to encourage businesses to invest in renewable energy projects. The construction of two large privately-funded solar power plants with a combined capacity of 250 megawatts (MW)[12] near Kibbutz Ashalim in the Negev Desert was approved by Decision 3338 in March 2008.[13] Simultaneously, the government introduced tax benefits for solar photovoltaic (PV) facilities.

In January 2009, Decision 4450 revised the 2002 renewable energy targets to 5 percent and 10 percent by 2014 and 2020, respectively, and included a quantitative target of 1,550MW and 2,760MW. Notably, the Ministry of National Infrastructure was tasked with the responsibility of promoting renewable energy projects as national infrastructure projects. Decision 3484, issued in July 2011, precisely defined grid-connected quotas for solar, wind, biogas and biomass technologies.[14] Solar energy, including residential PV and wind energy, received significantly higher quotas (Figure 1). These quotas were to be distributed by the Electricity Authority, the body in charge of enforcing RPS decisions.

Figure 1: Renewable Energy Quota Allocations, 2011–2012 (in MW)



Source: Author; Government Resolution No. 3484, July 17, 2011; A. Fakhouri & A. Kuperman, "Backup of Renewable Energy for an Electrical Island: Case Study of Israeli Electricity System—Current Status," *The Scientific World Journal* (Hindawi), 2014, p. 4.

In 2008, the Electricity Authority introduced the FIT as a financial incentive to advance Israel's renewable energy sector, and established the tariff rates that the IEC must pay to IPPs or domestic rooftop solar power producers.[15] Israel's solar generation capacity increased steadily and significantly from 2008 to 2012 (Table 1), when the FIT was phased out. Furthermore, as the Decision 3484 empowered the Electricity Authority to conduct a tariff review in order to meet renewable energy targets, it implemented a "net metering scheme" in January 2013. This was intended to encourage self-consumption by domestic producers who had solar panels installed on their roofs.[16] Under net-metering, the IEC would purchase excess energy generated on rooftops by home energy producers. According to the current provisions, whatever mechanism is used for the sale of renewable electricity by entrepreneurs and home users, the tariff will always be determined by the Electricity Authority.[17]

In the run-up to the Paris Climate Conference in November 2015, the Israeli government set a long-term national target of 17 percent clean energy generation by 2030 and a shorter-term target of 13 percent by 2025 to achieve net zero emissions.

In the run-up to the Paris Climate Conference in November 2015, the Israeli government set a long-term national target of 17 percent clean energy generation by 2030 and a shorter-term target of 13 percent by 2025 to achieve net zero emissions. Both of these targets were lofty, given that renewable energy accounted for only 2 percent of Israel's electricity generation at the time. Former Energy Minister Yuval Steinitz announced a new, higher target of 30 percent share by 2030 in February 2020, with an interim target of 17–20 percent by 2025.[18] The elimination of imported coal from Israel's energy mix and total self-sufficiency in electricity generation would occur concurrently. Notably, Israel's decision to raise the renewable energy target coincided with a 362MW increase in solar power capacity, indicating growing confidence in renewable energy development. The year 2020 saw the highest growth in solar power in the previous 15 years, with installed capacity nearly doubling (Table 1).

Table 1: Installed Capacity and Electricity Generation for Solar PV and Solar Thermal in Israel (2005-2020)

Year	Photovoltaic				Solar Thermal			
	Installed Capacity (MW)		Electricity Generation (GWh)		Installed Capacity (MW)		Electricity Generation (GWh)	
	Net Additions	Cumulative	Net Additions	Cumulative	Net Additions	Cumulative	Net Additions	Cumulative
2020	1,040.0	2,230	-	-	(-6.1)	242.0	435.7	447.7
2019	120.0	1,190	1,023	2,597	242	248.1	-	11.3
2018	101.0	1,070	63	1,574	0	6.1	-	11.3
2017	103.0	969	-15	1,511	0	6.1	-	11. 3
2016	100.3	866	365	1,525	0	6.1	-	11. 3
2015	95.8	766	320	1,160	0	6.1	-	11. 3
2014	250.0	670	346	840	0	6.1	-	11. 3
2013	183.3	420	92	494	0	6.1	-	11. 3
2012	47.0	237	80	402	0	6.1	-	11. 3
2011	119.8	190	204	322	0	6.1	-	11. 3
2010	45.4	70	77	119	0	6.1	-	11. 3
2009	21.5	25	37	42	0	6.1	0.2	11. 3
2008	1.2	3	2	5	0	6.1	-	11.1
2007	0.5	2	1	3	0	-	-	-
2006	0.3	1	1	2	0	-	-	-
2005	-	1	-	2	0	-	-	-

Source: International Renewable Energy Agency, September 2021.

Solar PV: Introduction of Competitive Tendering

As of 2017, it was becoming increasingly clear that there was a mismatch between the allotted quotas and their utilization. In light of this discrepancy, Israel's energy ministry decided to launch a new incentive plan for the deployment of 1,600MW of PV capacity over the next three years. The new scheme, designed to support all types of PV facilities—including ground-mounted units, large roofs, reservoirs and small roofs—included a call for tenders and the reinstatement of the FIT.[19] Small rooftop PV installations that did not compete in tenders could send power to the grid at a fixed rate under the FIT scheme. PV projects with a maximum capacity of 15KW were eligible for net metering or FIT for a period of 20–25 years.[20]

While the new scheme retained net metering for installations up to 5MW, the minimum capacity for a single tender was set at 50MW. A tender participant could either sell all electricity to the grid at the winning tariff or to other consumers connected to the same solar roof.[21] Another tendering process awarded the right to build 168MW of solar PV capacity in the Negev desert to three local companies in July 2020 as part of the 300MW scheme launched earlier that year.[22] These projects, which are expected to be completed by 2022, will allow Israel to meet its interim target of 17–20 percent renewables in electricity generation.[23]

By eliminating the bureaucratic regulatory burden that had long been a significant issue for developers, the transition from quota-based FITs to competitive auctions increased predictability in solar PV development.[24] Developers/entrepreneurs of renewable energy can now simply seize the opportunity by offering the best price. The Electricity Authority created open bids to encourage competition, which would eventually lead to lower electricity prices, benefiting consumers if not the profit margins of renewable developers.

In the midst of the COVID-19 pandemic-related losses, the Israeli government's "stimulus package" for economic recovery calls for the addition of 2GW of solar capacity, which will require a total of $7.1 billion in private investment. This capacity addition, backed by the government to the tune of $145 million USD (NIS 500 million) in state guarantees,[25] will complement the 15GW of solar energy required in the coming years to bring renewable energy to 30 percent of total electricity generation by 2030.[26]

In the midst of the COVID-19 pandemic-related losses, the Israeli government's "stimulus package" for economic recovery calls for the addition of 2GW of solar capacity, which will require a total of $7.1 billion in private investment.

