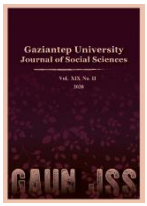

GAZİANTEP UNIVERSITY
JOURNAL OF SOCIAL SCIENCES

Journal homepage: http://dergipark.org.tr/tr/pub/jss

Araştırma Makalesi ● Research Article

Siber Güvenlik Açısından Savaş Yönetim Sistemleri ve Türkiye

Combat Management Systems in Terms of Cyber Security in Türkiye

Elif GÜRDAL LİMON[a]*

[a] Dr. Öğr. Üyesi, Gümüşhane Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Uluslararası İlişkiler Bölümü, Gümüşhane / TÜRKİYE
ORCID: 0000-0001-5110-6524

MAKALE BİLGİSİ

Makale Geçmişi:
Başvuru tarihi: 11 Ağustos 2023
Kabul tarihi: 3 Ekim 2023

Anahtar Kelimeler:
Siber güvenlik,
Savaş yönetim sistemi,
Askerî dijitalleşme,
Türkiye,
Savunmacı realizm.

ÖZ

Ulusal güvenliğin bir parçası olarak kabul gören siber güvenlik konsepti bu çalışmada devletlerin kendi başlarının çaresine bakma (self-help) yaklaşımıyla yorumlanmaktadır. Özellikle askerî birimlerde kullanılan Savaş Yönetim Sistemleri (SYS) gibi dijital yeniliklerden kaynaklı saldırı kaynağı, yeri, türü gibi belirsizlik arz eden siber savaş ortamına karşı devletler garanti siber güvenlik tedbirleri almaya yönelecektir. Çalışmada amaç siber güvenliğin ulusal güvenlikteki payının büyüdükçe devletlerin kendi başının çaresine bakma eğiliminin arttığını vurgulamaktır. Ayrıca siber güvenlik; mühendislik anlayışı bakımından değil, uluslararası ilişkilerdeki güç unsuru bakımından ele alınmıştır. Bunun için çalışma askerî teçhizatların yerli üretilme konusunu ve siber güvenliğini analiz etmeye çalışmaktadır. Çalışmanın teorik dayanağı savunmacı realist yaklaşımdır. Bu açıdan yapısalcı bir yaklaşım üzerinden askerî dijital yeniliklerin yeri oturtulmaya çalışılmıştır. Çalışmanın inceleme alanı Türkiye'deki SYS'dir. Türk menşeili savunma sanayi şirketleri ve Savunma Bakanlığı verileri üzerinden bir çalışma yapılmıştır. Ayrıca uluslararası enstitü indeksleri ile siber veri indekslerinden yararlanılmış ve bu alandaki önemli kurumlarla iletişim kurulmuştur. Sonuç olarak, Türkiye üzerinden yapılan bu çalışmada siber güvenlik ulusal güvenlikle özdeşleştirilmiştir. Siber güvenlik endişeleri Türk askerî dijital sistemlerinin millî üretimler olması gerekliliğinde bir etken olmuştur. Siber güvenliğin ulusal güvenlikteki rolü büyüdükçe devletlerin kendi başının çaresine bakma eğilimi artmaktadır. Ayrıca Türkiye'nin savunma sanayinde yerli üretimlere yöneldiği ancak bunu saldırgan eğilimle değil savunmacı bir perspektifle uyumlu olarak yaptığı görülmüştür.

ARTICLE INFO

Article History:
Received: August 11, 2023
Accepted: October 3, 2023

Keywords:
Cyber security,
Combat management system,
Military digitalization,
Türkiye,
Defensive realism.

ABSTRACT

The concept of cyber security, which is accepted as a part of national security, is interpreted with the self-help approach of states as emphasized in this study. Especially in combat management systems (CMS) used in military units, states will tend to take guaranteed cyber security measures against the cyber war environment, which is uncertain such as the source, location, and type of attack due to digital innovations. This study aims to reveal that the self-help tendency of states increases as the share of cyber security in national security grows. This study deals with cyber security not in terms of engineering but of power in international relations. For this, it tries to analyze the issue of domestic production of military equipment and its cyber security. The theoretical basis of the study is the defensive realist approach. In this respect, it has been tried to place military digital innovations through a structuralist approach. The field of study is CMS in Türkiye. It has been a study on the data of Turkish defense industry companies and the Ministry of Defense. In addition, international institute indexes and cyber data indexes were used. Important institutions have been contacted. As a result, in this study conducted over Türkiye, cyber security has been identified with national security. Cyber security concerns have been a factor in the necessity of Turkish military digital systems to be national productions. As the role of cyber security in national security grows, the self-help tendency of states increases. In addition, it has been observed that Türkiye is oriented towards domestic production in the defense industry, but this is done in line with a defensive perspective, not with an aggressive tendency.

* *Sorumlu yazar/Corresponding author*.
e-posta: elif.gurdal@gumushane.edu.tr

EXTENDED ABSTRACT

Hierarchy, which does not exist in the international system, is at the base of the power struggle that emerged as a result of the anarchic structure. Dilemmas arise in the actions of states that are based on international power. In these dilemmas, it can be seen that the choices in defensive and offensive actions are the issues that shape international relations. A security dilemma may arise due to the armament of a state and the belief or interpretation of the other actor in reading intent. However, this dilemma in cyber warfare does not create a clear armament situation because the security threshold in the cyber security environment is not clear or the security area cannot be separated with sharp lines. This is why the defensive priority is the only clear choice in digital security.

Power competition in international relations is also carried out in new areas due to the diversification of political tools. Digital transformation, which is an important factor in this regard, causes the diversification of battlefields and an increase in security areas. Cyber threats are increasing day by day, and the diversity in attack and defense methods creates new defense expenditures with an unknown threshold.

The fact that a state has not been able to develop itself in the field of technology in terms of material power capacities may still make it weak even if it eliminates all classical threats, overt or covert. The digital field is so absorbed into the whole world that technological competence has become a criterion in the definitions of state power. The concept of 'cyber' is important because it defines a new field of war and security. The issue of security concerns states, non-state actors, and even individuals. However, the responsible actor for security is the state. International issues such as cyber warfare and cyber security, which are now part of national security, force states to take singular defense-oriented precautions. It is seen that states are more inclined to maintain their security positions in the cyber warfare field.

Therefore, states are more inclined to self-help to create guarantee conditions to provide their cyber security in military systems. As cyber war risks further threaten national security, states will become even more defensive about military digitalization. In this respect, it can be said that cyber warfare in the military field can be defined as a defensive realist understanding. Relying on the technologies of other states for military digitalization will not provide a long-term cyber security guarantee.

This article exemplifies and examines the defensive realist approach to cyber protectionism in the military field through Türkiye. The study hypothesizes that as the share of cyber security in national security grows, the self-help tendency of states towards military digitalization increases. For this reason, Türkiye tends towards nationalization and displays a defensive realist approach. It can be said that Türkiye focuses on the defensive aspect in terms of focusing on technological investments and reducing imports. In light of these developments, it can be seen that Türkiye is trying to nationalize the arms sector and to get rid of foreign dependency in the field of cyber security.

The subject of the study started from the dates when military digitalization began to be decisive in international relations. This was determined especially by examining the development stages of CMS and MCS (Military Communication Systems), and it was seen that military digitalization and nationalization studies for Türkiye gained weight at the beginning of the 2000s. Therefore, the period from the beginning of the 2000s to 2022 is taken as a basis.

There is a balance of power in the national production of CMS and MCS and their sales to other countries. However, the issue of which countries' military product sales and technology support should be is another subject that needs academic study. The number of analyses on trade in digital military equipment should be increased.

After this introduction, the article is structured as follows. In the first part, the conceptual framework is explained. This is followed by the methodology of the study. Then, the importance of cyber warfare in terms of national power is examined. In the fourth chapter, CMSs are explained within the scope of technological developments in Türkiye. In the fifth chapter, the connection between the Turkish MCS and NATO is discussed, and in the sixth chapter, the risks of cyber warfare of these two divisions are discussed. In the conclusion part, the obtained findings are discussed.

In this study, while it is emphasized that Türkiye is moving towards nationalization in the field of military digitalization, it is to be explained that this situation is a defensive approach. Because nationalization in the military field alone is not evidence of an aggressive power rise. In addition, Türkiye is not one of the countries that stand out with its high military expenditures. It is a country that attaches importance to cooperation but accepts the necessity of nationalization in the field of defense due to national security concerns, and the characteristics of the digitalized age.

The methodology and empirical basis of the study are based on scientific articles, domestic and foreign open-source data, and interviews with institutions and organizations. For the study, Turkish-origin companies such as HAVELSAN and ASELSAN, as well as NATO, Turkish General Staff, and the Ministry of National Defense were contacted via e-mail, but negative responses were received from all units due to the violation of confidentiality. In particular, during the meeting with the Ministry of National Defense, it was emphasized that questions could not be answered due to national security. This shows that CMS and MCS are a special area. Due to this data privacy of the study area, the open sources of technology companies in the defense industry were followed, the publications of official institutions were scanned, the sales indexes of defense companies were examined, and the data of international institutes such as SIPRI were used. Türkiye’s military digitalization phases have been examined and analyzed.

