GÜVENLİK ÇALIŞMALARI DERGİSİ

Turkish Journal of Security Studies

ISSN: 2148-6166 | **e-ISSN:** 2757-7716 | **Cilt/**Volume: 26 | **Sayı/**Isssue: 2 | **Aralık/**December: 2024

GÜVENLİK ÇALIŞMALARI DERGİSİ

Turkish Journal of Security Studies

ISSN: 2148-6166 • **e-ISSN:** 2757-7716 • **Yıl/Year:** 26 • **Cilt/Volume:** 26 • **Sayı/Issue:** 2 • Aralık/December 2024

Yayın Sahibi / Owned by

Polis Akademisi Başkanlığı Güvenlik Bilimleri Enstitüsü Müdürlüğü adına

İmtiyaz Sahibi / Published by

Prof. Dr. Murat BALCI, Polis Akademisi Başkanı

Sorumlu Yazı İşleri Müdürü / Issuing Editor

Murat GÜNAY, 2. Sınıf Emniyet Müdürü

Yazışma Adresi / For Correspondence: Polis Akademisi Başkanlığı, Güvenlik Bilimleri Enstitüsü Müdürlüğü, Necatibey Cad: 108, 06580 Anıttepe - Çankaya - Ankara / TÜRKİYE Tel: +90 (312) 462 90 43
E-posta: guvenlikcalismalari@pa.edu.tr

Baskı: Polis Akademisi Başkanlığı Basım ve Yayım Şube Müdürlüğü Fatih Sultan Mehmet Bulvarı No:218, 06200 Yenimahalle, Ankara Sertifika No: 45724

GÜVENLİK ÇALIŞMALARI DERGİSİ

Turkish Journal of Security Studies

İÇİNDEKİLER / CONTENTS

Editörden

Güvenlik Çalışmaları Dergisi'nin yeni bir sayısını sizlere sunmaktan mutluluk duyuyoruz. Günümüzde güvenlik konuları, ulusal-uluslararası düzeyde gün geçtikçe daha karmaşık ve çok boyutlu bir yapıya bürünmektedir. Bu kapsamda, mevcut sayımız, önde gelen akademisyenler tarafından kaleme alınan çalışmalar sayesinde hem teorik bilgi hem de pratik çözüm yolları yanında, güvenlik alanındaki mevcut tartışmaları daha doğru anlamamıza imkân sağlayan dört makaleyle literatüre katkı sunmayı amaçlamaktadır.

Dergimizin "The Role of Intelligence in America's Grand Strategy" başlıklı ilk makalesi, Dr. Öğr. Üyesi Andaç Karabulut tarafından yazılmıştır. Söz konusu çalışmada, Amerika'nın bağımsızlığından I. Dünya Savaşı sonrasına kadar uzanan tarihî gelişmeler temelinde, istihbarat faaliyetlerinin çeşitlenerek kurumsallaştığı süreç ele alınmıştır. Makalede, ekonomik ve operasyonel istihbaratın 21. yüzyılda ABD'nin kritik rolünü ayrıntılı incelenmiştir.

Sayının ikinci makalesi Doç. Dr. Atalay Bahar'ın "Büyük Çaplı Krizlerde Emniyet Genel Müdürlüğünün Kullandığı Stratejik İletişim Yöntemleri: X Sosyal Medya Platformu Örneği" başlığını taşımaktadır. Yazar, 6 Şubat 2023'te meydana gelen Kahramanmaraş merkezli iki büyük deprem anında Emniyet Genel Müdürlüğünün yürüttüğü stratejik iletişim faaliyetlerini incelemiştir. Bu kapsamda kamuoyunun nasıl bilgilendirildiği, dezenformasyonla mücadele yanında toplumsal dayanışmayı destekleyici çalışmaların sosyal medya aracılığıyla nasıl yürütüldüğü analiz edilmiş ve elde edilen bulgular kriz iletişimi perspektifinde değerlendirilmiştir. Çalışma, stratejik iletişim süreçlerinin etkinliğinin önemini ortaya koymayı amaçlamaktadır.

Bu sayıda yer alan üçüncü makale, Dr. Yunus Öztürk tarafından kaleme alınmış olan "What Makes Civil Wars Protracted? A Review of Systemic, Organizational & Individual-Level Factors" dür. Makale, iç savaşların sürekliliğini etkileyen sistemik, örgütsel ve bireysel etkenleri kapsamlı bir şekilde incelemektedir. Ek olarak, Soğuk Savaş sonrası dönemde ortaya çıkan çok kutuplu düzen ve neoliberal ekonomi politikalarının küresel güvenliğe etkilerini belirlemek, iç savaşların çözümüne yönelik teorik ve pratik öneriler sunmak bu makalenin ana amacıdır.

“State Cyber Warfare: The Strategic Shift Towards Private Sector Targets” bu sayının dördüncü makalesidir. Dr. Esra Merve Çalışkan tarafından kaleme alınan çalışmada, devlet destekli siber saldırıların özel sektörü hedef almasının ulusal güvenlik ile ekonomik istikrar üzerindeki etkileri ele alınmış ve bu stratejik değişimi etkileyen faktörlerin irdelenmesi amaçlanmıştır. Çalışma, kritik altyapıları korumaya yönelik kamu-özel iş birliği ve uluslararası ortaklık ihtiyacını tartışarak yeni politika önerileri sunmuştur.

Son olarak, dergimizin bu sayısında yer alan tüm yazarlara ve desteklerini esirgemeyen değerli hakemlere teşekkürlerimizi sunarız. Güvenlik çalışmaları bağlamındaki akademik birikimin, literatüre verdiği katkılar yanında uygulamalı alandaki farkındalığı da artıracağına inanıyoruz. Bunun için gelecek sayılarımızda güvenlik temasının çeşitli boyutlarını irdeleyen bilimsel çalışmaları sizlerle buluşturmaya devam edeceğiz.

Şenol Yaprak

Turkish Journal of Security Studies

ISSN: 2148-6166
Year: 26 Volume: 26 Issue: 2 December 2024 p.140-155 Article Type: Research
Received Date: 19.10.2024- Accepted Date: 24.12.2024

The Role of Intelligence in America's Grand Strategy

Andaç KARABULUT*

Abstract: The importance of intelligence in the American Revolutionary War is undeniable. However, although George Washington, the commander of the Continental Army and the first president of the United States, was an influential figure in American intelligence during this war, the conditions of the time did not allow for the institutionalization of intelligence practices. Indeed, after World War I, the United States abandoned its isolationist foreign policy. This shift not only influenced the liberal policies adopted by Woodrow Wilson but also led to significant changes in American state policies and intelligence strategies. During the Cold War, the perception of communism as a threat to liberal policies and the global economic order led the United States to adopt a more rational and pragmatic approach to dealing with this threat. As a result, the United States not only developed a more disciplined approach to intelligence operations but also institutionalized them. The indirect victory of the United States in the Cold War and the dominant role of the US dollar in the global economic system significantly contributed to the strengthening of American hegemony and the implementation of the American Grand Strategy. This study seeks to answer the question: What role does intelligence play in the American Grand Strategy?