Over 80 percent of Israel's electricity generated during peak hours will come from renewable energy sources, primarily solar, with the remainder coming from indigenously produced natural gas. Renewables would meet 100 percent of demand during certain hours, and surplus energy would be stored in batteries.[27] Simultaneously, coal, which currently accounts for 30 percent of the country's electricity generation, would be phased out by 2025.[28] IPP-led investments in renewable generation facilities include the development of energy storage options and grid modernization. The IEC has also unveiled a complementary plan to double transmission capacity from the Negev, which is home to some of Israel's largest solar farms, to the central, more populated areas.

As the share of natural gas produced from Israel's Eastern Mediterranean reserves in electricity generation increases and coal-fired units are phased out, renewables promise increased self-sufficiency for Israel's isolated grid. The cost of solar energy generation continues to decline, and the price is approaching 20 agorot (5.8 cents) per kWh (kilowatt-hour),[29] the reported price at which the IEC will purchase power for 23 years from the winner of the July 2020 solar PV quota awards.[30] In June 2019, EDF Renewables Israel set a record low price of 8.68 agorot (3 cents) per kWh for Ashalim's fourth solar PV energy plant, a significant reduction from the 40 agorot (12 cents) per kWh of Ashalim's first solar thermal plant, which has been operational since December 2017.[31] When compared to natural gas, which costs nearly 7.5 cents per kWh,[32] PV solar appears to be Israel's cheapest energy source, achieving grid parity and kicking Israel's transition to clean energy into high gear.

Given Israel's promotion of rooftop solar panels as a means of increasing the share of renewable energy consumption in a small country, this capacity is increasing by leaps and bound; in 2020 alone, solar PV capacity increased by 87 percent (Table 1). Rooftop generation is a true democratization of electricity generation, and it is emerging as the driving force behind the greening of Israel's power grid.

Wind Energy Generation: A Perilous Endeavor

Wind energy development in Israel has been the slowest of all renewable energy technologies, despite its enormous potential in the country's hilly and mountainous terrain. In 2009, the Electricity Authority approved the FIT for small-scale wind turbines and established a quota of 30MW (domestic consumers up to 15kW and commercial turbines up to 50KW). It allocated 800MW for installation by 2020 and approved the FIT for medium and large wind turbines in 2011.[33] However, the government reduced the wind energy quota by 90MW in October 2014 via Decision 2117, claiming that the sharp decline in solar tariffs increased the cost of wind energy, and thereby transfer-ring approximately 110MW to the solar PV industry.[34]

Wind energy development in Israel has been the slowest of all renewable energy technologies, despite its enormous potential in the country's hilly and mountainous terrain.

Only a few of Israel's 23 proposed wind energy projects have received all of the necessary approvals, and only two wind farms have been connected to the power grid. This is due to the high cost of wind energy generation and opposition from a variety of groups, including environmental activists and the military. Since the early 1990s, Israel has operated a 6MW wind farm in Tel Asania on the Golan Heights,[35] though it is currently in need of repowering. There are currently conditional approvals for wind projects in Golan, specifically the Emek HaBacha (102MW) and Emek Haruchot (169MW) projects, as well as the Ruach Bereshit (130MW) project in the Lower Galilee region.[36] An added 152MW wind project in the northern Golan Heights is also in the works as a critical national infrastructure project.[37]

Emek HaBacha is the most advanced wind project in Israel, with completion scheduled for the end of 2021. Under a 20-year power purchase agreement, the IEC will purchase electricity from the Emek HaBacha project at a rate of 35.81 agorot (Shekel 0.3581) per kWh.[38] This price is instructive because it is lower than that of previously sanctioned projects, but still significantly higher than that of solar PV. In 2014, the Electricity Authority approved a purchase rate of 48.5 agorot (Shekel 0.4851) per kWh for the proposed wind farms in Ramat Sirin (9MW) and Ma'ale Gilboa (11.9MW).[39] In any case, these two projects remain dormant due to a lack of approval from authorities who have cited potential harm to bird and bat populations as well as interference with Israel Air Force operations.[40] Hence, cost is not the only impediment to wind energy development in Israel, as evidenced by the country's low installed capacity of 27MW.[41]

Opposition to Wind Energy

In comparison to solar PV and concentrated solar power, wind energy development has been hampered by strong domestic opposition. Wind turbines, according to environmentalists, harm rare birds nesting in Golan, where wind assessments are optimal for the establishment of wind farms.[42] Environmental-legal challenges brought against wind farm developers have slowed the development of wind energy projects. However, one positive result has been that developers have been forced to take extra precautions with their tasks, such as installing special night radar to reduce bird deaths.[43]

The Israeli Ministry of Defense has long been a formidable impediment to wind energy development, citing operational, radar and other critical system disruptions. Following the rejection of the Sirin project by the National Infrastructure Committee in January 2020, the Israeli ministries of energy, defense, and finance signed a framework agreement to jointly fund NIS 250 million ($72 million USD) for the development of new technology required for wind turbine operation without interfering with military or air force operations.[44] The agreement removes one of the major obstacles to large-scale projects in the Golan Heights.

Wind turbines have also met with strong opposition in Golan from both Arab Druze farmers and Jewish settlers, who fear the proposed installations will endanger human health and the region's fragile biodiversity. Druze farmers are concerned about a number of other issues as well. The planned renewable energy projects in Golan, according to al-Marsad, are a manifestation of Israel's efforts to strengthen its occupation of this Syrian territory. Al-Marsad notes in a forceful report, *Windfall*, that Israel has prioritized the production of natural resource industries in the occupied territories, owing to the fact that these industries are "physically embedded in the land."[45] Israel's creation of "facts on the ground," the authors argue, also explains its efforts to mine oil in the Golan Heights since 2013 from a geologically complex shale play.

According to the report, Israel is looking for a new way to bolster its hold on the Golan Heights by expanding wind energy development there. Many Druze farmers in Golan villages who leased their land to Israeli developer Energix for wind farms claim they were misled by "exaggerations, misleading information, and lies about the perceived benefits."[46] They claim that they signed the lease contracts out of desperation after being unable to sell their produce due to Syria's civil war and seeing their incomes dwindle. Energix's compensation offer appeared reasonable in these circumstances; however, it turned out to be significantly less than the amount offered to Jewish settlers and granted the company unqualified rights. Hundreds of Druze Agricultural Cooperatives and individuals have protested Energix's proposed wind energy development. However, the inspector appointed by the Israeli National Planning and Building Council (for national infrastructure) to investigate the Druze's complaint has rejected all of their objections.[47] Despite community opposition, Israeli companies plan to build 45 wind turbines on 600 hectares of Druze farmland.[48]

Hydropower Expansion as a Back-Up for New Renewables

Hydroelectricity is a tried-and-true, low-cost renewable energy source. The Israeli Energy Ministry has allocated 800MW of pumped hydro-storage capacity for national deployment. Israel lacked hydroelectric generation until July 2020, when the 300MW Gilboa Pumped Storage Hydropower (PSH) in the North began operations.[49] Another PSH project in the works is the 344MW Kokhav Hayarden PSH project in Israel's Northeast.[50] A third project, to build a 156MW PSH facility in Northern Israel, was granted a conditional license in June 2020.[51] Notably, Israel's PHS plants are located in Northern

Israel near Lake Tiberias, the country's primary source of fresh surface water.