Giriş

Uluslararası sistemde devletlerarası hiyerarşi yoktur. Diğer yandan ise hiyerarşi anarşik yapının sonucunda ortaya çıkan güç mücadelesinin temelindedir (Jervis, 1997, s. 108). Devletlerin uluslararası güç odaklı yürüttükleri eylemlerinde ikilemler ortaya çıkmaktadır. Bu ikilemlerde savunma ve saldırı eylemlerindeki tercihlerin uluslararası ilişkileri şekillendiren konular olduğu görülebilir (Snyder,1993, ss. 63, 217). Bir devletin silahlanması ve buna yönelik diğer aktörün niyet okumadaki inancı veya yorumlaması üzerinden bir güvenlik ikilemi sonucu doğabilmektedir. Ancak siber savaşta bu ikilem durumu siber güvenlik ortamındaki güvenlik eşiğinin net ol(a)maması veya güvenlik alanının keskin hatlarla ayrılamamasından dolayı net bir silahlanma durumunu doğuramamaktadır. Bundandır ki dijital güvenlikte net olan tek seçenek savunmaya yönelik önceliktir.

Realist açıdan bakıldığında devletler güç rekabeti üzerinden hareket eder. Bu konudaki araçlar giderek çeşitlenmektedir. Her devlet özünde güç artırımı ve bunun korunmasında şartları zorlayan eğilimde olacaktır (Waltz, 1979, s. 127). İş birliği veya uzlaşı durumları uluslararası düzenin işlevsel olabilmesi ve küresel sorunların çözümü için özellikle büyük güçlerin öncülüğünde teşvik edilen gerekli durumlardır.

Teknolojik gelişmeler riskleri ile birlikte hayatımıza girdiğinde bunun güvenlik boyutunun sağlanması karmaşık ve zor bir hâl almıştır. Devletler dijitalleşmenin avantajından yararlanırken bunun riskleri ile yüzleşmek zorunda kalmışlardır. Özellikle siber alanların hayatımıza girmesiyle, uluslararası ilişkilerde güvenlik anlamında avantajlardan çok endişenin daha ağır bastığı görülmektedir.

Maddi güç kapasiteleri açısından bir devletin teknoloji alanında kendini geliştirememiş olması açık veya gizli klasik tüm tehditleri bertaraf etse dahi onu yine de zayıf kılabilecektir. Dijital alan o denli dünyanın tüm alanına sindirilmektedir ki artık devletlerin güç tanımlarında teknolojik yeterlilik bir kıstas olmuştur. 'Siber' kavramının önemi de yeni bir savaş ve güvenlik alanını tanımlamasından dolayıdır. Güvenlik meselesi devletleri, devlet dışı aktörleri ve hatta bireyleri ilgilendirmektedir. Ancak güvenlik sorumluluğu devlettedir. Siber savaş ve siber güvenlik gibi artık ulusal güvenliğin bir parçası olan uluslararası konular devletleri tekil savunma odaklı tedbirlere zorlamaktadır. Siber savaş alanına karşı devletlerin güvenlik konumlarını korumaya daha eğilimli olduğu görülmektedir.

Siber saldırılardaki belirsizlikler, iki kutupluluğun politik bölünmesine nazaran çok kutuplu yapıda daha istikrarsız bir ortamı doğurmaktadır (Waltz, 2000, s. 6). Çok kutuplu yapıda potansiyel güç yükselişlerinin karmaşık bir ortamı doğurması bu konuda devletleri aşırı saldırgan güç odaklı bir davranış biçiminden ziyade daha savunmacı ve kendi başının çaresine bakabilir bir güçte olmaya odaklamaktadır.

Uluslararası ilişkilerdeki silah türü değişiklikleri bu kutup değişikliği kadar uluslararası ilişkileri etkileyen büyük değişikliklerdir (Waltz, 2000, s. 6). Siber silahlar bu yeni değişikliğin örneklerindendir. Bu yüzden koalisyonlar ve bunlara verilen teminatlar değişken olabilir. Devletler hem tekil bağlamda bir güce erişerek iç dengelerini sağlamaya hem de diğer devletlerle çıkarları elverdiği sürece güç dengesi oluşturarak bu dengeyi korumaya yöneleceklerdir (Waltz, 1979, ss. 102-105). Bu denge güvene dayalı olmayan, savaş korkusunun getirdiği bir iş birliğini getirmektedir (Waltz, 2001, ss. 201). Burada kısa vadeli ve sığ olan bir iş birliği vardır (Keohane ve Martin, 2003, s. 77). Güvene dayalı olmaması rekabetin ve teyakkuzda olmanın varlığını göstermektedir. Diğer yandan bu da kendi kendine savunabilme kapasitesini gerektirmektedir.

Dolayısıyla devletler askerî sistemlerinin siber güvenliklerini sağlayabilmek adına garanti koşullarını oluşturmak için kendi başlarının çaresine bakma durumuna daha meyillidirler. Siber savaş riskleri ulusal güvenliği tehdit ettikçe devletler askerî dijitalleşme konusunda daha da savunmacı olacaklardır. Bu bakımından askerî alandaki siber savaşın savunmacı bir realist anlayışa yönelik tanımlanabileceği söylenebilir. Askerî dijitalleşme konusunda diğer devletlerin teknolojilerine muhtaç olmak uzun vadeli bir siber güvenlik garantisi getirmeyecektir.

Bu makale, savunmacı realist yaklaşımın askerî alandaki siber korumacılığını Türkiye üzerinden örneklendirmekte ve incelemektedir. Çalışmanın hipotezi siber güvenliğin ulusal güvenlikteki payı büyüdükçe devletlerin askerî dijitalleşme konusunda kendi başının çaresine bakma eğiliminin arttığıdır. Bunun için Türkiye millîleşmeye yönelerek savunmacı bir realist yaklaşım sergilemektedir. Türkiye'nin teknolojik yatırımlara ağırlık vermesi ve ithalatı düşürme yönelimi bakımından savunmacı yöne ağırlık verdiği söylenebilir. Bu gelişmeler ışığında, Türkiye'nin silah sektöründe millîleşmeye ve siber güvenlik alanında dış bağımlılıktan kurtulmaya çalıştığı görülebilir.

Çalışma konusu askerî dijitalleşmenin uluslararası ilişkilerde belirleyici olmaya başladığı tarihlerden başlatılmıştır. Bu da özellikle SYS gelişim evreleri irdelenerek tespit edilmiştir. 2000'li yılların başıyla birlikte Türkiye için askerî dijitalleşme ve millîleşme çalışmalarının ağırlık kazandığı görülmektedir. Zaman aralığı olarak da özellikle 2000'li yılların başından 2022'ye bir sınır çizilmiştir.

SYS'nin millî üretimi ve bunların diğer ülkelere satışı konusunda güç dengesi oluşmaktadır. Ancak, askerî ürün satışı ve teknoloji desteğinin hangi ülkeler arasında olması gerektiği akademik çalışma yapılması gereken başka bir konudur. Dijital askerî teçhizatların ticareti konusundaki analizlerin sayısı arttırılmalıdır.

Bu giriş kısmından sonra makale şu şekilde yapılandırılmıştır. İlk bölümde kavramsal çerçeve açıklanmaktadır. Bunu çalışmanın metodolojisi izlemektedir. Daha sonra ulusal güç bakımından siber savaşın önemi incelenmektedir. Dördüncü bölümde Türkiye'deki teknolojik gelişmeler kapsamında SYS'ler anlatılmaktadır. Beşinci bölümde siber savaş riskleri ele alınmıştır. Sonuç bölümünde ise elde edilen bulgular tartışılmıştır.

Kavramsal Çerçeve

Bu çalışmada Türkiye'nin askerî dijitalleşme alanında millîleşmeye doğru gittiği vurgulanırken bu durumun savunmacı bir yaklaşım olduğu anlatılmaya çalışılmaktadır. Çünkü askerî alanda millîleşme tek başına saldırgan bir güç yükselişinin kanıtı değildir. Ayrıca Türkiye askerî harcamalarının yüksekliği ile öne çıkan ülkelerden değildir. İş birliğine önem veren ancak ulusal güvenlik endişeleri itibari ile savunma alanında millîleşmesi gerekliliğini dijitalleşmiş çağın özellikleri itibariyle kabul eden bir ülkedir. Bu açıdan kavramsal olarak savunmacı eğilimi öne çıkmaktadır. Dijital askerî araç gereçler bakımından millîleşme/yerlileşme projelerine öncelik vermesi bunu ulusal güvenliğin bir parçası olarak görmesindendir. Realizmin savunduğu yaklaşımlardan olan rekabetçi yapı, güç dengesi ve kendi başının çaresine bakabilen bir ülke anlayışı Türkiye için askerî dijitalleşme alanında geçerlidir. Bu yaklaşım silah ithalatında azalma, ihracatında ise özellikle dijitalleşmiş askerî silah bakımından artış sürecinde olmasıyla tutarlıdır. Bu yüzden çalışmada, savunmacı realist yaklaşımın Türkiye'nin askerî dijitalleşme ve siber güvenlik endişeleri bakımından tutarlı bir kavramsal çerçeve olduğu anlatılmaya çalışılmaktadır.