Keywords: Grand Strategy, Intelligence, International Relations, Liberalism, Hegemony

* Lecturer Dr., Yozgat Bozok University, Faculty of Economics and Administrative Sciences, Department of Political Science and International Relations - Andaç, andaç.karabulut@bozok.edu.tr, ORCID: 0000-0002-5620-2344

Güvenlik Çalışmaları Dergisi

ISSN: 2148-6166
Yıl: 26 Cilt: 26 Sayı: 2 Aralık 2024 s.140-155 Makale Türü: Araştırma
Makalenin Geliş Tarihi: 19.10.2024 Makalenin Kabul Tarihi: 24.12.2024

Amerika'nın Büyük Stratejisinde İstihbaratın Rolü

Andaç KARABULUT*

Öz: Amerika Birleşik Devletleri'nin Bağımsızlık Savaşı'ndaki istihbaratın önemi tartışmasızdır. Ancak, bu savaşta Kıta Ordusu'nun komutanı ve ABD'nin ilk başkanı olan George Washington, Amerikan istihbaratında önemli bir figür olmasına rağmen, dönemin koşulları istihbarat uygulamalarının kurumsallaşmasına olanak tanımamıştır. I. Dünya Savaşı sonrasında Amerika Birleşik Devletleri, izolasyonist dış politikasını terk etmiştir. Bu dönüşüm, yalnızca Woodrow Wilson'un benimsemiş olduğu liberal politikaları etkilemekle kalmamış, aynı zamanda Amerikan devlet politikalarında ve istihbarat stratejilerinde de önemli değişikliklere yol açmıştır. Soğuk Savaş dönemi, komünizmin liberal politikalara ve küresel ekonomik düzene tehdit olarak görülmesiyle ABD'nin, bu tehditle başa çıkabilmek için daha rasyonel ve pragmatik bir yaklaşımı benimsemesini sağlamıştır. Sonuç olarak, Amerika Birleşik Devletleri, istihbarat faaliyetlerinde daha disiplinli bir yaklaşım geliştirmekle kalmamış, aynı zamanda bu alanda kurumsallaşmaya gitmiştir. ABD'nin Soğuk Savaş'taki dolaylı zaferi ve Amerikan dolarının küresel ekonomik sistemdeki belirleyici rolü, Amerikan hegemonyasının güçlenmesine ve Amerikan Büyük Stratejisi'nin hayata geçirilmesine önemli katkılar sunmuştur. Bu çalışmada, şu soruya yanıt aranacaktır: İstihbarat, Amerikan Büyük Stratejisi'nde nasıl bir rol oynamaktadır?

Anahtar Kelimeler: Büyük Strateji, İstihbarat, Uluslararası İlişkiler, Liberalizm, Hegemonya

* Doktor Öğretim Üyesi, Yozgat Bozok Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Siyaset Bilimi ve Uluslararası İlişkiler Bölümü, andaç.karabulut@bozok.edu.tr, ORCID: 0000-0002-5620-2344

Introduction and Methodology

With Christopher Columbus' discovery of the Americas in the 15th century, this region quickly attracted the attention of the leading states of the time, eventually becoming a territory of colonies. A rapid wave of migration to the Americas began, primarily led by Spain, Portugal, France, and England. As a result, the Americas became a new region of exploitation, particularly for Europe. This colonial period also laid the foundations for what would later become the United States, a key player in the 21st century international system.

In contrast to countries like Germany, which have its roots in the Germanic tribes, France in the Franks, and England in the Anglo-Saxons, the United States is a unique state composed of colonies. For example, regions like New York, Delaware, and New Jersey were formed after the dissolution of Dutch colonies (Sencer, 1987, p.15). As mentioned above, the United States is a significant actor in the international system. When assessing the elements of U.S. national power within the framework of national power components, it is evident that the U.S. has notable policies in the international arena. A closer examination of the characteristic features of U.S. policies reveals that American political approaches are often influenced by those of England (Kılıçaslan, 2002, p. iii).

In the contemporary United States, scientific approaches play crucial role in shaping its political, foreign, and security policies. Scholars like Hans Morgenthau and Zbigniew Brzezinski, who have examined international relations within a scientific framework, have influenced American policies and contributed to the broader international field. However, the most significant factor underpinning America's modern political approach is its intelligence system. While scholars like Hans Morgenthau and Mert Bayat have emphasized national power elements, they have mostly overlooked intelligence, leading to a lack of focus on this critical aspect. Nevertheless, in the 21st century, intelligence has undeniably become a key component of national power for states (Karabulut, 2023, pp. 20-100).

The technological advancements brought about by the Cold War, along with the U.S.-led cooperation to establish supranational organizations in Europe, laid the technological and political groundwork for globalization in the international system. This development, especially following the terrorist attacks on the U.S. in 2001, also gave rise to the concepts of "global terrorism" and "global security." (Manfred, 2006, pp. 100-105).

With the dynamic nature of the international system, the role of intelligence in the implementation of the global policies of the United States, a dominant actor in the system, is undeniably significant. Franklin D. Roosevelt made the following statement on June 8, 1934: *"Fear and anxiety based on the unknown danger contribute to social unrest and economic demoralization"* (SSA, 2024). According to Franklin D. Roosevelt, identifying threats and dangers in advance is essential for

ensuring public order and maximizing social welfare. With the onset of the Cold War, the United States abandoned its isolationist policies. The rapid emergence of the communist threat, particularly after Nazi Germany, posed a significant danger even within U.S. borders.

During the Cold War, U.S. intelligence activities accelerated. Intelligence holds strategic importance in American security policies. However, rather than functioning within a traditional framework, the U.S. manages its intelligence activities within an institutional structure. Additionally, the U.S. evaluates intelligence work from a scientific perspective. For instance, U.S. intelligence efforts assess security issues in the international system not merely in terms of state threats, terrorism, or communism, but within the context of new security approaches. An example of this is the support provided by In-Q-Tel, a nonprofit venture capital firm, to Colossal Biosciences, which conducts genetic research on animals in the steppes of Russia, as part of its investments in 2023 (Crunchbase, 2024). The Central Intelligence Agency (CIA) financed In-Q-Tel, Inc., a newly established company in July 1999, to invest in the research of promising commercial technologies and to support the agency's critical operations by developing of new technologies (Molzhan, 2023, p. 47).

Theories are essential for analyzing the relationships between relevant phenomena and events in a scientific field within a specific framework. Just as they are important in the natural sciences, theories are also crucial for preventing wars and establishing peace. For this reason, "theories" hold significant importance in Political Science and International Relations, which are branches of the social sciences. In scientific studies, data synthesis and analysis rely heavily on theories. While this may impose certain limitations on the study, it contributes to healthier analyses of relevant topics in social sciences, where experimentation is not feasible. International relations theory aims to explain why international events occur. Despite these theories, the vast majority of theorists engage in speculation regarding the relationships between sovereign states. Their goal is interpreted as finding and understanding the patterns of mutual political interactions between states (Aydin, 1996, pp. 90-95). The research article will be conducted using a qualitative method along with a literature review.