In light of Israel's water scarcity, the country's hydroelectric projects are PHS systems that require the construction of two reservoirs separated by a steep gradient and connected via a network of tunnels. Water is allowed to fall from the upper reservoir onto the turbine blades, turning them and generating electricity. After that, water is channeled to collect in the lower reservoir. When the grid is overloaded with power (typically at night or during periods of low demand), the turbines reverse direction to recharge the upper reservoir. Because a PHS project does not qualify as 'new renewable energy source' under the current governmental regulations, the IEC must purchase electricity from it under a 20-year fixed dispatch agreement rather than through the feed-in tariff.

Benefits of Hydroelectricity to Israel

PSH plants are critical components of grid management and control. They can provide electricity to the national grid in less than two minutes and meet peak demand, ensuring grid stability. Moreover, PSH plants eliminate the need for more expensive and environmentally harmful conventional power plants. The upper and lower reservoirs in a PSH plant act as potential energy stores that can be used when needed to ensure the reliability of an electricity system. Hydroelectric generation can meet a significant portion of the grid's variable electricity load as Israel's grid incorporates an increasing amount of renewable energy.

In the event of a power outage, hydroelectricity would allow the IEC to respond quickly and effectively. PSH plants can store energy for extended periods of time, making them an important tool for managing, controlling and streamlining the power system. They are also extremely valuable because they reduce Israel's reliance on imported fossil fuels, improving the country's energy security.

Biogas and Renewable Municipal Waste: A New Frontier

Biogas technology is a technique for producing fuel gas from organic matter such as animal manure, agricultural waste, municipal waste, green plants, sewage, agro-industry and food waste. Biogas is a low-energy fuel because it contains between 50–75 percent methane, as opposed to natural gas, which contains between 80–90 percent methane. Biogas is an excellent energy source for stoves, heaters, lamps, refrigerators and internal combustion engines. The use of a generator to convert biogas to electricity is a well-established technology. Power generation plants using biogas have a significant advantage over solar and wind facilities in that they provide a consistent, non-weather-dependent source of energy. The production of biogas and renewable municipal waste energy also contributes to environmental cleanliness, sanitation, hygiene and groundwater protection. In Israel, where agricultural emissions account for 2.8 percent of total greenhouse gas emissions (2.26 million tons), biogas production could help maximize resource efficiency.[52]

The Electricity Authority established a FIT for biogas plants with a maximum capacity of 160MW in 2011. Nonetheless, in 2014, a ministerial decision allocated 60MW of the biogas quota to solar PV due to growing interest. As of 2020, Israel had 29.3MW of installed renewable energy capacity for biogas and municipal waste out of a total of 100MW quota allocated in 2011 (Table 2). Despite significant progress, biogas projects have been slow to gain traction as biogas cannot supply grid-level electricity, making it less profitable than wind or solar. While biogas will never be able to completely replace conventional fuels, it does have significant emission-reduction potential, which alone should qualify it for increased government support.

Israel is currently building the world's most advanced and environmentally friendly waste-to-energy facility in the Ma'ale Adumim settlement near Jerusalem.[53] This facility would be the first in a series of environmentally friendly alternatives to Israel's landfills, and it is one of several infrastructure projects being promoted by the government as part of the larger 2030 Infrastructure Program, which includes transportation, water, energy and environmental protection. It will help to significantly reduce the national landfill disposal rate from 80 percent to 26 percent.[54]

Despite significant progress, biogas projects have been slow to gain traction as biogas cannot supply grid-level electricity, making it less profitable than wind or solar.

Table 2: Energy from Biogas and Renewable Municipal Waste since the Introduction of Quota and FIT

Year	Biogas		Renewable Municipal Waste	
	Installed Capacity (MW)	Electricity Generation (GWh)	Installed Capacity (MW)	Electricity Generation (GWh)
	Cumulative	Cumulative	Cumulative	Cumulative
2020	26.0	-	-	-
2019	25.0	81.3	3.2	-
2018	25.0	162.7	3.2	-
2017	25.0	162.7	3.2	8
2016	25.0	162.7	3.2	8
2015	25.03	162.7	3.2	8
2014	13.8	89.6	3.2	8
2013	10.9	71.1	3.2	8
2012	6.9	45.1	3.2	8
2011	6.9	45.1	3.2	8

Source: IRENA, September 2021.

Biogas as a Tool for Promoting Peace

Portable bio-gas generators known as 'digesters,' made in Israel, are increasingly being used to generate clean energy for Palestinian villages in remote, off-grid areas of the West Bank.[55] Around 40 digesters have been installed in Al-Awja, a Palestinian village in the Jordan Valley, as part of a European Union-funded pilot project to promote Israeli-Palestinian cooperation through Tel Aviv's Peres Center for Peace and Innovation.[56] In addition, researchers affiliated with the Arava Environmental Studies Institute (AEIS) in the Negev have provided organic waste digesters to Susya, a rural village in Hebron, in collaboration with the Israeli NGO Villages Group. In this location, bio-digesters generate electricity and fertilizer for Palestinian farmers.[57]

A number of bio-digesters have also been installed in Bedouin communities in Israel and Jordan as part of a joint effort between the Middle East Regional Cooperation Program, a USAID-funded research grant program, and AEIS.[58] By utilizing livestock manure that would otherwise accumulate on their land, cause disease and pollute the environment, the biogas equipment now provides low-cost cooking gas to these rural communities.[59] These digesters are portable and can be easily relocated if the Bedouin community so desires.

Smart Grid and Renewable Energy Integration

In Israel, electricity is distributed centrally from power plants that use fossil fuels, allowing the IEC to maintain control over supply and demand. The transition to renewable energy and decentralized electricity generation in Israel will necessitate a shift in grid structure. The increased emphasis on rooftop and backyard solar generation results in bidirectional electricity flow, necessitating efficient management of thousands of producers with varying outputs. In this decentralized production scenario, any endpoint on the grid can act as both a producer and a consumer of green electricity.[60] The 'smart grid' comes into play here.