Siber güvenlik açısından orta büyüklükteki devletlerin millîleşme ve yerlileşme (indigenization) çabalarının arttığı gözlenmektedir. Bu, uluslararası ilişkiler seviyesinde

devletlerin dijital güvenlik endişesine kapılmalarının bir sonucudur. Anarşik doğanın vurgusu öne çıktığından dolayı yapısalcı realist yaklaşım kavramsal olarak dayanağımızdır. Yapısalcı realizmin kendi başının çaresine bakma/güç dengesi/denge gibi yaklaşımları çalışmaya uygunluk bakımından tutarlıdır.

Neorealistler ile klasik realistler güç dengesi anlayışını savaştan kaçınma nedeni olarak savunmaları bakımından benzerlik göstermektedir. Ancak bilindiği gibi yapısal bir açıdan incelenen neorealizmin güç dengesini yorumlaması uluslararası sistem seviyesindedir (Waltz,1979, s. 39). Bu şekilde klasik realistlerden ayrılır (Jeffrey, 2000, s. 131). Uluslararası sistemde belirleyici unsurlar vardır. Bunlar; sistemi düzenleyici prensipler, devlet karakterleri ve devletlerin kabiliyet dağılımlarıdır. Devlet karakterleri aynıdır ancak kabiliyet dağılımları her devlette farklıdır. (Waltz, 1979, s. 97). Bu kabiliyetler devletlerin yetenekleri ile belirli seviyelerde güçler olmasını sağlayacak ve uluslararası sistemi şekillendirecek bir özelliktir. Bahsi geçen kabiliyetlerin benzer seviyelerde oluşması ve dengelenmesi ile savaş risklerinin azaltılması savunulmaktadır.

Neorealistler kendi arasında saldırgan ve savunmacı realistler olarak ikiye ayrılır. Bunlar bir devletin güç evrelerine göre izleyebileceği farklı yaklaşımlar olabilirler (Copeland, 2012, s. 49-73). Savunmacı realist yaklaşıma göre güç dengesi anlayışının özünde olan göreli güç eşitliğinde saldırı maliyeti artacaktır. Saldırıdan kaçınılmaya çalışılacaktır. Bu, benzer güce sahip devletlerin birbirine saldırma olasılığını azaltan bir anlayıştır. Rasyonel devletler düşman devlet konusunda karar alırsa güvenliği artırmaya yönelik seçimler yapabilir. Ancak bu, saldırganlar gibi her devleti potansiyel düşman olarak isimlendirmek ve en üst düzeyde bir güvenlik alanı oluşturmak anlamına gelmemektedir.

Mevcut durumdaki diğer aktörün davranışını en kötü senaryoya uyarlamak ve buna tepki için hazırlanmak saldırgan realistlerin savunduğu maliyetli, yorucu ve yayılmacı bir yaklaşımdır (Copeland, 2012, s. 59). Diğerlerini potansiyel düşman olarak görmek yerine seçilen aktörlerin düşman olup olmadığı konusunda seçim yapmak daha rasyoneldir. Saldırgan realizm biraz daha hegemonik güç yükselişine odaklanırken savunmacı realizm güvenlik bakımından sürekli hazırlıklı bir hâlde olabilmeye odaklanmıştır. Buna göre devletler kendi güvenliklilerini sağlamak için kendi kendilerine yeterli olmalıdır.

Uluslararası ilişkilerde şiddetin kullanımı olasıdır. Buna hazırlıklı olmak için devletler teknolojilerini güncel tutmalıdır. Bu teknolojiler devletlerin millî üretimleri ve yerli sistemleri olmalıdır. İş birlikleri, uluslararası anlaşmalar ve kurumlar önemli olmakla birlikte eylemler konusunda sınırlıdır. Bu oluşumlar devletlerin çıkarlarını koruduğu sürece sürdürülebilir ve katılım gerçekleşir. Örneğin Five Eye istihbarat anlaşması üye devletlere diğer devletlerin erişemediği kazanımlar ve çıkarlar sağladığı müddetçe değerli bir uluslararası örgüttür. Bir diğer örnekte, Türkiye son yıllarda BM daimî üyelerini hedef alacak şekilde "dünya beşten büyüktür" söylemleri ile çok kutupluluğu savunmaktadır. BM örgütünün daimî üyelerinin karar alıcı gücünü eleştirmektedir. Eğer Türkiye bu daimî üyelerden biri olsaydı bu söylemlerde bulunmayabilirdi. Bu da çıkarı gereği uluslararası iş birliklerine devletlerin katılımı olduğunu göstermektedir. Bu çalışmadaki savaş teknolojilerinde millîleşme yönelimi savunmacı realizmin bu savları ile tutarlıdır.

Neoliberal anlayışın savunduğu karşılıklı bağımlılık yaklaşımının bu çalışmada ele alınan askerî birimlerin siber güvenliği konusundaki eylemlerini izah etmede yetersiz kalacağı görülmektedir. Çünkü çok kutuplu yapıdaki risklere dijitalleşme de eklenince bu devletleri kendi başının çaresine bakma anlayışı için zorlamaktadır. Devletlerin savunma sanayii bakımından bütçelerini millîleşme çalışmalarına yöneltmeye çalıştıkları görülmektedir. Askerî birimlerin siber güvenliği konusundaki yazılımların ticaretinin yapılması güvenlik riskini

doğurur, bu nedenle neoliberal anlayışın karşılıklı bağımlılığın avantaj olduğu konusundaki görüşü bu noktada geçerli değildir. Türkiye askerî birimlerin dijitalleşmesinde iç dengesini sağladıktan sonra güç dengesine odaklanmıştır. Bu da küresel bir denge için kendi askerî dijital millîleşmesini sağladıktan sonra bu gücü kendi gücünü aşmayacak oranda müttefiklerine sağlama (ihraç) yoluna gitmesinde görülmektedir.

Türkiye'nin, savunmacı realist bakış açısının içerisinde olan diğer devletlerin gücünü aşmayacak oranda kendi gücünü artırarak güç dengesi, bir diğer deyişle sistemik denge kurabilmeyi askerî konularla ilgili siber alanda gerçekleştirdiği söylenebilir. SYS'ler ile dış bağımlılıktan kurtulmak için yerli yazılımlara yönelmek, bu askerî dijital tasarımları saldırıdan ziyade savunma ve güvenlik odaklı kullanmak, iş birliği ile siber güvenliklerini sağlama yoluna gitmek yerine öncelikli olarak tekil tedbirler almak, tasarlanan bu yazılımları NATO askerî iletişim ağına alternatif olacak şekilde denge kurarak müttefik ülkelere sunabilen kaynak ülke konuma gelmek Türkiye'nin askerî alandaki siber güvenliğini savunmacı bir odakla sağladığını gösterebilir. NATO üyeliği güç dengesi için gerekli, NATO dışı hazırlık ise kendi başının çaresine bakabilen güçlü bir profil için zorunludur.

Metodoloji

Çalışmanın metodolojisi; bilimsel makaleler, yerli ve yabancı açık kaynak verileri ile kurum ve kuruluşlar ile yapılan görüşmelere dayanmaktadır. Çalışma için, HAVELSAN ve ASELSAN gibi Türk menşeili şirketlerin yanı sıra, NATO ve Türkiye Cumhuriyeti Genelkurmay Başkanlığı ve Millî Savunma Bakanlığı ile elektronik posta yoluyla iletişime geçilmiş, fakat tüm birimlerden soruların gizlilik ihlali nedeniyle olumsuz yanıt alınmıştır. Özellikle Millî Savunma Bakanlığıyla yapılan görüşmede ulusal güvenlik nedeniyle sorulara yanıt verilemeyeceği vurgulanmıştır. Bu da SYS konulu verilerin gizli bir alan olduğunu göstermektedir. Çalışma alanının bu veri gizliliği nedeniyle teknoloji şirketlerinin savunma sanayindeki açık kaynakları takip edilerek resmî kurumların yayınları taranmış, savunma şirketlerinin satış indeksleri incelenmiş, SIPRI gibi uluslararası enstitülerin verilerinden yararlanılmıştır. Türkiye'nin askerî dijitalleşme evreleri incelenerek analiz edilmiştir.

Ulusal Güç Bakımından Siber Güvenlik

Siber savaş; siber saldırı ve buna karşı savunma odaklı güvenlik durumunun gerektiği bir çatışma hâli olmaktadır. Siber saldırı ışık hızıyla olabilen ve dijital araçların bir saldırı gücü olarak kullanıldığı, coğrafi sınırların öneminin olmadığı, aynı anda birden fazla yerde etki edebilen dijital ortam saldırılarıdır. Bilgisayar tabanlı bir cihazın sisteminin verilerine yönelik yapılmaktadır (Hunker, 2010, ss. 13). Fiziksel hasar doğrudan olmamaktadır. Sistemlere hasar verilebilmektedir. Ancak bu sistemsel hatalar fiziksel hasarlara ve hatta örneğin bir sağlık kurumunun dijital sistemine yapılan saldırıda olabileceği gibi de ölümlere neden olabilir.

Siber tehditler bilgisayar sistemlerine verilen zararlar olarak tanımlanır. Bu bilgisayar sistemleri, devletlerin hayati organlarının entegre edildiği bir dijital dönüşüm sağlamaktadır. Bu açıdan bu sistemler devletlerin asimetrik bir savaş içerisinde zayıflatılmaya çalışıldığı bir saldırı alanı hâline gelmiştir. Saldırı kapasitesinde bir yatırımdan ziyade ilk aşamada etkin bir savunma alt yapısı hazırlanmak zorunludur. Bu savaş ortamında bilinmeyen düşman unsur ve saldırı tipinin belirsizliği gibi sorunlarla karşılaşılabilir.