Theory: Realism and National Interest

The United States seeks to maximize its national interests in line with its grand strategy. Although the concepts of national interest and national security are often examined together within the international system, there are times when the concept of national interest is prioritized over national security, or when states shape their high-level policies based on national interests (Birdişli, 2011, p. 152). Although Hans Morgenthau directly associates national interest with military power, many international relations theorists view the joint examination of natio-

nal interest and military power as a tragic situation. According to Raymond Aron, national interest should not be solely linked to foreign policy. This is because national interest is a historical category (Trifunovic and Curcic, 2021, p. 80). Hans Morgenthau explains power as the primary objective of international politics and a means to achieve that objective. Along with this explanation, he systematically assesses a nation's power (Morgenthau, 1976, pp. 141-152). National power is defined as the sum of a nation's elements to achieve its national objectives (Tezkan, 2000, p. 11). In his work "The Relations of Nations," Frederick Hartman defines national power as the identification of a nation's strengths and weaknesses to secure itself (Hartman, 1957, pp. 118-121).

The theory of realism, which holds a significant place in international relations theories, emphasizes the importance of national security and military power. While realist theorists stress the significance of military power and maintaining control, they also highlight the absence of permanent friends or enemies for states. For instance, in Dr. Ifay F. Chang's work "Hegemony & Anti-Hegemony in US-China Relations," he references Henry Kissinger's statement, "America has no permanent friends or enemies, only interests," underscoring the enduring importance of national interest today (Machiavelli, 2002, pp. 40-45; Chang, 2023, pp. 5-15).

In 1950, the importance of the concept of "national interest" rapidly increased. This concept became the core argument of America's policy against the Soviets. Hans Morgenthau began examining the relationship between diplomacy and national interest shortly after the Soviet nuclear test. This contributed to the development of negotiation relations between the United States and the Soviet Union (Navari, 2016, pp. 47-50).

Hans Morgenthau asserts that elements such as law and international morality are of secondary importance compared to the concepts of national power and national interest. Protecting national interests has been established as the most important aspect of American foreign policy. In this context, he emphasizes that the Soviet threat directly endangers American national interest (Morgenthau, 1970, pp. 7-14).

Referring to the Cold War period, it is noted that many countries, including China and Ethiopia, emphasized concepts such as collective security, universal democracy, and lasting and just peace within the framework of liberal policies. These concepts had an impact on national interests, particularly in terms of rigid changes in territorial status. Hans Morgenthau highlights that due to the rigid changes at borders, the national interests of states will always lead to conflict (Morgenthau, 1947, pp. 57-78).

Hegemonic Stability Theory and America's Grand Strategy

Hegemony was initially defined in international relations as being limited to military power. Although the expansion and strengthening of hegemony are often equated with increase in military power, this perspective is incomplete. However,

political scientists have emphasized that hegemonic control can be more effectively managed through economic power. This emphasis has led to the argument that hegemony should focus on the elements of national power. (Aydın, 2019, pp. 1346-1347).

States that possess critical raw materials, control significant capital resources, and have access to large markets for imports are described as hegemonic. From a neoliberal perspective, these states are characterized by their extensive free trade networks and economic size, while the neorealist view defines them based on the importance of political power, national income, economic growth, and social stability (Prabhakar, 2010, pp. 1-3). According to Benjamin J. Cohen, American hegemony is described as an advanced version of classical colonial imperialism. Cohen notes that American hegemony has developed following the Cold War (Cohen, 2008, pp. 22-25).

Since 1945, the primary factor guiding American foreign policy has been the maintenance of American global hegemony. For this reason, Steven Hurst argues that among the reasons for America's invasion of Iraq were the easy access to and transport of Middle Eastern oil and energy resources for the continuation of global American hegemony, ensuring Israel's security, and preventing the establishment of potential hegemony in the region (Hurst, 2009, p. 8).

Richard Rosecrance and Arthur Stein define the concept of "Grand Strategy" as "generalship in war or deterrence in peacetime." The British military historian and theorist B. H. Liddell Hart emphasizes the military aspect of grand strategy, arguing that its role is to "coordinate and direct all the resources of a nation or group of nations to achieve the political objectives of war." Liddell Hart also discusses the mobilization of material and immaterial resources to "maintain the services of war" and regulate the distribution of power armed forces and industry. Other topics frequently contemplated by grand strategists include the selection of primary and secondary theaters of war, priorities in arms production, and finding suitable allies. Looking at modern history, grand strategy evokes images of Bismarckian power balance. When these approaches are generally assessed, the interpretation of the concept of "Grand Strategy" can be understood as the integration of a state's elements of national power in both war and peace, while ensuring the security of its allies (Williams, 2021, pp. 40-41).

While the United States has rapidly begun to expand its hegemony, studies have been conducted on the topic of Grand Strategy, which is the approach defined in America. While hegemony primarily focuses on economic interests, with military power taking a secondary role, Grand Strategy differs by prioritizing security issues. It encompasses the identification of elements that pose threats to the American nation and the determination of allies. According to William C. Martel, Grand Strategy comprises elements encompassing politics, doctrine, strategy, and operations (Martel, 2015, pp. 20-55).

With the end of the Cold War, America's Grand Strategy was to expand its own hegemony. Christopher Layne points out that, unlike other hegemonic studies, the factors shaping American hegemony stem not from threats or structural necessities, but rather from American domestic politics. However, the most significant issue he discusses is the term "Grand Strategy." According to Layne, the United States has aligned its goals and means in its quest for security. During peacetime, the United States implements its Grand Strategy by defining security interests, identifying threats to those interests, and defending state interests. Creating a power imbalance in the international system is crucial for America, as such an imbalance fosters hegemony. In this context, military and economic power are essential (Layne, 1998, pp. 8-17). For example, the United States has shaped other countries' policies through the Marshall Plan to align with its global interests. A key tool in shaping this global development policy according to its own interests is the public diplomacy it employs. American public diplomacy aims to facilitate the control of raw material resources, capital exports, and the monitoring of markets without the need for direct violence or warfare (Bağce, 2003, p. 74).

As previously mentioned, America's Grand Strategy encompasses a part of its hegemony, signifying the promotion of liberal economics and the safeguarding of the American economy. However, following the Cold War, factors such as the increase in regional conflicts and the rapid rise of regional actors have brought "security" to the forefront of America's Grand Strategy. Dr. Richard D. Hooker, who served as Deputy Commander and Dean at the NATO Defence College in Rome in 2013, emphasizes that the scope of America's Grand Strategy is related to American security. According to Hooker, the tools of Grand Strategy include alliances and bilateral security treaties, a robust military structure, and the presence of this military structure in global bases, as well as a strong intelligence service (Hooker, 2016, pp. 1-6).

The Role of Intelligence in American Grand Strategy

With the discovery of America, rapid colonization and missionary activities allowed European states to penetrate the geography. In the 17th century, England's increasing influence in America, and the Dutch beginning to establish their presence in the region, impacted the Spanish and Portuguese monopoly in the area. As England quickly colonized, each colony was responsible for managing its own territory. However, at the head of the colonial assemblies were governors appointed by the King of England (Yıldız and Arslan, 2023, pp. 242-245).