A smart grid is an upgraded electricity distribution system that makes use of two-way, automated communication technology to collect and analyze real-time data. It enables producers and consumers to make real-time energy purchasing, sales and storage decisions—similar to mobile phone usage packages. As an integral part of the smart grid, smart meters benefit both producers and consumers. While they enable electric utilities to forecast demand in real time, they also provide consumers with real-time information about their electricity usage. Utility companies can reduce operating and management costs by understanding consumption patterns, while consumers can tailor their electricity usage more precisely to their needs, saving both energy and money.

Israel's Smart Grid and Smart Meter Rollout

As part of the IEC's smart grid efforts, the company bid to replace the existing DMS (distribution management system) with an Advanced System (ADMS).[61] In March 2019, the state-owned electricity supplier signed a contract with GE for ADMS; its implementation began in December 2019 with completion scheduled for mid-2021.[62] The IEC's three-stage smart metering initiative is thus currently underway.[63]

The project's first phase, finished in 2014, included the installation of approximately 4,400 smart meters in Binyamina, Givat Ada and the Caesarea Industrial Zone in Northwestern Israel. In February 2017, the IEC awarded Erikson Israel Company a contract to supply smart meters for installation over the next three years as part of the project's second phase. Over 30,000 meters have been installed across the country, allowing the IEC to conduct a practical cost-benefit/tariff analysis of a full transition to smart meters.[64]

The IEC, which constructs, maintains and operates electricity transmission and distribution networks, plans to invest approximately $1 billion in grid modernization to meet the requirements of the 2018 electricity market reforms law.

The final phase will see a nationwide rollout of 2.6 million smart meter units beginning in 2021, ensuring that every meter in Israel will be a smart meter within a few years.[65] The IEC, which constructs, maintains and operates electricity transmission and distribution networks, plans to invest approximately $1 billion in grid modernization to meet the requirements of the 2018 electricity market reforms law. For example, given the more than doubling of Israel's solar energy capacity over the last five years (Table 1), which has been driven by solar power plants in the Negev, the IEC is building a massive Eshkol Negev power transmission line that is expected to be completed in 2023.[66]

Religious Opposition to Smart Meters

Implementing smart grid measures has sparked a number of public concerns, some of which are universal and some of which are unique to Israel. Some people are concerned that the detailed data collected on electricity consumption by smart meters constitutes an unprecedented invasion of their privacy. This is a recurring source of concern for this constituency. Others, including Binyamina residents, have expressed concern about the health risks associated with smart meter radiation. The IEC has responded that home meters would transmit data via a power cable to a regional data box, which would then transmit it via a cellular network to the company's computers, avoiding unnecessary radiation exposure.[67] The religious debate over the use of meters on the Sabbath is a uniquely Israeli issue. The observant Jewish community has already adopted a large number of automated electrical appliances to avoid violating the religious prohibition against using electricity on the Sabbath. There is no reason to believe that a solution to this smart meter problem cannot be found.[68]

Conclusion

The Israeli Ministry of Energy is adamant about eliminating coal, gasoline and diesel from electricity generation and transportation by 2030, and promoting the use of renewable energy and less carbon-intensive natural gas from indigenous fields. Solar PV generation has reached grid parity and has the potential to displace natural gas, which has been critical in Israel's power generation and industrial operations for more than a decade. Along with the liberalization of the electricity market, the renewable energy sector, particularly solar energy, is being vigorously promoted through policy measures. While there is currently no legislation mandating rooftop solar installation as part of the building code, it is clear that such measures could result in increased solar energy penetration. With renewables supplying an increasing amount of electricity, grid fluctuations caused by their intermittent nature present a challenge that must be managed carefully. In the event of a power outage, Israel's PSH can easily inject the necessary electricity into the country's grid, thus providing the country with unprecedented energy security.

Several concerns have been raised about Israel's burgeoning solar market, including whether the country's preference for abundant natural gas will lessen the urgency of renewable energy development. The IEC plans to replace coal-fired power plants in Hadera and Ashkelon with natural gas turbines, and the government is investing in gas infrastructure in the hopes that gas will continue to meet the majority of energy demand in the coming years. It is illogical to propose that Israel's energy system change and eliminate indigenous natural gas, which has provided the country with relative energy independence. Nonetheless, solar PV plants that have begun generating electricity at a significantly lower cost have called into question the cost-effectiveness of natural gas use in the power sector. In view of the imperatives of climate change mitigation and the country's need for a continuous and sustainable source of energy, it is safe to say that while natural gas will remain critical to Israel's energy system for the foreseeable future, renewable energy will contribute to increased electricity generation in the coming years.

Endnotes

1 According to the *BP Statistical Review of World Energy 2021*, renewable energy accounted for 3.3 percent of power generation in 2019 and 5.7 percent in 2020.

2 Annual incident solar irradiance is approximately 2000 kWh per square meter (sqm) at approximately 30 degrees North latitude, which equates to an average of 5.5 kWh per sqm radiative energy per day, indicating a very high intensity.

3 *The Israeli Net Metering Scheme: Lessons Learned*, Israel: Public Utilities Authority (PUA) Electricity, September 29, 2014, p. 2.

4 *Electricity Market Report for 2017*, Israel: Ministry of Energy, 2017, p. 63.

5 "Alternative Energy/Cleantech," *Nefesh B'Nefesh*, 2019, https://www.nbn.org.il/aliyahpedia/employment-israel/professions-index-employment-israel/hi-tech/alternative-energy/.

6 "Overview of the Israeli Electricity Market 2020," *LNRG Technology*, August 30, 2020, https://www.lnrg.technology/2020/08/30/overview-of-the-israeli-electricity-market-2020/.

7 Alon Tal, "Will we Always Have Paris? Israel's Tepid Climate Change Strategy," *Israel Journal of Foreign* Affairs, Vol. 10, No. 3 (September 2016), p. 411.

8 "Renewable Energy Planning and Policy—An Overview: Lawmakers Pass First Solar Energy Legislation," *Ministry of Environmental Protection*, February 19, 2017, https://www.sviva.gov.il/English/env_topics/climatechange/renewable-energy/Pages/Renewable-Energy-Planning-And-Policy.aspx.

9 K. Hudon et al., *Low-Cost Solar Water Heating Research and Development Roadmap*, Denver, Colorado: National Renewable Energy Laboratory, US Department of Energy, Office of Energy Efficiency & Renewable Energy, 2012, p. 23.

10 "Renewable Energy Standards," *Solar Energy Industries Association*, 2020, https://www.seia.org/initiatives/renewable-energy-standards; "Renewable Portfolio Standards," *National Renewable Energy Laboratory*, https://www.nrel.gov/state-local-tribal/basics-portfolio-standards.html.

11 *Decision Number 2664: Electricity Generation Policy—Renewable Energy* (in Hebrew), 2002.