Savaş alanları sırasıyla kara, deniz, hava ve uzay olarak kendini göstermiştir (Gray, 2013, ss. 9-15). Artık 21. yüzyıl ile birlikte siber uzay alanı da beşinci savaş alanı olarak belirlenmektedir (Warsaw Summit Communiqué, 2022). Siber savaş uygulama alanı bakımından stratejik ve operasyonel olarak iki alana ayrılmaktadır. Stratejik siber savaş; devletlerin veya devletle bağlantılı bir grubun başka bir devletin kurumlarına veya toplumuna yönelik saldırılardır. Operasyonel siber savaş ise savaş ortamında devletlerin askerî olan ve

askerî bağlantılı olan birimlerine yönelik yapılan saldırılardır (Libicki, 2009). Bu çalışmada siber saldırılar ikinci alanda bir savaş kuvveti olarak görülmektedir. Bu açıdan siber savaşın askerî odaklı yapılması geleneksel savaşın bir modern uzantısı gibi düşünülebilir.

Bir savaş alanı olarak kabullenilmesinden dolayı siber uzayın güvenliği devletler için ulusal güvenliklerinin bir uzantısı olarak görülmektedir. Bu anlayışta kara, deniz, hava ve uzay güvenliğini ulusal güvenlikleri açısından sağlamak isteyen devletler özellikle karmaşık bir tehdit ortamında siber uzayın da güvenliğini ulusal güvenlikleri için almak zorundadırlar. Örneğin Türkiye, ulusal güvenliği ile bağlantılı olarak gördüğü siber güvenlik için üç ayrı eylem planı yayınlamıştır (Türkiye Cumhuriyeti Ulaştırma ve Altyapı Bakanlığı, 2023). Bunlar 2013-2014, 2016-2019 ve son olarak 2020-2023 yıllarını kapsayan üç ayrı belgedir. İlk belgede "siber zafiyetler ulusal güvenliğin ihlaline neden olabilecektir"; ikinci eylem planında "iletişim sistemlerinin güvenliğinin sağlanması ulusal güvenliğimizin önemli bir boyutudur"; son eylem planı belgesinde ise "siber tehditler milli güvenliğimizin önemli bir parçasıdır" sözleri ulusal güvenlik ile siber tehditlerin bütünleştirildiğini ve ilke olarak benimsendiğini göstermektedir (Türkiye Cumhuriyeti Ulaştırma ve Altyapı Bakanlığı, 2023).

Ulusal güvenlik, siber tehditte görüleceği üzere bir tehdide karşı o tehditten uzaklaşılmasını sağlayacak güç oluşturulmasıdır (Birdişli, 2011, ss. 149-169). Bu bakımdan güç biçimleri güvenliğin sağlayıcılarıdır. İnsan gücü, coğrafi güç, askerî güç, ekonomik güç, politik güç, sosyal güç, bilimsel ve teknolojik güç olarak yedi güç unsuru tanımlanırken siber güç sekizinci ulusal güç unsuru olarak görülebilir (Şenol, 2018, s. 201). Siber güç ile ilgili güvenlik teorisi çalışmaları yapan araştırmalar da siber gücü 'belirsiz' olan bir güç türü olarak yorumlamaktadır (Gray, 2013, s. 14). Bu güç siber uzayın fiziksel ve sanal alanlarında devletlere zarar verebilmektedir (Şenol, 2018, s. 193). Siber güç unsuru ile özellikle devletlerin fiziksel varlıkları olan askerî sistemlerine zarar verilebilir hem de sanal bir zarar olarak askerî veriler üzerinden bir saldırı yapılabilir.

Ulusal güvenliği tehdit edici saldırılara karşılık tepkiler bakımından meşru müdafaa yöntemleri siber savaşta ayrışmaktadır. Siber saldırının karşı taarruzu başka zaman, mekân ve yöntemle olabilir. Bu daha hazırlıksız etki edebilecek bir yöntemdir. Aksi halde saldırı yapan siber eylemci aynı saldırı yöntemine karşı kendi savunmasını çoktan almıştır. Bu da nükleer savaş dönemini günümüz dijital döneminden ayırmaktadır.

Siber savaşta caydırıcılık durumu aynı eşit tepki bakımından uygun olmayabilir. Verilerin çalınması durumunda bu eylemi yapan devlet, devlet destekli gruba veya örgüte aynı şiddette karşılık vermek olanaksız olabileceğinden saldırı sonrası cezalandırma algısı zorlaşabilir. Örneğin, böylesi bir casusluk yoluyla elde edilecek işlevsel bir bilgi saldırıyı yapan karşı tarafta benzer şekilde olmayabilir. Kaldı ki casusluk eyleminin yapılmasında eylemi yapanın kimliğinin tespit edilememesi de söz konusudur. Bu gibi bir durumda casusluk eylemini başarıyla ilk yapabilen bu ilk vuruşu geri bir saldırı olasılığını ortadan kaldıracak şekilde yapmaktadır.

Ülkelerin siber savaştaki hazırlıklı olma eğilimleri giderek artmaktadır. Bu konuda 2017'de yapılan bir araştırmaya göre ülkelerin siber saldırıya hazırlıklı olma kapasiteleri ele alınmıştır. Bu kapsamda 193 ülkeye davet gönderilmiş, 134 ülke araştırmaya katılmıştır. Buna göre siber saldırıda hazırlıklı olma konusunda Singapur ilk sırada, ABD 2. sırada, Rusya 11. sırada, Türkiye ise 43. sırada yer almıştır (Global Cybersecurity Index, 2017). Araştırmada, Gürcistan'ın siber saldırıda savunma bakımından üst sıralarda olduğu tespit edilmiştir. Bu durum 2008'de yaşadığı saldırılardan sonra askerî verilerin korunması için özel bir birim kurması ile sağladığı hususi tedbire bağlanabilir (Global Cybersecurity Index, 2017). Diğer yandan Gürcistan'ın örneğin SYS'lerinde ABD girişimleri vardır (General Atomics Aeronautical Systems, 2023). JADC2 adlı Amerikan tasarımı SYS Gürcistan askerî

komutasında kullanılacaktır (The US Congressional Research Service, 2022). Rusya'dan gelecek siber saldırılara karşı ABD merkezli bir savunma geliştirildiği söylenebilir. Hatta siber suçlar bakımından da Avrupa'ya bağlılık vardır. AB, Budapeşte Siber Suçlar Anlaşmasına uygun olarak siber suç mevzuatı oluşturmuştur (Convention on Cybercrime Budapest, 23.XI.2001; General Policy And Legislation On Cybercrime). Bu açıdan bu listedeki veriler millî savunma tedbirlerine dayalı olarak düşünülmemelidir. Bu gibi dış destekli bir savunma mekanizmasıyla güçlendirme sağlanabilir ancak bu mekanizmanın tam güvenilirliği de ulusal güvenlik açısından tartışmalı olmaktadır.

Ülkelerin siber savaştaki hazırlıklı olma kapasiteleri onları siber güç olmaya zorlamaktadır. 2020 yılında Harvard Üniversitesi Belfer Center tarafından yapılan bir başka araştırmaya göre siber güç sıralamasının yedi unsuru bulunmaktadır: 1) Yerel grupların gözlemlenmesi; 2) Ulusal siber savunmaların geliştirilmesi; 3) Yabancı istihbarat toplanması; 4) Siber alan üzerinden millî gelir elde edilmesi; 5) Bilgi ortamının yönetilmesi; 6) Düşmanın altyapılarının ve sistemlerinin devre dışı bırakılması; 7) Siber normların ve standartların tanımlanması.

Belfer Center'ın bu araştırmasına göre siber güç bakımından bir dünya sıralaması çıkartılmıştır. Sırasıyla ABD, Çin, İngiltere'nin ilk üçte yer aldığı listede örneğin Türkiye 22. sıradadır. Bu oranlarda görüldüğü üzere Türkiye ilk 10 arasında dahi değildir. Ancak Türkiye'nin bahsi geçen yedi kriter arasında özellikle siber bilgi yönetiminde ve siber alan konusunda millî gelir elde etme bakımında başarılı olduğu görülmüştür (Voo vd., 2020). Savunma sanayi konusunda millî teçhizatların dış pazar alanına yayılmasındaki eğilim de bu yönde tutarlıdır. Bu da uluslararası sistemde güç dengesi için önemlidir.

Askerî platformların giderek artan bir şekilde bilgisayar ağ bağlantılı olması ulusal güvenliği ve gücü etkilemektedir. Bu konudaki saldırı riski de artmaktadır. Örneğin 2015'ten beri ABD Savunma Bakanlığı'na yönelik 12 binden fazla siber saldırı yapılmıştır (the U.S. Government Accountability Office, 2022). NATO'nun bu konudaki hazırlığı da giderek yoğunlaşmıştır. NATO Askerî Sistemler İçin Siber Güvenlik Risk Değerlendirme Süreci başlıklı raporunda bunu vurgulamıştır. Tekrarlanan risk değerlendirmeleri askerî sistemler için giderek önemli olmuştur (NATO, 2021). Çünkü siber güvenlik, sürekliliği gerektiren bir alandır. Askerî sistemlere yönelik siber saldırılar yaygın kullanılan araçlar olmasalar da kritik olmalarından dolayı siber saldırıda tercih edilen alanlardır.