During America's War of Independence, England employed tactical propaganda as an intelligence tool among British mercenaries. The narrative that mercenaries would live in prosperity influenced the American War of Independence. This discourse also persuaded rival elements during the conflict (Avcı, 2018, p. 106). In addition, two critical elements were present for decision-makers: intel-

ligence and reconnaissance. The British were unable to associate reconnaissance movements with the presence of cavalry units in their army system. As a result, reconnaissance lost its significance, while intelligence quickly gained importance. Although intelligence was vital in the mid-18th century, it was organized in a primitive manner. There was no separate intelligence unit; instead, intelligence was conducted by intelligence officers. British Baron I. Amherst conducted intelligence work to identify supply routes against the French during the war. In contrast, British General Henry Clinton emphasized operational intelligence, focusing on the information regarding the weapons and ammunition in the rebels' inventories (Kaplan, 1990, pp. 115-125).

George Washington's military career significantly guided the intelligence system. His intelligence skills directly influenced the American War of Independence. With support from England, Washington conducted substantial intelligence operations against the French. George Washington emphasized the importance of intelligence: "There is nothing more necessary than good intelligence to defeat an enemy, and to obtain it requires greater effort" (Rose, n.d., p. 2).

According to George Washington, the concept of intelligence was seen as synonymous with secrecy and cunning. However, he believed that to have a strong intelligence system, he first needed the army's full support. By gaining the support of the people, Washington aimed to achieve success in the field of intelligence, as he considered intelligence the primary element necessary for success on the battlefield. Although these statements align with the paradigm of espionage activities, Washington later realized that relying solely on espionage was insufficient. During the War of Independence, the need for counterintelligence—a radical intelligence activity of the time—became essential for Washington. In response, he established a secret committee solely dedicated to counterintelligence activities (Brad and Mensch, 2018, pp. 20-55).

As previously mentioned, in addition to his military identity, George Washington was a remarkable political leader and America's first intelligence chief. During the American War of Independence, he allocated 10% of military funds to intelligence activities. Washington established offices for espionage and counterintelligence and set up special offices for military intelligence in Boston, New York, and Philadelphia. He personally oversaw the management of these offices. In New York, a group of intelligence agents known as the Culper Ring, consisting of 20 members, attempted to conduct covert intelligence operations by engaging in trade to disguise their activities (DIA, 2014).

After England evacuated Philadelphia during the American War of Independence, Henry Clinton was appointed by the British to manage agents and informants. Meanwhile, between 1780 and 1790, logistical support for the revolutionaries was secretly provided by the Mount Vernon nonprofit organization, owned by the Washington family. During this period, the Indigenous people of America, known as the "Redskins," served as an important intelligence asset for George

Washington. Their skills in tracking and trailing made them particularly effective as intelligence agents against the French (Grizzard, 2002, pp. 10-20).

During the American War of Independence, George Washington attempted to conduct intelligence activities by leveraging companies, organizations, and ethnic groups such as Native Americans, even though a formal intelligence structure had not yet been established. The presence of numerous states competing for colonization, from England to Spain, also led to intelligence wars in the region. Washington's military experience did not translate effectively into intelligence operations. Initially, he relied on his subordinates to gather intelligence through reconnaissance and provide feedback, but the prevalence of inaccurate reports increased the likelihood of losing the American War of Independence. According to Sergeant Quinnus G. Caldwell, who served in the American Armed Forces, one reason for the failures in intelligence operations during the war was a lack of training for spies, as well as the absence of necessary strategies and skills to operate covertly. However, over time, American intelligence gained momentum by adopting materials such as encrypted reports and invisible ink letters developed by chemist and physician Sir James Jay (Caldwell, 2018, pp.1-3).

After the war with Spain in 1898, America took its first steps toward becoming a "global power." The United States, through the treaty signed in 1898, acquired Puerto Rico and Guam as war reparations and gained the Philippines for 20 million dollars. With Cuba gaining its independence, America emerged as an East Asian state. The post-World War I era marked the first official step in America's shift from isolationist policies to a global political role, particularly with the emergence of Woodrow Wilson, a leader from outside Europe, as a regulatory actor in the international system (Özdal and Karaca, 2015, pp. 350-355).

With the Cold War, American economic, political, and security policies underwent significant changes, leading to a transformation in the traditional understanding of American intelligence that dates back to the George Washington era. According to Hans Morgenthau, intelligence plays a crucial role in determining national interests. Accordingly, a natural relationship exists between the policies outlined in the Grand Strategy and intelligence. Intelligence can help address the major issue of uncertainty present in the policies established for the Grand Strategy (Fingar, 2012, pp. 119-121).

The United States significantly emphasizes intelligence operations during both wartime and peacetime. Diplomatic maneuvers carried out in peacetime are determined through intelligence, enabling the effective allocation of resources in line with the Grand Strategy. Among the most important tools of the Grand Strategy during both war and peace are intelligence and propaganda (NDISC, 2022). For instance, during the Cold War, the spread of communism in Latin American countries posed a threat to U.S. hegemony in the region. The United States' policies to combat communism were sometimes implemented at the intelligence level. Following a military intervention in Bolivia in 1947, approximately 30,000

individuals, mostly miners and agricultural workers, organized various actions, while U.S. support for the Bolivian junta increased American dominance over Bolivia. Notably, the operational activities of the Central Intelligence Agency (CIA) led to the capture of Che Guevara in 1967, after which he was executed by the junta-controlled Bolivian army (Langguth, 1978, pp. 285-286). John Perkins states, *"There are many ways to eliminate a leader who threatens U.S. hegemony… (Bolivia) It's no surprise that the CIA was involved in the coup. Coups and counter-coups were never absent from Bolivia throughout the seventies."* This expression highlights the role of American intelligence in military coups when U.S. hegemony is under threat (Perkins, 2009, pp. 10-56).

The role of intelligence has been significant in the United States' established Grand Strategy. While the U.S. views regimes that may contradict its liberal ideals as security threats, it has carried out numerous covert operations in various countries to expand its hegemony. Former CIA agent John Perkins explains this situation as follows:

> *"The U.S. maintains the world's most sophisticated military. Although the empire is economically based (with the involvement of economic hitmen), world leaders know that when other sanctions are insufficient (as in Iraq), the military will be deployed"* (Perkins, 2009, pp. 10-11).

The previous explanations suggest that while the role of intelligence in America's Grand Strategy appears to be operational, this perspective is incomplete. According to an article published by the Central Intelligence Agency titled "Strategic Intelligence Situation," the key approach to intelligence within the Grand Strategy is strategic intelligence. Strategic intelligence not only shapes the Grand Strategy but is also described as the logic that directs the execution of the formulated strategy, rather than merely being an implementation plan (Heidenrich, 2007, pp. 2-4).

The United States' strategy for maintaining its hegemony includes economic liberalization as a core component of its Grand Strategy. One of the reasons the U.S. perceives communism as a threat is its resistance to liberal policies. Following the end of the Cold War, the most significant impact on the international system was the rapid liberalization of the global economic system, alongside the emergence of regional conflicts and newly independent states. This situation has provided a breeding ground for weak states to harbor terrorist organizations. Consequently, the uncontrolled management of Middle Eastern energy resources by terrorists and weak states poses a threat to the U.S. from both economic and security standpoints. A clear example of this is the presence of Al-Qaeda in Afghanistan, a weak state, which culminated in the attacks on September 11, 2001 (Ellis, 2009, pp. 362-366).