12 A megawatt is a unit for measuring power, equivalent to one million watts.

13 "Financing has been Completed in a BOT Tender for the Planning, Construction and Operation of the Thermal Power Plant in Ashalim," *Ministry of Energy*, June 25, 2014, https://www.gov.il/he/Departments/news/ashalim_energy_station.

14 "Government Resolution No. 3484," *Government of Israel*, July 17, 2011, https://www.gov.il/he/Departments/policies/2011_des3484.

15 A FIT is a long-term contract between a government public utility and a small-scale renewable energy producer. It guarantees an over-the-counter price for each electrical unit injected into the grid by a producer. *The Israeli Renewable Energy Market and Regulation: Current Status Report*, Israel: PUA Electricity, June 1, 2013, p. 1; Arnulf Jäger-Waldau, *PV Status Report 2019*, Luxembourg: Publications Office of the European Union, 2019, pp. 1–85, https://ec.europa.eu/jrc/sites/jrcsh/files/kjna29938enn_1.pdf.

16 Net metering is a tax credit that allows homeowners and businesses with solar PV systems to export their net surplus to the grid. In exchange, 'credits' can be redeemed for a reduction in the user's electricity bill or for use at night or at other times of the year (for example, during the winter months) when electricity consumption exceeds output and more electricity is drawn from the grid. See "Israel Net-Metering Regulation Framework," *International Energy Agency*, August 25, 2017, https://www.iea.org/policies/6381-israel-net-metering-regulation-framework.

17 *The Israeli Net Metering Scheme*, p. 1.

18 Gwen Ackerman & Filipe Pacheco, "Renewable Energy Push Boosts Bets on Wind, Solar in Israel," *Bloomberg Quint*, August 26, 2020, https://www.bloombergquint.com/technology/renewable-energy-push-boosts-israel-investor-bets-on-wind-solar.

19 "Policy Principles—Additional Quota Required to Meet Government Targets for Electricity Generation from Renewable Energy by 2020," *Ministry of Energy*, November 26, 2017, https://www.gov.il/he/Departments/policies/renewable_energy_2020.

20 Veselina Petrova, "Israel Unveils Plans for 1st Solar Tenders, 1.6-GW Goal—Report," *Renewables Now*, November 27, 2017, https://renewablesnow.com/news/israel-unveils-plans-for-1st-solar-tenders-16-gw-goal-report-592435/.

21 Emiliano Bellini, "Israel Issues 1.6 GW Scheme for Rooftop Solar," *PV Magazine*, March 29, 2018, https://www.pv-magazine.com/2018/03/29/israel-issues-1-6-gw-scheme-for-rooftop-solar/.

22 José R. Martín, "Israel Seeks Developers for 300MW Solar Project in Negev Desert," *PV Tech*, January 24, 2020, https://www.pv-tech.org/news/israel-seeks-developers-for-300mw-solar-project-in-negev-desert.

23 Vaselina Petrova, "Pre-qualification Round in 300-MW Israeli Solar Tender Gets 27 Bids," *Renewables Now*, June 24, 2020, https://renewablesnow.com/news/pre-qualification-round-in-300-mw-israeli-solar-tender-gets-27-bids-703840/.

24 *Electricity Market Report for 2017*, Israel: PUA Electricity, 2017, pp. 66–67, https://www.gov.il/BlobFolder/generalpage/dochmeshek/he/Files_doch_meshek_hashmal_doch_meshek_2017_eng.pdf.

25 Emiliano Bellini, "Israel's Plan to Recover from Covid-19 Crisis Includes 2 GW of New Solar," *PV Magazine*, April 29, 2020, https://www.pv-magazine.com/2020/04/29/israels-plan-to-recover-from-covid-19-crisis-includes-2-gw-of-new-solar/.

26 Anu Bhambhani, "Israel Wants over 15 GW Solar By 2030," *Taiyang News*, June 3, 2020, http://taiyangnews.info/markets/israel-wants-over-15-gw-solar-by-2030/.

27 Amiram Barakat, "Israel's Renewable Energy Target: 30% by 2030," *Globes*, June 2, 2020, https://en.globes.co.il/en/article-israels-renewable-energy-target-30-by-2030-1001330943.

28 "Review of Developments in the Natural Gas Economy" (in Hebrew), *Ministry of Energy*, March 22, 2020, p. 11. https://www.gov.il/he/Departments/publications/reports/ng_2019.

29 A kilowatt-hour is a measure of electrical energy equivalent to a power consumption of one thousand watts for one hour.

30 Yoram Gabison, "An Energy Revolution for Israel: Solar Power to be Cheaper than Fossil Fuel," *Haaretz*, July 15, 2020, https://www.haaretz.com/israel-news/business/.premium-an-energy-revolution-for-israel-solar-power-to-be-cheaper-than-fossil-fuel-1.8994782.

31 Sue Surkes, "EDF Renewables Wins Tender to Build Solar Plant, Sets New Low in Prices," *The Times of Israel*, December 5, 2019, https://www.timesofisrael.com/edf-renewables-wins-tender-to-build-solar-plant-sets-new-low-in-prices/.

32 Lior Gutman, "Electricity from Solar Power has Become so Cheap, No Other Sources can even Compete," *CTECH (Calcalist)*, September 7, 2020, https://www.calcalistech.com/ctech/articles/0,7340,L-3848585,00.html; "Israel: EDF Renewables Wins a Call for Tenders for the Construction of a Solar Power Plant," *i24News*, December 8, 2019, https://www.i24news.tv/fr/actu/israel/1575654251-israel-edf-renouvelables-remporte-un-appel-d-offres-pour-la-construction-d-une-centrale-solaire%C2%A0%C2%A0.

33 "Market Overview—Renewables," *Green Energy Association of Israel*, *202*0, http://www.greenrg.org.il/he-il/english.htm#:~:text=Small%2Dscale%20wind%20turbine%20FIT,introducing%20a%20quota%20of%20800MW; Heather O'Brian, "Israel Plans Two-tier Wind Tariff," *WindPower Monthly*, February 1, 2011, https://www.windpowermonthly.com/article/1052519/israel-plans-two-tier-feed-in-tariff.

34 "Government Resolution 2117: Implementation of Government Targets for Electricity Generation from Renewable Sources—A Discussion of Appeals against the Decision of the Ministerial Committee on the Promotion, Development and Implementation of Renewable Energy," *Government of Israel*, October 22, 2014, https://www.gov.il/he/Departments/policies/2014_govdec2117; Ivan Shumkov, "Israel Revises Quotas to Open Space for 520MW of Additional PV," *Renewables Now*, October 23, 2014, https://renewablesnow.com/news/israel-revises-quotas-to-open-space-for-520-mw-of-additional-pv-444560/.