Savaş Yönetim Sistemleri ve Türkiye

Savaş Yönetim Sistemi, savaş alanında hava-kara, hava-deniz, deniz-deniz veya kara-deniz gibi farklı savaş konumları arasında muharebe bilgilerini paylaşmak için oluşturulan sistemlerin genel adıdır. Merkezi koordinasyon ve bilgi akışı bu alanlarda savaş esnasında veya güvenliğin riskli olduğu durumlarda hayati önem taşımaktadır. SYS askerî birliklerin komutası ve senkronizasyonudur. Donanmalar üzerinde komuta kontrolü olarak kullanılırken kara alanları ile de irtibat sağlanır. Hava-kara komutası için de tasarlanabilir. Teknoloji geliştikçe savaş gemilerinin harp kabiliyeti de artmış ve artan bu kapasite ile denizde savaş giderek daha karmaşık hale gelmiştir. Bunun için komuta edebilme ve anında müdahale, siber savaşın da yeni bir savaş alanı olarak kabul edildiği mevcut uluslararası işleyişte önemli bir savunma konusu hâline gelmiştir.

SYS, herhangi bir zamanda bir saha komutanı tarafından ihtiyaç duyulan tüm önemli verileri etkin bir şekilde görüntüleyerek tam durumsal farkındalık sağlar. Savaş ortamında, olayları yönetme ve kontrol etme yeteneği geliştikçe görev başarısı artmaktadır. Ayrıca hızlı hareket eden operasyonların başarılı bir şekilde yürütülmesi, hızlandırılmış bir karar verme sürecini gerektirmektedir. Önemli olan ise artık teknolojik gelişmelerin de katkısıyla

operasyonları aynı anda yürütme becerisidir. Başarı, etkili komuta ve kontrolle sağlanabilecektir.

SYS'nin bilgisayar entegre çalışmaları aslında dünya geneline bakıldığında çok önceleri başlamıştır. 1987 yılında ABD ordusu için hazırlanan bir araştırma enstitüsü raporu, yapay zekâdan faydalanarak otomatik kontrol ve komut konusunda SYS'ye çalışmıştır. Bu rapora göre SYS, savaş alanı bilgilerinin alınması, işlenmesi, depolanması ve iletilmesi için entegre bir teknolojiler kompleksidir. Taburdan daha alt seviyedeki zırhlı birliklerin komuta, kontrol ve iletişimini kısmen otomatikleştirmesi beklenmektedir. Raporda araçlar arası aktarılabilen bilgi sistemi oluşturup bunu orta vadeli yükseltmek ve yapay zekâ ile geliştirmek istenmiştir (Johnson ve Henderson, 1987). İleriki yıllarda bu gerçekleşmiş ve dijital ağ tabanlı SYS ortaya çıkmıştır.

Savaş teknolojilerinin gelişmesiyle birlikte artan ihtiyaçların karşılanması için komuta kontrol koordinasyonunda destek sağlamak ve komuta kadrosunu desteklemek gerekmektedir. Türkiye'de bu ihtiyaca yönelik ilk modern girişim 1970'lerde başlamıştır. Bu yurt dışından tedarik edilen TCG Doğan hücumbotuna entegre edilen STACOS SEWACO sistemidir (Defence Turkey Magazine, 2019, ss. 68-71). Daha sonra Barbaros sınıfı firkateynlerle birlikte TACTICOS SYS tanıtılmıştır (Thalesgruoup, 2018).

Askerî birimler bu tür SYS iletişiminde sivil internet araçlarını kullanmamaktadır. Ağ destekli savaş alanında NATO temelli hareket eden Türkiye, entegre muharebe sistemi olan TAFICS projesi ile "TSK-Ağı" adlı ağı kullanmaktadır. TAFICS alt yapısı olmayan alanlarda ise taktik saha muharebe sistemi olan TASMUS'u ve bir İsveç şirketi olan THALES savunma sanayi ürünü olan TACTICOS'u da kullanmaktadır (Thalesgruoup, 2023).

1990'lı yıllarda Türk Deniz Araştırma Merkezi Komutanlığı tarafından Tepe Sınıfı Firkateynler için K-5 Komuta Kontrol Sistemi geliştirilmiştir (Defence Turkey Magazine, 2019, ss. 68-71). Yurt dışından sağlanan diğer sistemlere ek olarak bu sistem de Türk Deniz Kuvvetleri'nin kullanımına sunulmuştur. Ancak bu teknik komuta iletişimi konusunda güvenlik ve güç bakımından dışa bağımlılık anlamına gelmekte ve millî bir sistem ihtiyacı devam etmektedir.

Bu gelişmeler dijital ağ tabanlı sistemlerin gelişmesiyle ve de siber güvenlik kavramının daha önemli olması ile eş zamanlı ilerlemiştir. Çünkü 2000'li yılların başı dijital gelişmelerin uluslararası ilişkileri tam anlamıyla etkilemeye başladığı yıllardır. Siber saldırı ve siber savaş kavramları yine bu tarihlerde gündem olmaya başlamıştır. Nitekim 2003'te ABD'nin ilk siber uzay tanımı, Siber Uzay Güvenliği Stratejilerinde (Cyberspace Security Strategy) belirtilmiştir (the US National Strategy to Secure Cyberspace, 2003). Artık dijital dönüşüm odaklı modern bir askerî yapılanma hedeflenirken siber savaşta güçlü bir millî savunma gerekli hâle gelmiştir. Böylelikle 2000'lere doğru Türkiye'nin millî SYS üretme çalışmaları başlamıştır. Örneğin 2005'te, Türk Deniz Araştırma Merkezi Komutanlığı ve Havelsan iş birliğinde millî sistem GENESİS SYS ortaya çıkmıştır (Türk Deniz Kuvvetleri Komutanlığı, 2023).

SYS'lerin dış kaynaklı teminine karşılık bu sistemlerde ve haberleşme ağ yapılarında yerlileşme ihtiyacının giderilmesine odaklanılmış. Bunun için de 2010 yılında Havelsan ve Türk Deniz Araştırma Merkezi Komutanlığı iş birliğinde tamamen millî ve yerli ADVENT deniz SYS geliştirilmiştir (Havelsan, 2023). Deniz ve hava ağ bağlantılı savaş sistemi olarak artık millî ve yerli ADVENT SYS kullanılmaktadır (Şenol ve Karaçuha, 2020, s. 58-60). Böylelikle Anadolu'nun ortasındaki bir komuta merkezinden Doğu Karadeniz'de bulunan donanma veya denizaltı ile Akdeniz'in batısı veya doğusunda bulunan diğer tüm kuvvetlere kadar tüm deniz gücü tek merkezden komuta edilebilir. Hangi mevkiden nereye yönelik bir eylem yapılacağı senkronize şekilde belirlenebilir.

Bu çalışmalar devam ederken ileri bir aşamada bunların diğer ülkelere de sağlanabilmesiyle teknolojik rekabette bir kıstas olması istenmektedir. Böylelikle ADVENT'in tüm hava, su üstü, sualtı ve kara platformlarında kullanılması ve bu karışık platformlarda kullanılmak üzere ihraç edilmesi amaçlanmıştır. Bu sistemler verilen izinler ile yurt dışında üretilebilecektir. Örneğin Havelsan'ın ADVENT SYS'sini Pakistan kendi gemilerinde kullanacaktır. Böylelikle, Havelsan Pakistan'ın savaş gemilerindeki veri dağılımını sağlayan sistemin sağlayıcısı olacaktır (Havelsan Dergi, 2021, s.8). Ayrıca Havelsan Pakistan AGOSTA 90B Sınıfı Denizaltıların Projesinde, STM firmasının ana yükleniciliğinde ilgili denizaltının savaş sistemi sorumluluğunu üstlenmiştir (Havelsan Dergi, 2022, s.77). Pakistan'ın ardından Ukrayna'ya da ihraç edilen ADVENT, son olarak Endonezya resmî havacılık ve uzay şirketi ile yapılan anlaşma neticesinde Endonezya'ya da sunulacaktır (Havelsan Dergi, 2021, ss. 16, 28; Rahmat, 2021).

Dünyaca ünlü SYS tasarımı yapan şirketler sıralamasına Türkiye de girmeye çalışmaktadır. Thales, Lockheed Martin, Elbit Systems, BAE Systems, SAAB, Raytheon Technologies gibi büyük çaplı şirketler savunma sanayiinde dijital sistemler üreten şirketlerdir (Thales, 2023; Lockheed Martin, 2023; Elbit Systems, 2023; BAE Systems, 2023; Saab, 2023, Raytheon Missiles And Defense, 2023). Türk şirketi Havelsan Türk Deniz Kuvvetleri Komutanlığı ile iş birliğinde bu kategoride rekabet edebilecek bir yükselişe geçmiştir.