The United States' "Grand Power Strategy" fundamentally consists of four interrelated parameters. The first is the enhancement of military power in both qualitative and quantitative terms, with emphasizing on supporting allies—most

notably, the previously mentioned support for Israel. Additionally, it aims to integrate states into the global economic order organized by the United States and prevent the proliferation of nuclear weapons. In this process, the support of a multifaceted intelligence field, ranging from economic intelligence to nuclear intelligence, is undeniably significant. The emergence of the People's Republic of China as a notable actor in the international system, along with the rise of regional actors, negatively affects American hegemony. While Patrick Porter notes in his article "Why America's Grand Strategy Has Not Changed" that the global economic crisis has negatively impacted American hegemony, he also argues that the United States' institutionalized state structure and the interactive assessment of National Power Elements do not present a pessimistic outlook regarding American hegemony (Porter, 2018, pp. 10-11).

It is noted that while the United States dollar holds a significant position in the international economy, the increasing presence of the People's Republic of China in the global system directly negatively affects American hegemony rather than merely impacting the U.S. economy. Alongside America's geopolitical superiority, the hegemony of the dollar, particularly in the context of the United States' trillion-dollar budget deficit, constitutes a crucial prerequisite for the U.S. in terms of its global security commitments and the distribution of power within the international system (Stokes, 2013, pp. 1070-1075). The United States' increasing vulnerability to dollar hegemony in the face of the People's Republic of China implies a need to strengthen economic intelligence rather than just focusing on strategic or operational intelligence. Although American senator Daniel Patrick Moynihan emphasized that the Central Intelligence Agency failed in economic and technological espionage, particularly during the Cold War, advocating for the passive treatment of these intelligence domains, in the 21st century, economic intelligence has become an essential requirement within the framework of American Grand Strategy, just like strategic and operational intelligence (Foley, 1994, p. 136).

In a report published by the RAND Corporation in 2021, it was emphasized that military power should not be used as a tool in American Grand Strategy; instead, diplomacy should take precedence. Accordingly, in the expansion of diplomatic relations, strategic and intelligence diplomacy are highlighted over operational intelligence (NDISC, 2022).

In the studies mentioned above, we emphasized that the United States' perception of threats is integrated with military power. However, in the 21st century, the new threat perception of the United States has been defined as a state by realist theorists, who have indicated that states can also engage in economic warfare. The rapid shift of East Asian and Latin American countries toward heavy industry, along with their participation in the global search for raw materials, poses a threat to the American economy. This also jeopardizes the hegemony established by the United States. Under these conditions, Lieutenant Robert A. Rowe, who has served in the U.S. Navy, has stated that economic intelligence needs to be developed (Rowe, 1948, p. 546).

Conclusion

The importance of military policies became apparent with the onset of the decline of colonization movements during the American War of Independence. Under the leadership of George Washington, the American independence movement was realized alongside an intelligence approach that had yet to achieve institutionalization. The success of intelligence activities during the American War of Independence remains a subject of debate. This is primarily because 19th century American intelligence was limited to military intelligence and propaganda efforts, which did not extend beyond these realms. However, American intelligence underwent a significant evolution following World War I.

The devastating effects of World War I had a profound impact on the entire world, leading to shifts in the political perspectives of many nations, including the United States. The changes in economic policies, particularly those resulting from economic successes, also prompted alterations in state policies. Woodrow Wilson's liberal economic philosophy and the political and diplomatic understanding rooted in Wilsonian principles influenced global dynamics significantly. Although it could not prevent the outbreak of World War II, it fundamentally transformed the United States' political, security, and diplomatic approaches.

With the Cold War, the United States' understanding of security emphasized the need to evaluate national power elements, as articulated by Hans Morgenthau, rather than relying solely on classical military policies. While intelligence remained a subsidiary aspect of military policy during this period it operated with a multidisciplinary approach.

The end of the Cold War marked the dollar's emergence as a significant tool in the global economy, establishing a foundational step for America's hegemony. Consequently, the United States' grand strategy adopted a more rational role, facilitating the support and strengthening of American hegemony. However, no strategy, policy, or diplomatic maneuver can be successfully implemented without prior knowledge. Strong strategies necessitate robust intelligence, which is an indispensable requirement. In this context, the success or failure of America's grand strategy will be more realistically determined by the effectiveness of intelligence operations rather than military presence.

While not the focus of this study, America's attempts to expand its hegemony to Vietnam, and its use of military force to overthrow Saddam in Iraq, illustrates this point. In Vietnam, the U.S. suffered a loss, and its success in Iraq remains debatable. However, the operational intelligence conducted against the Taliban has drawn international attention due to its lower budget and effective execution.

The maximization of America's interests and the continuation of its hegemony are contingent upon the strength of the dollar in the international economy and the effectiveness of the People's Republic of China's policies within the international

system. In this context, the United States requires a dynamic intelligence policy to maintain and protect its hegemony. This necessity extends beyond military intelligence to encompass strategic and economic intelligence efforts as well.

In conclusion, the role of intelligence in the United States' Grand Strategy has evolved significantly over time, adapting to shifting geopolitical landscapes and emerging threats. From its early reliance on rudimentary intelligence practices during the American Revolution to the sophisticated economic and strategic intelligence operations of the 21st century, the U.S. has continuously sought to maintain its hegemony and address challenges posed by rival powers, particularly in the context of globalization and regional conflicts.

During the United States' independence process, intelligence was closely associated with military operations. Notably, America's perception of intelligence has influenced a wide range of topics, from foreign policy formulation to its grand strategy, especially after the Cold War. As a result, the United States has diversified the scope of intelligence, expanding it beyond purely military intelligence to include areas such as nuclear, operational, health, and economic intelligence et al. In our study, it has been determined that the most significant intelligence issues affecting America's grand strategy are operational and economic intelligence.

References

Aydın, G. (2019). The ebb and flow in the US trade policy: Does the hegemonic stability theory have explanatory power?, *Journal of Economic and Administrative Sciences*, 33(4), pp. 1345 – 1366.

Aydın, M. (1996). Approach, theory and analysis in international relations, *Ankara University Faculty of Social Sciences Journal, 51(1)*, pp. 71-114, DOI:https://doi.org/10.1501/SBFder_0000001917

Arslan, L., & Yıldız, S. (2023). Amerika Kıtasında Kolonizasyon ve Birleşik Devletlerin Kuruluşu. *Dünya Multidisipliner Araştırmalar Dergisi*, 6 (Prof. Dr. Durmuş Ali Aslan Özel Sayısı), 242-260.

Avcı, Ö. (2018). *İletişim ve Propaganda: Propagandanın Türleri*, In M. Karaca & C. Çakı (Eds.), Konya: Education Publishing House.

Bağce, E. (2003). Emperyalizm Kuramları ve Amerikan Kamu Diplomasisi. *İstanbul Üniversitesi Siyasal Bilgiler Fakültesi Dergisi*.