35 The Golan Heights (commonly known as Golan) is a 1,800-square-kilometer rocky plateau on the border between Israel and Syria in Southwestern Syria. Israel occupied the Golan Heights, the West Bank, East Jerusalem and the Gaza Strip during the June 1967 Arab-Israeli War. Following the establishment of an armistice line, the region came under Israeli military control. Syria attempted but failed to reclaim the Golan Heights during the 1973 War. Both countries signed an armistice in 1974; since then, a UN observer force has been stationed along the ceasefire line. Israel permanently occupied the Golan Heights and East Jerusalem in 1981, a move that has not been recognized by the international community.

36 Jan Dodd, "Israel's Plans to Tap into Wind Power Take Shape," *WindPower Monthly*, January 30, 2015, https://www.windpowermonthly.com/article/1331651/analysis-israels-plans-tap-wind-power-shape.

37 "Periodic Report for 2017," *Energix Group*, 2017, p. 44, https://www.energix-group.com/uploads/1543916097.pdf.

38 Yoram Gabison, "Largest Wind Energy Project in Israel Commences: Will Bring in NIS 105 Million Per Year," *The Marker* (in Hebrew), June 10, 2018, https://www.themarker.com/markets/1.6159248.

39 Aviram Barakat, "Electricity Regulator Accused of Smothering Wind Energy," *Globes*, June 30, 2014, https://en.globes.co.il/en/article-electricity-regulator-accused-of-smothering-wind-energy-1000950342.

40 Zafirt Rinat, "State Panel Rejects Wind Turbine Project in Israel's Lower Galilee," *Haaretz*, October 2, 2019, https://www.haaretz.com/israel-news/.premium-state-panel-rejects-wind-turbine-project-in-israel-s-lower-galilee-1.7924543.

41 "Onshore Wind Energy," in *Renewable Energy Statistics 2021*, New York: IRENA, 2021.

42 Andrew Lee, "Bird Campaigners Bid to Halt Israel's Largest Wind Farm," *Recharge*, February 11, 2019, https://www.rechargenews.com/wind/bird-campaigners-bid-to-halt-israels-largest-wind-farm/2-1-540367.

43 Rinat, Zafrir, "Wind Turbines in Israel Kill Many More Birds, Bats than Expected," *Haaretz*, December 20, 2017, https://www.haaretz.com/israel-news/wind-turbines-in-israel-kill-many-more-birds-bats-than-expected-1.5629170.

44 Eytan Halon, "Israel Green Lights Hundreds of Wind Turbines in North," *Jerusalem Post*, January 1, 2020, https://www.jpost.com/israel-news/israel-green-lights-hundreds-of-wind-turbines-in-northern-israel-612757.

45 Aaron Southlea & D. Nazeh Brik, *Windfall: The Exploitation of Wind Energy in the Occupied Syrian Golan*, Majdal Shams, Golan Heights: Al-Marshad Arab Human Rights Centre in Golan Heights, January 2019, p. 8.

46 Ibid, p. 18.

47 Al-Haq et al., "Occupied Syrian Golan Wind Turbine Project Poses Existential Threat to Indigenous Syrian Population," *Business and Human Rights Resource Centre*, https://www.business-humanrights.org/en/latest-news/occupied-syrian-golan-wind-turbine-project-poses-existential-threat-to-indigenous-syrian-population/.

48 Hazem Sabbagh, "People of Golan Reiterate Rejection of Israeli Occupation's Plans to Wind Turbines on their Land," *Sana News Agency*, May 18, 2020, http://sana.sy/en/?p=191964.

49 "Israel's 300-MW Mount Gilboa Pumped Storage Begins Operating," *World Energy*, May 8, 2020, https://www.world-energy.org/article/9080.html.

50 "GE Renewable Energy Books $100+MM Deal for Hydro Pumped Storage Project in Israel," *General Electric*, August 8, 2017, https://www.ge.com/news/press-releases/ge-renewable-energy-books-100mm-deal-hydro-pumped-storage-project-israel.

51 Max Hall, "Israel Prepares 800MW of Pumped Hydro Storage," *PV Magazine*, June 24, 2020, https://www.pv-magazine.com/2020/06/24/israel-prepares-800-mw-of-pumped-hydro-storage/.

52 Aimee Teplitskiy, "The Start-up that Turns Cow Patties into Clean Energy," *Israel21c*, August 4, 2019, https://www.israel21c.org/the-startup-that-turns-cow-patties-into-clean-energy/.

53 The international community considers all settlements built by Israel in territories occupied by it during the 1967 Arab-Israeli war to be illegal.

54 Etan Yalon, "Israel to Construct First Waste-to-energy Power Plant," *Jerusalem Post*, October 15, 2019, https://www.jpost.com/israel-news/israel-to-construct-first-waste-to-energy-power-plant-604380.

55 Robert Hackwill, "Palestinian Engineer Develops Affordable Gas Generator Powered by Waste," *Euronews*, December 1, 2015, https://www.euronews.com/2015/12/01/palestinian-engineer-develops-affordable-gas-generator-powered-by-waste.

56 Ori Lewis & Elana Ringler, "Israeli Biogas Digesters Energize Isolated Palestinian Village," *Reuters*, August 24, 2015, https://www.reuters.com/article/us-israel-palestinians-biofuels/israeli-biogas-digesters-energize-isolated-palestinian-village-idUSKCN0QT0RB20150824.

57 "Organic Waste Recycling & Biogas Production," *Arava Institute for Environmental Studies (AIES)*, https://arava.org/arava-research-centers/center-for-renewable-energy/organic-waste-recycling-biogas-production/.

58 Ibid.

59 Ibid.

60 Kirsi Kotilainen & Ulla A. Saari, "Policy Influence on Consumers' Evolution into Prosumers: Empirical Findings from an Exploratory Survey in Europe," *Sustainability*, Vol. 10, No. 186 (2018), p. 1.

61 DMS is an information technology system for utilities that collects, organizes, displays and analyzes data on a real-time electrical distribution system, enabling operators to plan and operate complex electricity distribution-related operations. It optimizes grid efficiency, prevents overload, and optimizes power flows. Apart from DMS operations, ADMS as a software platform enables the integration of renewable energy into the grid. Due to the fact that a large amount of cumulative power is injected into the grid's distribution section at various times (via decentralized renewable generation), ADMS includes functions that forecast load, prevent interruption and automatically restore shutdown. This way, the distribution network's performance can be optimized. *Utilities Find Success Using NREL's ADMS Test Bed for Grid Modernization*, Office of Energy Efficiency and Renewable Energy, US Department of Energy, March 2020, pp. 1–2; "Distribution Management System," *Open EI*, 2012, https://openei.org/wiki/Definition:Distribution_Management_System.

62 "Israel Electric Corporation Ltd. Electricity Generation, Transmission, Distribution, and Supply," *BDI Code*, 2018, https://www.bdicode.co.il/en/company/israel-electric-corporation-ltd-en/.