ASELSAN, STM ve TAİS gibi şirketlerin de Havelsan gibi sistem tasarım projeleri vardır. Savunma Sanayii Başkanlığı kontrolünde ASELSAN, STM ve TAİS gibi şirketlerin dâhil olduğu millî gemi projesi olan MİLGEM buna örnektir. Savaş sisteminde entegre muhabere sistemi, elektronik harp sistemi, elektro optik sistemler, seyrüsefer sistemleri, radarlar, hava savunma ve silah sistemleri, atış kontrol sistemleri, sonarlar ve torpido karşı tedbir sistemleri ile savaş sistemi entegrasyonunu gerçekleştirmektedir (Türkiye Deniz Kuvvetleri Komutanlığı, 2023; ASELSAN, 2023).

Türk savunma sanayi şirketlerinin yükselişte olduğu görülmektedir. ASELSAN'ın millî silah üretiminde artan değerine bakıldığında bu durum görülecektir. 2022 yılı itibari ile 160 üründe millîleşme gerçekleştirmiştir (SavunmaSanayiST, 2022). Dünya sırlamasında silah satışında ise ASELSAN 2012 yılında 91. sıralarda yer alırken giderek ön sıralara yükselmeye başlamıştır. 2021'de 56. sıraya gelmiş ve Türk ürünlerinin ihracatında önemli bir savunma sanayi şirketi olmuştur (The SIPRI, 2012). 2022 yılında millî silahların satışlarında da yükseliş vardır. Örneğin uzaktan komutalı silah sistemlerinden SARP millî yazılımla entegre olan 22 ülkeye ihraç edilmektedir (Tübitak Bilgem, 2021; ASELSAN, 2023, TRT, 2023).

Bahsi geçen yukarıdaki gelişmelere NATO üzerinden bakıldığında bir iletişim iş birliği zorunluluğu görülebilir. Askerî anlamda teknolojik gelişmelerin iletişim kabiliyetine yansımaya başladığı ilk yıllarda NATO, üye ülkeler için SYS'leri bir sisteme oturtmaya çalışmıştır. Bunun için NATO üyesi tüm ülkelerin ürettikleri askerî ürünlerin STANAG (Standardization Agreement) denilen bir uygunluk çemberine girmesi öngörülmüştür. Standardizasyon Anlaşması olan STANAG'a göre üye ülkeler ortak bir standarda göre silah veya askerî teçhizat üretimine gidebilmektedir (NATO Standardization Office, 2023).

Buna benzer olarak teknolojik gelişim ihtiyacı olan devletlere daha gelişmiş durumda olanlar bilgi ve tecrübe aktarımını sağlayarak NATO tek bir askerî standartta kalmaya çalışmaktadır. Böylelikle ortak standartlara erişmiş benzer ülkeler ortaya çıkmaktadır. SYS'ler de bu anlaşmaya göre olmak zorundadır. Zaten yerli üretim yapılmadığı alanlarda yurtdışı teknoloji desteği de bu standarda göre alınmaktadır. Bu durum bir iş birliğini göstermektedir. Ancak NATO üyeleri yine de millî ürünler üretmeye gitmektedir. Siber saldırı için, bu iş birliği ile sınırlı kalan bir güvenlik tedbiri ulusal güvenlikte risk demektir. Zira iş birliklerinde

uluslararası ilişkilerin doğası gereği tam bir güvenilirlikten bahsetmek pek mümkün değildir. Sadece NATO üyeliğine bağımlı bir güvenlik politikası Türkiye'nin sürdüreceği uzun vadeli politikaları ile uygun olmayacaktır. SYS'de millîleşme/yerlileşme ile askerî teknolojiler geliştirilmek istenirken bunların Türkiye üreticisi olarak NATO dışı müttefiklere sunulma amacı vardır.

Siber Güvenlikte Savaş Yönetim Sistemleri

Ulusal gücün göstergesi ilk etapta güçlü bir silahlı kuvvetlerdir (Ahmad, 2012, s. 95). Silahlı güçlerin güvenilirliği için savunma sanayinde bilim ve teknolojinin desteğine ihtiyacı vardır. Savunma sanayi alanında kendi kendine yeterlilik sağlanabilmesi ve yabancı askerî teçhizat üreticilerine bağımlılığın azaltılması gerekmektedir (Ariffin ve Arof, 2019). Dijital dönüşüme girmiş bu askerî teçhizatların ve sistemlerin güvenliği ise gerek silah pazarındaki konumu bakımından gerekse siber savaş alanındaki konumu bakımından elzem konular hâline gelmiştir.

Dijital gelişmelerin takip edilmesi millîleşme çabaları ile desteklenmeye çalışılmaktadır. Diğer yandan Türkiye'nin silah ithalatında da azalma hedeflenmiştir. Kendi kendine yetebilen bir ülke profili için silah ithalatında azalma ve güvenliğin millî ürünlerle sağlanması hedeflenmektedir. İlk olarak, Ukrayna savaşından hemen önce 2021 yılında Türkiye'nin son beş yılına bakıldığında silah ithalatında yüzde 59 düşüşe gittiği görülecektir. Bu durum dış bağımlılığın düşürülmesi bakımından önemli bir değişimdir. İkinci olarak, Türkiye silah üretiminde artışa gitmesi ile bu durumu dengelemeye çalışmaktadır. Türkiye'nin silah ihracatında artışlar da başlamıştır. 2013 ile 2022 yılı arasında Türkiye'nin silah ihracatında yüzde 69'luk bir artış olmuştur (Wezeman, Gadon ve Wezeman, 2022). Üçüncü olarak ABD'den en çok silah alan ilk 10 ülke arasında yer alan Türkiye, önceki yıllara göre ABD'den silah satın alımında son 5 yılda düşüşe gitmiş ve 27. sıralara kadar gerilemiştir (Wezeman, Gadon ve Wezeman, 2022). Bu millîleşme ve ithal silah alımında azalma politikaları ile de yorumlanmalıdır. Dördüncü olarak, diğer ülkelerin de silah satın aldıkları ülkeleri çeşitlendirme ihtiyaçları vardır. Örneğin Mali'nin artan silah ithalatında Rusya'nın payı yüksektir. Bu yüksek oranı dengelemek için başka ülkelerden de silah satın alarak çeşitlilik yaratması gerekmektedir. Türkiye, Mali ve benzeri ülkelere silah satmaya başlayan ülkelerdendir (Wezeman, Gadon ve Wezeman, 2022). Son olarak Türkiye'nin denizlerle çevrili coğrafyası gereği özellikle Yunanistan ile yaşanan gerginliklerde güvenliğini arttırması gerekmiştir. Örneğin Yunanistan Fransa'dan firkateyn siparişinde bulunurken Türkiye çoğu savaş gemisini kendi üretebilmektedir (Wezeman, Gadon ve Wezeman, 2022).

Türkiye savunma sanayiine büyük yatırımlar yapmaktadır. Ancak askerî harcamada dünya sıralamasında ilk 15 ülke arasında değildir (SIPRI, Military Expenditure, 2023). Askerî harcamaların yüksek olması tek başına bir ülkenin saldırgan mı yoksa savunmacı mı olduğunu göstermez. Silahlanma türü ve amacı da önemlidir. Burada Türkiye'nin özellikle dijitalleşmiş askerî silahlarda millîleşmeye önem verdiği görülebilir. SYS ve askerî amaçlı yazılımlar bu konuda dikkat çekmektedir.

Türkiye'de yazılım ihracatı destek sağlanması gereken hizmet satışları arasına alınmıştır. TURQUALITY adındaki proje ile Türkiye, dünyada ilk ve tek markalaşmayı destekleyen devlet destek projesini oluşturmuştur. Böylelikle Türk markalarına daha fazla rekabet olanağı sağlamak ve dünyada güçlü markalar hâline gelmelerinde destek vermek amaçlanmaktadır (Circular of Turquality Promotion Project Support, (15/11/2022) Decision No. 5973). Bu markalaşma programında Türk savunma sanayi şirketlerinde ASELSAN ve Roketsan da yer almaktadır (www.turquality.com, 2023). Yazılımın savunma sanayinde ihracatı devlet destekli bir ticaret sektörüne doğru ilerlemiştir. Bu durum yabancı yazılım

şirketlerine bağımlılığı kırmak için karşılıklı bağımlılığa değil aksine güç dengesine yönelik görülebilir.

Yazılım ticaretinin 2019 dünya piyasasındaki boyutu yaklaşık 565 milyar dolar civarındadır. Hâlihazırda dünyadaki en büyük on şirketin yedisi teknoloji firmasıdır. Bunların beşi de yazılım üzerine çalışabilen şirketlerdir (https://tusiad.org, 2021). Türkiye de bu pazardaki yerini arttırmaya çalışmaktadır. Türkiye'nin ihracatının %0,5'i yazılım sektöründen gelmektedir. Bu sektörün giderek büyüyeceği öngörüleri beraberinde yeni güvenlik ihtiyaçları, hukuksal sorunlar ve maddi boyutların tartışılmasını da getirebilir (https://tusiad.org, 2021). Böylelikle yazılım ihracatı ile bu hizmetin siber tehditlere karşı güvenli olup olmadığı ve etik ilkeler gereği satıcı tarafa bir güvenlik teslimiyeti anlamına mı geleceği soruları akıllara gelmektedir. Özellikle askerî alandaki yazılımlar bu konuda hem karmaşık hem de zor bir yeniliği ortaya çıkarmıştır.