Birdişli, F. (2011). Ulusal Güvenlik Kavramının Tarihsel ve Düşünsel Temelleri. *Erciyes Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 1(31), 149-169.

Brad, M., & Mensch, J. (2018). *The first conspiracy: The secret plot to kill George Washington*, New York: Flatiron Books.

Chang, I. F. (2023). *Hegemony & anti-hegemony in US-China relations*, U.S.: Independently published.

Caldwell, Q. G. (2018). The importance of spies to Washington's success, *NCO Journal*, *Sergeants Major Course Class 67*.

Cohen, B. J. (2008). *International political economy*, New Jersey: Princeton University Press.

Ellis, D. C. (2009). U.S. grand strategy following the George W. Bush presidency, *International Studies Perspectives, 10(1).* pp. 361-377.

Fingar, T. (2012). Intelligence and grand strategy, *ORBIS, 56(1)*, pp. 118-134.

Folley, T. D. (1994). The role of the CIA in economic and technological intelligence. *The Fletcher Forum of World Affairs, 18(1)*, pp. 135-145.

Grizzard, F. E. (2002). *George Washington: A biographical companion*, New York: ABC-CLIO.

Hartmann, F. (1957). *The Relations of Nations*, New York: The Macmillan Company.

Heidenrich, J. G. (2007). The state of strategic intelligence, *Studies in Intelligence, 51(2).*

Hurst, S. (2009). *The United States and Iraq since 1979: Hegemony, oil and war*, Scotland: Edinburgh University Press.

Hooker, R. D. (2016). *American grand strategy*, Washington.: National Defence University Press.

Kaplan, R. (1990). The hidden war: British intelligence operations during the American Revolution, *The William and Mary Quarterly, 47(1)*, pp.115-138. DOI: https://doi.org/10.2307/2938043.

Kılıçaslan, A. (2022). Bir disiplin olarak sosyal çalışmanın doğuşu ve kurumsallaşması: ABD örneği, Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Langguth, A. J. (1978). *Hidden Terrors*, New York: Pantheon Books.

Layne, C. (1998). Rethinking American grand strategy: Hegemony or balance of power in the twenty-first century? *SAGE, 15(2),* pp.8-28.
Machiavelli. (2002). *The art of war,* (Nazım Güvenç, Trans.), Istanbul: Anahtar Kitapları.
Manfred, S. B. (2006). *Globalization*, (Abdullah Ersoy, Trans.), Ankara: Dost Kitapevi.
Martel, W. C. (2015). *Grand strategy in theory and practice: The need for an effective American foreign policy,* London: Cambridge University Press.
Molzhan, W. (2023). The CIA's In-Q-Tel model and its applicability, *Acquisition Review Quarterly*, Winter 2003.
Morgenthau, H. (1976). *International politics*, (Baskın Oran & Ünsal Oskay, Trans.). Ankara: Turkish Political Science Association Publications.
Morgenthau, H. (n.d.). *Scientific man vs. power politics*, Middlesex: Latimer House Limited.
Navari, C. (2016). Hans Morgenthau and the national interest. *Ethics & International Affairs, 30(1),* pp.47-54. DOI:10.1017/S089267941500060X.
Özdal, B., & Karaca, K. (2015). *Diplomasi Tarihi I*, Turkiye: Dora Yayınları.
Perkins, J. (2009). *Confessions of an economic hitman*, (Cihat Taşçıoğlu, Trans), Istanbul: APRIL Publishing.
Porter, P. (2018). Why America's grand strategy has not changed, *International Security, 42(4),* pp. 9–34.
Prabhakar, R. (2010). Hegemonic stability theory and the 20th century international economy, *E-International Relations.*
Rose, P. K. (n.d.). The founding fathers of American intelligence, Retrieved July 31, 2024, from www.cia.gov.tr.
Rowe, R. A. (1945). The Need for Strategic Intelligence on Economic War Potential, *Proceedings, 47(7).*
Sencer, M. (1987). The American Revolution in terms of human rights, *Human Rights Yearbook, Number.9.*
Stokes, D. (2013). Achilles' deal: Dollar decline and US grand strategy after the crisis, *Review of International Political Economy, 21(5),* pp. 1071-1094 DOI:http://dx.doi.org/10.1080/09692290.2013.779592 l
Trifunovic, D., & Curcic, M. (2021). National interest in security science: A realist perspective, *NSF Journal, 22(3),* pp.73-89. DOI: https://doi.org/10.37458/nstf.22.3.3
Williams, B. (2021). *Japanese foreign intelligence and grand strategy from the Cold War to the Abe era*, Washington.: Georgetown University Press.
Tezkan, Y. (2000). *Siyaset, Strateji ve Milli Güvenlik*, Ankara: Ülke Yayınları.

Internet Reference

Crunchbase.com. (n.d.). In-Q-Tel. Retrieved June 6, 2024, from https://www.crunchbase.com/organization/in-q-tel/recent_investments

Defense Intelligence Agency. (2014). George Washington: More than a general and a president. DIA Public Affairs. Retrieved August 1, 2024, from https://www.dia.mil/News-Features/Articles/Article-View/Article/566965/george-washington-more-than-a-general-and-a-president/#:~:text=Not%20only%20was%20George%20Washington,funding%20on%20intelligence%2Drelated%20activities.

SSA, FDR's Statements on Social Security. Retrieved June 4, 2024, from https://www.ssa.gov/history/fdrstmts.html

Notre Dame International Security Center, (2022), Retrieved June 4, 2024,https://ndisc.nd.edu

Güvenlik Çalışmaları Dergisi

ISSN: 2148-6166
Yıl: 26 Cilt: 26 Sayı: 2 Aralık 2024 s156-179 Makale Türü: Araştırma
Makalenin Geliş Tarihi: 12.10.2024 Makalenin Kabul Tarihi: 24.12.2024

Büyük Çaplı Krizlerde Emniyet Genel Müdürlüğünün Kullandığı Stratejik İletişim Yöntemleri: X Sosyal Medya Platformu Örneği

Atalay BAHAR*

Öz: 6 Şubat 2023 tarihinde meydana gelen Kahramanmaraş merkezli depremler gerek yayılım ölçeği gerekse depreme eşlik eden ikincil afetler nedeniyle yoğun yıkıma yol açmış; 11 il etkilenmiş, 50 binden fazla kişi hayatını kaybetmiş ve 100 binden fazla kişi de yaralanmıştır. Tüm kamu kurumlarının, özel kuruluşların ve vatandaşların iş birliği ile kurtarma ve yardım çalışmalarının sürdürüldüğü depremlerde Emniyet Genel Müdürlüğü (EGM) de aktif olarak görev almış ve deprem sonrasında bilinçlendirme faaliyetlerine hem geleneksel medya hem de sosyal medya platformları üzerinden devam etmiştir. Bu çalışmanın amacı, EGM'nin kamuoyunu bilgilendirmek, kasıtlı ve yanlış bilgilere karşı korumak, proaktif ve reaktif stratejilerle toplumu aydınlatmak için sürdürdüğü faaliyetleri stratejik iletişim yöntemleri ve kriz iletişim çalışmaları bağlamında incelemektir. Çalışma kapsamında, EGM'nin sosyal medya platformu X (eski adıyla Twitter) üzerinden Kahramanmaraş merkezli depremlere yönelik önleyici tedbirleri ve yardım çalışmaları ile dijital platformlarda yayılan provokatif paylaşımlar ve dijital dolandırıcılık faaliyetlerine yönelik gerçekleştirdiği çalışmalara odaklanılmıştır. Nitel araştırma yöntemlerinden betimsel analiz ile yürütülen bu çalışmada Kahramanmaraş merkezli depremlerin meydana geldiği 6 Şubat-31 Mart 2023 tarihleri arasında X platformunda, EGM tarafından dolaşıma sunulan 161 paylaşım tespit edilmiş ve bahsi geçen paylaşımlar stratejik iletişim yöntemleri bağlamında irdelenmiştir.

