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 incomplete; 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.