Askerî alanda teknolojik ticaret riskli bir durumdur. Özellikle yazılım hizmeti sağlandığında kriz anında ülkeleri olası bir saldırı ile savunmasız bırakma riski vardır. Askerî iletişim; özelinde SYS, genelinde yazılım ticareti sıkı bir anlaşma ve güvenilirlik temelinde yapılmak zorundadır. Hizmeti sağlayan taraf için örneğin yazılımın çözülebilmesi, kopyalanabilmesi ve mühendislik bilgisinin açığa çıkması riski söz konusu olabilir. Diğer yandan alıcı taraf için risk ise yazılımın güvenilirliği olabilir. Kullanılan sistemin alan işlevi dışındaki ülke verilerine erişimi olup olmadığı, kriz anında kendini bloke edip etmeyeceği, bilgileri kontrol edip etmediği güvenilirlik esaslarıdır.

Satıcı taraf için ortaya çıkan riske örnek olarak tersine mühendislik gösterilebilir. Tersine mühendislik en basit ifade ile çalışır bir cihazın yazılımının işleyişinin yani çalışma sisteminin çözülebilmesidir (https://ethics.csc.ncsu.edu, 2023). Buradaki işleyiş yeni bir cihaz ortaya çıkarmanın aksine var olan cihazın nasıl işlediğini ve ne için çalıştığını öğrenmek için tersine bir çözümlemedir. Bunun için yazılım kaynağının açık kaynaklı kod olması gerekmektedir. Tersine mühendislik meslek sırlarının ve patent gerektiren ürünlerin işleyişlerinin çözülebilmesi anlamına geleceğinden tartışmalı bir durumdur. Yine de güvenilirlik için açık kodlu hizmetler yapılmaktadır. Açık kod ile işleyen cihazın işleyiş şekli ve hangi amaca hizmet ettiği açık kodlarla gösterilmektedir (Paulson, Succi ve Eberlein, 2004, ss. 246-256). Kullanıcı bu açık erişimle bilgi güvenliğinin kapsamını öğrenebilir. Android, ki günlük hayatta çoğu telefonda da kullanılan sistemdir, açık kaynaklı kod sistemlerindendir. Linux tabanlı olan Android, Google tarafından 2005 yılında satın alınmıştır. Diğer yandan genellikle rakip firmaların meslek sırlarının korunması için tersine mühendisliğe karşı korunaklı olması istenmektedir. Bunun için kapalı kaynaklı kodlar tercih edilebilir. Bu tür yazılımlar tasarımcısı hariç kimse tarafından değiştirilemez. Microsoft Windows ve MS Office bu kapalı kodlu yazılımlardandır (Canbaz ve Erdemir, 2021, ss. 30-37).

SYS'lerde dijital ağ ve yapay zekâ tabanlı gelişmeler genç bir alandır. Bu yüzden olası güvenlik açıklarının keşfedilmesinde zorluklar olabilecektir. Özellikle, bu tür sistemlerin yurt dışı tedarikli olması güvenlik riskini ve savunma kabiliyetini daha da riske sokacaktır. Dolayısıyla millî sistemlerin değeri, keşfedilmemiş saldırılara en azından hazırlanabilmek adına daha hâkim olunabilecek bir savunma mekanizması anlamına gelmektedir. Bu millîleşmeye askerî iletişim kanallarındaki yerli iletişim başarısı da eklenirse bir ülke için etkin bir siber savunma oluşturulabilecektir.

Sonuç ve Tartışma

Siber savaşta saldırı kaynağının belirlenmesi geleneksel savaşlar kadar net değildir. Bu durum devletlerin çatışmacı ortamında uluslararası iş birliğinin sorun çözücü rolünü etkileyebilir. Siber saldırıların tek başına bir saldırı aracı olarak kullanılmasından ziyade

geleneksel yöntemleri destekleyici unsurlar olarak kullanıldığında toplam tahrip gücü daha yüksek olmaya başlamıştır. Siber saldırılar devletlerce giderek daha fazla geleneksel savaşın bir parçası olarak kullanılacak ve bütünleştirilecektir. Böylelikle konvansiyonel savaşların sonuçları siber savaş ile daha fazla etkilenebilecektir. Askerî alanda siber güvenlik konusu da bu alanda internet bağlantılı cihazların sayısı arttıkça saldırı riski de artacağından önemini koruyacaktır. Ayrıca gelecekte yapay zekâ ve makine öğrenimi destekli saldırı tespiti gibi yöntemlerin kullanılma potansiyeli bu alanı giderek daha karmaşık hâle getirebilecektir.

Türkiye, dijital ağ tabanlı sistemlerin gelişmesiyle ve de siber güvenlik kavramının giderek önemli olmaya başlamasına eş zamanlı olarak askerî dijital dönüşümde millîleşme/yerlileşme çalışmalarına gitmiştir. Ayrıca siber savaş olgusuna en başından beri askerî birimlerle bağlantı kurularak yaklaşılmıştır. Çünkü siber güvenlik sürekli bir çabayı gerektirmektedir.

Uluslararası ilişkilerde siber güvenlik ve özelinde askerî dijitalleşme konusunda liberal bir kurumsallaşmaya yönelik olan karşılıklı bağımlılık yaklaşımı devletlerin ulusal güvenlik endişeleri bakımından uygulanamamakta, askerî siber güvenlik konusunda yapısalcı bir realist yaklaşım daha tutarlı olmaktadır. Bu duruma Türkiye üzerinden bakıldığında özellikle yapısalcı realizmin güç dengesi anlayışını burada görmek mümkündür. Türkiye askerî dijitalleşmede millîleşmeye giderek güçlü devletlerin peşine takılma eğiliminden kurtulmak ve askerî teknolojide kendine yeter bir ülke olarak bu alanda denge sağlayıcı aktör olmaya odaklanmıştır. Zira anarşik uluslararası sistemde aktörler birim olarak eşit olsa da kabiliyetleri onları birbirinden ayırmaktadır. Dijital kabiliyet de bir güç olarak görülmelidir. Türkiye'nin millî dijital kabiliyeti ve siber güvenliği etkili olan bir ülke olabilmesi onu uluslararası siyasi sistemde yapıya etki edecek bir aktör konumuna yükseltecektir.

Nihai olarak görülmektedir ki siber savaş kavramın hayatımıza girmesi ile doğru orantılı şekilde devletlerin SYS'de millî-yerli unsurlara yönelme eğilimleri artmıştır. Genel anlamda Türkiye'nin silah ithalatında düşüşe gitmesi ve dış bağımlılığını kesmeye çalışması, millî silah çalışmalarını arttırarak Türk silah sanayini ihraç edebilir bir konuma getirmesi savunmacı realist yaklaşım uygulamalarının göstergesidir. Silah alanında millîleşme tek başına bir saldırganlık göstergesi değildir. Zira Türkiye askerî harcamalarda en çok harcama yapan ilk 15 ülke arasında dahi değildir. Millîleşme için öncelikle silah ihraç oranında her geçen gün artışa gitmektedir. Bu da millî ve yerli üretime yatırım yapmasıyla açıklanmaktadır.

Devletlerin siber yetenekleri de artık bir güç kategorisi olduğundan uluslararası sistemde devletlerin dijital kabiliyetlerinin dağılımı uluslararası sistemin yapısını etkileyecektir. Türkiye'nin dijital güç bakımından kendine ait millî bir yazılım ve dijital ağ sistemi geliştirmesi bir güç kabiliyetidir. Bu yapısal seviyedeki değişimlere önce bölgesel daha sonra ileri bir aşamada küresel bir etki yaratabilecektir. Millî SYS, insansız hava araçları gibi Türk menşeili teçhizatları Pakistan, Ukrayna, Endonezya gibi ülkelere sağlaması ise güç bakımından yakın eşitlik oluşturulmasının büyük savaş olasılığını azaltacağındandır. Benzer güçler hem güç dengesini sağlar hem de büyük savaşlara girmekten kaçınır. Güç eşitsizliği savaşın riskini arttırır. Türkiye siber gücünü diğer ülkelerle paylaşma yoluna gitmeyip benzer güç oluşturulmasına katkı sağlamaz ve saldırgan olursa, bu durumda aynı güç kategorisinden daha büyük karşı koalisyonlarca mağlup edilme olasılığını taşıyacak ve maliyetli bir savaş riski ile yüzleşecektir.

Kaynakça

Ahmad, A. (2012). Concept of national power. *Strategic Studies*, 32 (2/3), 83-101.

Ariffin, Z., Arof, A. (2019). Challenges in developing indigenous combat management systems for Malaysian maritime defense and enforcement services, *Marine Frontier*, 10 (1).

Aselsan (2021). Milgem-5 savaş sistemi tedariki projesi, https://wwwcdn.aselsan.com/api/file/MILGEM_5-TR.pdf

Aselsan (2023). Uzaktan komutalı stabilize silah sistem: SARP. https://www.aselsan.com/tr/defence/urun/1860/sarp.

BAE Systems (2023). https://www.baesystems.com/en/home

Birdişli, F. (2011). Ulusal güvenlik kavramının tarihsel ve düşünsel temelleri, *Sosyal Bilimler Enstitüsü Dergisi,* 31/2, 149-169.

Canbaz, S. ve Erdemir, G. (2021). Açık kaynak kodlu gerçek zamanlı işletim sistemlerinin incelenmesi. *İstanbul Sabahattin Zaim Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, 30-37.