Anahtar Kelimeler: Dezenformasyonla Mücadele, Emniyet Genel Müdürlüğü, Kriz İletişimi, Stratejik İletişim.

* Doç. Dr. Polis Akademisi Başkanlığı, İstanbul Arnavutköy Polis Eğitim Merkezi, E-mail: atly.bhr@gmail.com, ORCID: 0000-0002-3146-1833.

Turkish Journal of Security Studies

ISSN: 2148-6166
Year: 26 Volume: 26 Issue: 2 December 2024 p.156-179 Article Type: Research
Received Date: 12.10.2024 Accepted Date: 24.12.2024

Strategic Communication Methods Used by the Turkish National Police in Large-Scale Crises: The Case of X Social Media Platform

Atalay BAHAR*

Abstract: The Kahramanmaraş-centered earthquakes that occurred on February 6, 2023, caused intense destruction due to both the scale of spread and the secondary disasters accompanying the earthquake; 11 provinces were affected, more than 50 people lost their lives, and more than 100 thousand people were injured. Turkish National Police Organization (EGM) also played an active role during earthquakes, where rescue and aid efforts were carried out with the cooperation of all public institutions, private organizations and citizens. It continued its awareness-raising activities both through the traditional media and social media platforms after the earthquakes. This study aims to examine the activities carried out by EGM to inform the public, protect it against deliberate and false information, and enlighten the society with proactive and reactive strategies within the context of strategic communication methods and crisis communication studies. The scope of the study focused on EGM's preventive measures and aid efforts for Kahramanmaraş earthquakes via the social media platform X (formerly known as Twitter), as well as the work carried out against provocative posts and digital fraud activities disseminating on digital platforms. In this study, which was carried out with the descriptive analysis method, one of the qualitative research methods, 161 posts circulated by the EGM were found on the X platform between February 6, 2023, and March 31, 2023, during the Kahramanmaraş earthquakes, and they were examined in the context of strategic communication methods.

Keywords: Combating Disinformation, Turkish National Police Organization, Crisis Communication, Strategic Communication.

* Assoc. Prof. Dr. Presidency of National Police Academy Istanbul Arnavutköy Police Vocational Training Center, E-mail: atly.bhr@gmail.com, ORCID: 0000-0002-3146-1833.

Giriş

Stratejik iletişim, sadece olağan zamanlarda değil, kriz anlarında da organizasyonların hedef kitleleriyle etkili bir biçimde iletişim kurmalarını sağlayan planlı ve sistematik bir yaklaşımı temsil etmektedir. Stratejik iletişimin temel amacı, kurumların güvenilirliği yanında itibarını korumak, kamuoyuna doğru ve güvenilir bilgi aktarımını sağlamaktır (Zheng, Liu ve Davison, 2018, s. 58). Özellikle büyük çaplı krizlerde, bilgi kirliliğinin yayılmasını önlemek ve kamuoyunu doğru yönlendirmek için stratejik iletişim süreçlerinin etkin bir şekilde yönetilmesi gerekmektedir (Buhmann ve Likely, 2018, s. 630). Bununla birlikte, kriz sonrası iyileşme süreçlerinde halkın doğru bilgilendirilmesi ve toplumsal dayanışmanın sağlanmasında stratejik iletişim kilit bir rol oynamaktadır.

Kriz iletişimi, ani gelişen beklenmedik olaylar karşısında, bir kurumun ya da organizasyonun kamuoyuyla kurduğu iletişim süreçlerini kapsamaktadır. Kriz anlarında hızlı ve doğru bilgi akışı sağlamak, yalnızca toplumun güvenini yeniden inşa etmek için değil, kriz yönetiminin etkin bir şekilde sürdürülmesi için de önemlidir (Reynolds ve Seeger, 2005, s. 45). Kriz iletişimi süreçlerinde; şeffaflık, güven ve empati gibi unsurlar, toplumun krizle başa çıkabilme kapasitesini artırmakta ve sonrasındaki iyileşme sürecine katkıda bulunmaktadır. Bu süreçte kullanılan doğru stratejiler, toplumsal moralin korunması ve yanlış bilgilerin yayılmasının önlenmesi açısından da kritik bir rol oynamaktadır. Dolayısıyla kriz iletişiminin zamanında ve etkili bir şekilde uygulanması, afet sonrası ortaya çıkabilecek ikincil krizleri önlemek için hayati bir öneme sahiptir.

Depremler, yer kabuğunda biriken enerjinin ani salınımıyla oluşan doğal afetlerdir ve tarih boyunca büyük can kayıplarına, ekonomik zararlara ve sosyal yıkımlara yol açmıştır. Tektonik plakaların hareketleri sonucu oluşan bu yer sarsıntıları, özellikle fay hatlarının yoğun olduğu bölgelerde büyük riskler oluşturmaktadır (Stein ve Wysession, 2003, s. 66). Bu riskler, yalnızca fiziksel hasarla sınırlı kalmayarak toplumsal düzenin bozulmasına, güvenlik sorunlarının ortaya çıkmasına, sağlık hizmetlerinin aksamasına ve uzun vadeli olumsuz ekonomik sonuçların doğmasına yol açarak çok boyutlu bir kriz ortamı ortaya çıkarmaktadır. Bu bağlamda, afetlerin yalnızca kısa süreli etkileri değil, uzun vadeli sonuçları da dikkate alınmalı ve bu doğrultuda etkin kriz yönetimi stratejilerinin geliştirilmesi gerekmektedir.

Dünya genelinde tarih boyunca yaşanan büyük depremler, bu felaketlerin yıkıcı etkilerini açık bir şekilde ortaya koymaktadır. Şili'de 1960 yılında meydana gelen 9,5 büyüklüğündeki Valdivia Depremi hem şiddeti hem de yol açtığı hasar açısından modern dönemin en büyük depremlerinden biri olarak kabul edilmektedir (United States Geological Survey, 2020, s.1). Bu durumun diğer bir örneği 2004 yılında Hint Okyanusu'nda meydana gelen 9.1 büyüklüğündeki deprem ve sonrasında oluşan tsunamidir. Bu olay, bölgesel bir felaket olmanın ötesinde 14

ülkeyi etkileyen küresel bir krize dönüşmüştür (Telford ve Cosgrave, 2006, s. 33). Büyük çaplı afetler hem ulusal hem de uluslararası boyutta iletişim ve müdahale kapasitelerinin yeterliği ile etkinliğinin geniş bir çerçevede ele alınarak sorgulanmasına zemin hazırlamaktadır. Afetlerin yıkıcı etkileri, ülkelerin sadece altyapılarını değil; sosyal, ekonomik ve güvenlik sistemlerini de derinden etkilemektedir.