63 *Financial Reports*, Israel Electric Corporation Ltd, December 31, 2016, p. 77.

64 "Ericsson Israel Won a Procurement Tender for Supplying Smart Meters in the Electricity Network," *Tashtiot*, February 12, 2017, http://www.tashtiot.co.il.

65 "Smart Meters," *Tnuda*, January 23, 2018, https://www.tnuda.org.il/en/policy-and-legislation/smart-meters.

66 Amiram Barkat, "5% of Israel's Electricity Now Produced from Solar Energy," *Globes*, November 6, 2019, https://en.globes.co.il/en/article-5-of-israels-electricity-now-produced-from-solar-energy-1001306287.

67 Nati Yefet, "Erickson Israel Will Supply 200,000 Smart Meters to the IEC," *Globes*, February 2, 2017, https://www.globes.co.il/news/article.aspx?did=1001176544.

68 Lucy Michaels & Yael Parag, "Motivations and Barriers to Integrating 'Prosuming' Services into the Future Decentralized Electricity Grid: Findings from Israel," *Energy Research & Social Science*, Vol. 21 (November 2016), p. 71.

BOOK REVIEW

The Hell of Good Intentions: America's Foreign Policy Elite and the Decline of U.S. Primacy

By Stephen Walt

New York: Farrar, Straus & Giroux Inc., 2018, 400 pages, ISBN: 978-0-374-71246-4

In his resounding book, *The Hell of Good Intentions: America's Foreign Policy Elite and the Decline of U.S. Primacy*, Stephen M. Walt, Professor of International Affairs at Harvard University, scrutinizes the flaws and weaknesses of the U.S. contemporary foreign policy establishment. Walt is a member of the neorealist school of thought in the International Relations discipline, alongside leading scholars such as John J. Mearsheimer, Barry Posen and Christopher Layne. Whilst these realist theorists believe that great powers' behaviors are characterized mainly by systemic variables, they are strict opponents of liberal hegemonic strategy, which is based on norms, beliefs and ideas. They eschew approaches such as promoting democracy and liberal values in foreign policy behaviors. In line with these views, Walt's core motivation in *The Hell of Good Intentions* is to criticize the liberal hegemony policy that the U.S. has pursued since the beginning of the 1990s. According to Walt, the U.S., from then onward, has sought to spread liberal internationalist values and beliefs such as democracy, freedoms, institutions and a liberal economic system based on free-market strategy. Walt asserts that this strategy has caused the U.S.'s mutual relations with various countries to deteriorate, prolonged wars and exacerbated conflicts in many regions and led rivals to obstruct U.S. initiatives in international politics.

Walt divides his book into seven main chapters to test liberal hegemony strategy. In the first, "A Dismal Record," Walt explores the political attitudes of the administrations that took power after 1990 and fiercely criticizes the liberal foreign policy establishment. In the second chapter, "Why Liberal Hegemony Failed," Walt classifies the reasons behind the failed strategy and further clarifies the grounds that have led to undesirable results for the position of the U.S. in world politics during the last three decades. In the third and fourth chapters, "Defining the 'Blob': What is the 'Foreign Policy Community'?"

and "Selling a Failing Foreign Policy," Walt focuses on the formal/informal organizations and individuals that shape the American foreign policy agenda and explains the relations between the foreign policy community and American society on foreign policy issues. In these chapters, Walt investigates how different political tools used by the foreign policy community have created change, and how they have influenced the American society's foreign policy interpretation. In the last three chapters "Is Anyone Accountable?" "How Not to Fix U.S. Foreign Policy" and "A Better Way," Walt discusses Donald Trump's unsuccessful foreign policymaking, offers a new grand strategy formation, namely offshore balancing, for U.S. foreign policy and explains why this strategy is the best way to maintain the interests and hegemonic position of the U.S. in international politics.

In the first chapter, Walt substantially assesses Bill Clinton, George W. Bush and Barack Obama's foreign strategy and policy formation. Walt indicates that the U.S. was the sole superpower in world politics at the beginning of the 1990s, and that no country then had the economic and military power to challenge U.S. hegemony. Both China and Russia, as possible challengers, were quite weak both militarily and politically, and U.S. relations with them were acceptably good and stable at the time. Furthermore, Walt analyses power indicators, noting that the U.S. had the largest economic power with approximately 60% GDP rates, and produced nearly 25% of total services and goods in the world during this period. In addition to its huge economic power, the U.S. was also a unique power that had a military presence in many parts of the world. Walt argues that all of these circumstances situated the U.S. in a special position in political history.

From the 1990s onward, President Clinton adopted a national security strategy based on "engagement and enlargement," Bush declared a period of "democratic peace" and Obama supported liberal international values. Despite their positive attitudes, Walt deems that the strategies implemented by these presidents exacerbated global and regional problems, such as the Israel-Palestinian issue, North Korean nuclear armament and the challenges posed by Iran and Al-Qaeda, making these problems much worse and more complicated and leaving the U.S. with intractable problems.

In the second chapter, Walt explains why the liberal hegemonic strategy that has been implemented since the beginning of the 1990s has failed. According to Walt, liberal hegemony based on misguided strategic calculations has many visible shortcomings. He argues that there are several important reasons why the liberal hegemony strategy has failed. Liberal theorists and policymakers suppose that this strategy can effortlessly spread democracy and intensify mutual economic interdependence among states. In contrast, Walt claims that economic interdependence, economic globalization and democracy have limited explanatory power in understanding world politics. Walt maintains that the wisdom put forward by liberals does not eliminate uncertainty and rivalry among states. Similarly, Walt contends that liberal theorists exaggerate the ability and importance of institutions to prevent international conflicts or wars. Institutions such as NATO, the WTO and the World Bank may work well if states have clear motivations to support them. Since states' intentions are uncertain, they use institutions as a foreign policy tool in order to protect their vital interests and/or to increase their sphere of influence.

In the third chapter, Walt addresses the "Foreign Policy Community," which consists of formal/informal organizations and individuals that directly or indirectly shape the foreign policy agenda of the country. As Walt states, the community involves many actors, such as international relations professors, think tank members, senators, interest groups, lobbies, media, CIA analysts and officers of the U.S. Foreign Service. Walt considers that many of the community members defend the idea that the U.S. should implement a liberal hegemonic strategy to be more prosperous and more secure, and deduce that for this reason, the U.S. should take on a leadership role in solving international problems and keeping the liberal international order established by the U.S. alive. Nonetheless, Walt stresses that the U.S. public has a totally different opinion when compared to the community's policy approaches; many American citizens are uncertain about the country's deep liberal engagement with global issues.