Copeland, D. (2012). Realism and Neorealism in the study of regional conflict. In T. Paul (Ed.), *International Relations Theory and Regional Transformation* (pp. 49-73). Cambridge: Cambridge University Press. doi:10.1017/CBO9781139096836.005

Council of Europe (2001). Convention on Cybercrime Budapest, 23.XI.2001, https://rm.coe.int/1680081561

Defence Turkey (2019). ADVENT Combat Management System. *Defence Turkey Magazine*, 14 (96), 68-71. https://www.defenceturkey.com/en/content/advent-combat-management-system-3742.

Elbit Systems (2023). https://elbitsystems.com/

General Atomics Aeronautical Systems, Inc. (GA-ASI) (2023). https://www.ga.com/ga-asi-awarded-id-iq-contract-for-advanced-battle-management-system

General Policy And Legislation On Cybercrime (2017). https://police.ge/en/projects/kiberdanashauli/kanonmdebloba-kiber-danashaulze-da-zogadi-politika#:~:text=In%20Georgia%20cybercrime%20issues%20are,Data%20or%20Computer%20System%20(Art

Gray, Colin S. (2013). *Making strategic sense of cyber power: Why the sky is not falling*, Strategic Studies Institute and U.S. Army War College Press, 9-15.

Havelsan (2021). Komuta kontrol yeteneklerimiz: Advent Savaş Yönetim Sistem, *Havelsan Dergi*, Sayı 9 (3), 16, 28, 46.

Havelsan (2021). Pakistan MİLGEM'lerinin savaş sistemleri entegratörü: Havelsan, *Havelsan Dergi*, 10 (3), 8- 10, https://www.havelsan.com.tr/haberler/guncel/havelsan-pakistan-milgem-korvetlerinin-savas-sistemi-ana-entegratoru

Havelsan (2022). SEDA'dan tam isabet. *Havelsan Dergi*, 13-14 (3). 77, https://www.havelsan.com.tr/kurumsal/medya-merkezi/havelsan-dergi#7865

Havelsan (2023). "Advent: Ağ Destekli Veri Entegre Savaş Yönetim Sistemi" https://www.havelsan.com.tr/sektorler/savunma-ve-guvenlik/deniz/su-ustu-savas-yonetim-sistemleri/havelsan-advent

Hunker, J. (2010). Cyber war and cyber power: Issues for NATO doctrine, *NATO Defense College*, No. 62,1-13.

ITU (2017). Global Cybersecurity Index, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

Jervis, R. (1997). *System Effects: Complexity in Political and Social Life*. Princeton: Princeton University Press.

Johnson, E. M. ve Henderson, D. (Mayıs 1987). Training Requirements for the Battlefield Management System (BMS): A Preliminary Analysis, Research Product 87-18, Kentucky, *U.S. Army Research Institute for the Behavioral and Social Sciences*, https://apps.dtic.mil/sti/pdfs/ADA185468.pdf

Lockheed Martin (2023). https://www.lockheedmartin.com/

Martin C. Libicki (2009). *Cyberdeterrence and Cyberwar*, USA: RAND Corporation.
NATO Standardization Office (2023). NSDD, https://nso.nato.int/nso/nsdd/main/list-promulg.
NATO (2021). Cyber Security Risk Assessment Process for Military Systems, STO TECHNICAL REPORT AC/323(IST-151)TP/1030.
NC State University (2023). Ethics in computing, https://ethics.csc.ncsu.edu/intellectual/reverse/study.php
Paulson, J. W., Succi, G., ve Eberlein, A. (2004). An empirical study of open-source and closed-source software products. *IEEE transactions on software engineering*, 30(4), 246-256.
Rahmat, R. (November 2021). Havelsan teams up with Thales on Indonesia's 90 m OPV programme, https://www.janes.com/defence-news/news-detail/havelsan-teams-up-with-thales-on-indonesias-90-m-opv-programme
Raytheon Missiles And Defense (2023). https://www.raytheonmissilesanddefense.com/
Robert O. Keohane ve Lisa L. Martin (2003). Institutional Theory as a Research Program, Progress in International Relations Theory: Appraising the Field, eds: Colin Elman and Miriam Fendius Elman, London: MIT Press
Saab (2023). https://www.saab.com/
SavunmaSanayiST (Şubat 2023). Aselsan'ın 2022 yılı finansal sonuçları açıklandı. https://www.savunmasanayist.com/aselsanin-2022-yili-finansal-sonuclari-aciklandi/.
Snyder, J. (1991). *Myths of Empire: Domestic Politics and International Ambition*. Cornell University Press, pp. 63,217
Şenol, M. (2018). Hibrit savaş kapsamında siber savaş ve siber caydırıcılık, *siber güvenlik ve savunma farkındalık ve caydırıcılık.* Şeref Sağıroğlu, Mustafa Alkan (Ed.). Ankara: Grafiker Yayıncılık.
Şenol, M. ve Karaçuha, E. (2020). Ağların gücü: Ağ destekli yaşam, yönetim ve savaş, *Havelsan Dergi*, 6 (2), 58-60.
Taliaferro, Jeffrey W. "Security Seeking under Anarchy: Defensive Realism Revisited." International Security, vol. 25, no. 3, 2000, pp. 128–61: 131. JSTOR, http://www.jstor.org/stable/2626708. Accessed 12 Apr. 2023.
Thales (2023). https://www.thalesgroup.com/en
Thales, TACTICOS- Combat Management System, https://www.thalesgroup.com/en/tacticos-combat-management-system
Thalesgruoup (2018). https://www.thalesdsi.com/wp-content/uploads/2018/12/thales_tacticos.pdf
The SIPRI (2012). https://www.sipri.org/databases/armsindustry, the SIPRI Top 100 arms-producing and military services companies in the world (excluding China), 2012(a)
The SIPRI (2023). Military expenditure, https://www.sipri.org/research/armament-and-disarmament/arms-and-military-expenditure/military-expenditure
The USA Congressional Research Service (2022). Joint All-Domain Command and Control, https://sgp.fas.org/crs/natsec/IF11493.pdf.
The U.S. Government Accountability Office (2022). DOD Cybersecurity: Enhanced Attention Needed to Ensure Cyber Incidents Are Appropriately Reported and Shared, https://www.gao.gov/products/gao-23-105084.
The White House (February 2003). National Strategy to Secure Cyberspace, National Strategy for Homeland Security, https://www.energy.gov/sites/prod/files/National%20Strategy%20to%20Secure%20Cyberspace.pdf, (19.05.2022)
TRT (2023). 22 ülke Aselsan silahları ile korunuyor. https://www.trthaber.com/haber/savunma/22-ulke-aselsan-silahlari-ile-korunuyor-759192.html

Turqualıt (2023). Destek programı kapsamındaki firmalar. http://www.turquality.com/markalar/turquality-destek-programi-kapsamindaki-firmalar

Tusiad (2021). Türkiye'de yazılım ekosisteminin geleceği, https://tusiad.org/tr/yayinlar/raporlar/item/download/9542_a7e88172c603200ba9a01ddd99a33c5f

Tübitak Bilgem (2021). Gerçek zamanlı işletim sistemi (GİS), Aselsan SARP ile sahada. https://bilgem.tubitak.gov.tr/tr/haber/tubitak-bilgem-gercek-zamanli-isletim-sistemi-gis-aselsan-sarp-ile-sahada.

Türkiye Cumhuriyeti Ticaret Bakanlığı (2022). Circular of Turquality Promotion Project Support (15.11.2022). Decision No. 5973 on Export Supports, https://ticaret.gov.tr/destekler/ihracat-destekleri/5973-sayili-ihracat-destekleri-hakkinda-karara-iliskin-genelgeler

Türkiye Cumhuriyeti Ulaştırma ve Altyapı Bakanlığı (2013). Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-plani-2013-2014-5a3412cf8f45a.pdf

Türkiye Cumhuriyeti Ulaştırma ve Altyapı Bakanlığı (2016). Ulusal Siber Güvenlik Stratejisi 2016-2019, https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf

Türkiye Cumhuriyeti Ulaştırma ve Altyapı Bakanlığı (2020). Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023, https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusal-siber-guvenlik-stratejisi-ve-eylem-plani-2020-2023.pdf

Türkiye Deniz Kuvvetleri Komutanlığı (2023). ADA sınıfı korvet projesi (MİLGEM). https://www.dzkk.tsk.tr/Arge/icerik/firkateyn-muhrip-projeleri

Türkiye Deniz Kuvvetleri Komutanlığı (2023). Fırkateyn Muhrip Projeleri, https://www.dzkk.tsk.tr/Arge/icerik/firkateyn-muhrip-projeleri

Voo, J. Et al. (2020). National Cyber Power Index 2020, Harward Kennedy School Belfere Center, https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf

Waltz, K. (1979). *Theory of international politics*. Berkeley: University of California.

Waltz, K. (2000). Structural Realism after the Cold War. *International Security*, *25*(1), 5–41.

Waltz, K. (2018). *Man, the state and war: A theoretıcal analysis*. New York: Columbia University Press.

Warsaw Summit Communiqué (2016). Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw on 8-9 July.

Wezeman, P. D., Gadon, J ve Wezeman, S. T. (2022). Trends in international arms transfers, *SIPRI Fact Sheet*, https://www.sipri.org/sites/default/files/2023-03/2303_at_fact_sheet_2022_v2.pdf.