The fourth chapter deals with the subject of the previous chapter in more detail. Walt insists that since there is a strict difference between the community and the public on foreign policy problems, the community employs various arguments and rhetoric in order to convince American society to support liberal hegemony. In that respect, the first considerable step taken by the community is to overstate the international dangers that the U.S. faces. This step is recognized by Walt as "Threat Inflation." Inflators view the world as full of threats and dangers and they absolutize that the U.S. must always act rapidly against any threats. By exaggerating antagonists' capabilities and manipulating international uncertainty, threat inflators generally attempt to convince the public. They also overstate the advantages of liberal hegemonic strategy.

In the last chapter, Walt offers an alternative strategy for U.S. foreign policy in light of the constant failures of the past administrations. According to Walt, the strategy that the U.S. should implement is offshore balancing in order to maintain its hegemonic position in global politics. Walt, as an offshore balancer, claims that few regions in the world have crucial significance for the U.S. position and security. These regions are the Western Hemisphere, the Persian Gulf, Europe and Northeast Asia. Offshore balancing depends on the theory of the distribution of power, which asserts that if there is a potential hegemonic power that can challenge the status quo in these regions, the U.S. should directly deploy its forces there in order to preserve the balance of power and to prevent the actions of threatening rising powers. Walt reckons that this strategy has several noticeable advantages and gains for the U.S. By implementing offshore balancing, Walt asserts, the U.S. can reduce its defense expenditure and can cut unnecessary military costs as well. Thus, it can increase its spending in other important areas such as education, health, R&D and infrastructure within the country.

The Hell of Good Intentions may be classified as a crucial book for readers interested in recent trends in American foreign policy. The book is written appropriately enough for any casual reader to enjoy, and is deep enough to benefit international relations scholars too. Anyone who intends to comprehend the past and contemporary foreign policy strategies of the U.S. and their outcomes will find the book satisfying and well-organized. In a similar vein, the book is an outstanding critique of liberal hegemony. Walt's critical assessment that the U.S.'s attempts to promote liberal values globally since the end of the Cold War period have caused the U.S. to become less safe and prosperous is timely and relevant. And it should not be forgotten that the alternative foreign policy strategy Walt proposes, namely offshore balancing, is a grand strategy with growing influence on the U.S.' future policy approach to international politics.

Orhan Çifçi
Research Assistant / PhD Candidate
Turkish National Police Academy
Department of International Security
ORCID: 0000-0002-5746-4258

Style and Format

Articles submitted to the journal should be original contributions. If another version of the article is under consideration by another publication, or has been or will be published elsewhere, authors should clearly indicate this at the time of submission. Manuscripts should be submitted to: e-mail: perceptions@mfa.gov.tr The final decision on whether the manuscript is accepted for publication in the Journal or not is made by the Editorial Board depending on the anonymous referees' review reports.

A standard length for PERCEPTIONS articles is 6,000 to 8,000 words including endnotes. The manuscript should begin with an indented and italicised summary up to 150 words, which should describe the main arguments and conclusions, and 5-7 keywords, indicating to main themes of the manuscript. A title page should be attached to the manuscript, including the title of the manuscript, full name (s) of the authors, academic and/or other professional affiliations if any, complete mailing address, fax and phone numbers of the author to whom proofs and correspondence should be sent. The author is also expected to give a brief biography in a footnote at the beginning of the article. Perceptions also publishes reviews of new books or reports; 'book reviews' are usually around 700-1,500-words."

Manuscripts should be single-spaced written by Times New Roman regular font, 11 point throughout. Justified margins; top and bottom 3 cm, left and right 2.4 cm are required. Manuscripts should be numbered consecutively throughout the paper. Only the first letters of title words should be 'upper case'. Quotations should be placed within double quotation marks ("……"). Quotations larger than four lines should be indented at left margin and single-spaced. Use endnotes and avoid bibliography. British punctuation and spelling should be used throughout. Dates should be in the form 3 November 1996; 1995-1998; and 1990s. All diagrams, charts and graphs should be referred to as figures and consecutively numbered. Tables should be kept to a minimum and contain only essential data. Each figure and table must be given an Arabic numeral, followed by a heading, and be referred to in the text. Appropriate places of tables should be indicated in the text and tables should be submitted in a separate file. If copyrighted material is used in the article, it is the author's responsibility to obtain permission from the copyright holder.

Names of the authors, places and the publishing houses are required to be written in their original forms. The styles of the references in endnotes should conform the following examples:

Books

John Smith, The Book Title, New York, New York Publishing Co., 1999, p. 100.

John E. Smith (ed.), The Book Title, New York, New York Publishing Co., 1999, pp. 100-102.

John Smith and Mary Jones, The Book Title, New York, New York Publishing Co., 1999, p. 100. Subsequent references should appear as: Smith, The Book Title, p. 100. In endnotes 'Ibid.' should be used where possible, but it should not be used where the previous note contains more than one source.

Articles in Journals

John Smith, "Article Title", Journal Name, Vol. #, No. # (Month Year), p. #.

Subsequent references should appear as: Smith, "Article Title", p. #.

Articles in Edited Books

John Smith, "Article Title", in Mary Jones (ed.), Book Title, New York, New York Publishing Co., 1999, p. 100.

Newspaper Articles

Christopher Hooton, "Japan is Turning Its Abandoned Golf Courses into Solar Power Plants", The Independent, 21 July 2015.

Manuscript References

PRO King's Remembrancer's Memoranda Roll, E159/69, m. 78. BM Add. MS 36042, fo.2 (plural fos.). Four-figure numerals without comma or space: 2572. Titles of other record repositories, and names of collections of papers, in full in first reference: Scottish Record Office (hereafter SRO), Airlie Papers, GD 16, section 38/82, April 5, 1844. Compton Papers, kept at the estate office of the Marquess of Northampton, Castle Ashby (hereafter CA), bdle. 1011, no.29.

Official Papers

Parliamentary Papers: Select Committee on Manufacturers (Parl. Papers, 1833, VI), 0.456. Subsequent references as: SC on ... (PP, 1839, VII), 00.2347.

Hansard (Commons), 4th ser. XXXVI, 641–2, 22 Aug. 1895.

Theses

For titles of published and unpublished theses use italics: John E. Smith, Title of Thesis, unpublished Ph.D. thesis, Name of the University, Year, Chapter #, p. #

Internet References

Azam Ahmed and Julie Hirschfeld Davis, "U.S. and Cuba Reopen Long-Closed Embassies", The New York Times, 20 July 2015, http://www.nytimes.com/2015/07/21/world/americas/cu-ba-us-em-bassy-diplomatic-relations.html?ref=world&_r=0 (Accessed 21 July 2017).

Title of Book Reviews

Türk Basınında Dış Habercilik (Foreign News Reporting in the Turkish Media), by M. Mücahit Küçükyıl-maz and Hakan Çopur. Ankara: SETA, 2010, 168 pages, ISBN 9786054023073.

9 343986 001595