Türkiye, coğrafi konumu gereği depremlerin sıkça meydana geldiği bir ülkedir. Örneğin, Kuzey Anadolu Fay Hattının üzerinde olduğu bölgeler, tarih boyunca ciddi derecede depremleri yaşadığı için toplumda derin izler bırakmıştır (Gündoğan ve Karimzadeh, 2019, s. 79). Özellikle 1999 yılında yaşanan Gölcük Depremi, Türkiye'de stratejik iletişim, afet yönetimi ve kriz iletişimi açısından bir dönüm noktası olmuştur. Yaklaşık 17.000 kişinin hayatını kaybettiği bu olay, Türkiye'nin afet yönetimi kapasitesini yeniden değerlendirmesine neden olmuş ve bu alanda çeşitli reformlar gerçekleştirilmiştir (Kaya ve Şahan, 2023, s. 1909). Bu süreçte stratejik iletişimin önemi daha belirginleşmiş; afet sonrası hızlı, şeffaf ve etkili bilgi paylaşımının toplumun toparlanma sürecinde önemli olduğu anlaşılmıştır.

Deprem gibi büyük ölçekli afetlerde, kamuoyunun doğru bilgilendirilmesi ve yanlış bilgilerin yayılmasının engellenmesi, kriz yönetiminin başarıyla yürütülmesinde oldukça önemlidir. 6 Şubat 2023 tarihinde Kahramanmaraş merkezli yaşanan depremler, Türkiye'nin 11 ilinde (Kahramanmaraş, Hatay, Adıyaman, Gaziantep, Malatya, Osmaniye, Kilis, Şanlıurfa, Diyarbakır, Adana ve Elâzığ) büyük yıkıma neden olmuş, yüz binlerce insanı doğrudan etkilemiş ve toplumda geniş çaplı bir kriz ortamının çıkmasına yol açmıştır. Bu tür afetlerde, yalnızca fiziksel müdahale yeterli olmamakta, doğru bilgilendirme ve dezenformasyonla mücadele gibi iletişim süreçlerini de etkin bir şekilde yönetebilmek gerekmektedir.

Bu doğrultuda EGM tarafından Kahramanmaraş depremlerinin meydana gelmesiyle birlikte, sosyal medya platformu X (eski adıyla Twitter) üzerinden stratejik iletişim faaliyetleri gerçekleştirilmiştir. Nitel araştırma yöntemlerinden betimsel analiz ile gerçekleştirilen bu çalışmada; EGM'nin önleyici tedbirleri ve yardım çalışmaları hakkında kamuoyunu bilgilendirilmesi, yanlış ve provokatif bilgilerin düzeltilmesi ve yayılmasının engellenmesi ile dijital dolandırıcılıklara karşı korunması amacıyla 6 Şubat-31 Mart 2023 tarihleri arasında Kahramanmaraş depremlerine yönelik X platformunda dolaşıma sunduğu 161 ileti incelenmiştir. Çalışma; depremlerin meydana geldiği tarihten itibaren EGM'nin X platformunda paylaştığı iletileri, stratejik iletişim yönetiminin ve kriz iletişimi faaliyetleri kapsamında analiz etmeyi ve bu süreçteki önemini ortaya koymayı hedeflemektedir.

EGM'nin Kahramanmaraş depremlerine ilişkin X platformunda kesintisiz sürdürdüğü sanal kamusal alan etkileşimi, stratejik iletişim yönetimi ve kriz iletişimi açısından önemli bir vaka çalışması niteliği taşımaktadır. Bu çalışma, dijital medya araçlarının ve sosyal medya platformlarının kriz dönemlerinde ne kadar etkili bir iletişim aracı olduğunu ve kolluk kuvvetlerinin bu tür durumlarda, stratejik iletişim yöntemlerini nasıl kullanabileceğine dair önemli veriler sunmaktadır. Elde edilen bulgular, gelecekte benzer kriz durumlarında iletişim stratejilerinin uygulanmasına yönelik değerli öneriler sağlamaktadır.

Stratejik İletişim

Khang ve diğerleri (2012, s. 279) tarafından yapılan bir çalışmada 436 makale incelenmiş ve buradan hareketle iletişim alanında sıklıkla kullanılan çeşitli teorik kalıpların belirlenmesi amaçlanmıştır. Dijitalleşme sürecine bağlı olarak en sık çalışılan teoriler; sosyal bilgi işleme teorisi, kullanımlar ve doyumlar teorisi, ilişki yönetimi teorisi, gündem belirleme veya çerçeveleme teorisi ve inovasyonun yayılması teorisidir. Bu bağlamda strateji, iletişim çalışmalarında çokça tartışılan ancak ihmal edilen bir kavramdır. Bunun nedenlerinden biri, stratejik iletişimin en olumsuz anlamıyla ikna ile ilişkilendirilebilmesidir. Bu sebeple, stratejik iletişim çeşitli uygulama alanlarındaki pratik uygulamasının ötesine uzanır. Bilhassa iletişimin toplumun merkezinde yer alması her türlü organizasyonda yürütüldüğü güç ve çıkar çerçeveleri üzerine düşünmeyi gerektirir. Bunlara; şirketler, kâr amacı gütmeyen kuruluşlar, aktivist gruplar, siyasi partiler veya hareketler, hükûmet kuruluşları ve günümüz kültürünün karma yapısını oluşturan her türlü aktör dahildir (Holtzhausen ve Zerfass, 2015, s.1).

Ortaya çıktığı ilk yıllarda salt ulusal hükûmetler ve ordu alanındaki iletişim programları için kullanılan (Farwell, 2012, s. 143; Paul, 2011, s. 129) stratejik iletişim; günümüzde halkla ilişkiler, pazarlama ve finansal iletişim, sağlık iletişimi, kamu diplomasisi ve benzeri alanları kapsayan çeşitli hedef odaklı iletişim faaliyetlerini içeren bir şemsiye kavramdır. Stratejik iletişim, organizasyonların hedef kitleleriyle etkileşimlerini etkili bir şekilde yönetmelerini sağlamak amacıyla gerçekleştirilen tüm faaliyetleri kapsamaktadır. Stratejik iletişim çalışmalarının neden gerekli olduğuna dair yapılan bir çalışmada gerekçeler dört ana başlık altında sunulmuştur: Geleneksel iletişim faaliyetleri arasında ayrım yapmada yaşanan sorunlar, farklı iletişim biçimleri arasında ayrım yapmayı giderek zorlaştıran teknolojideki değişiklikler, kuruluşların paydaşlarla doğrudan iletişim kurmak için kullandıkları yöntemlerdeki artış ve amaçlı iletişimin "*kuruluşlar tarafından gerçekleştirilen iletişimin temel hedefi"* olmasıdır (Hallahan vd., 2007, s. 10).. ABD'de birçok üniversite var olan stratejik iletişim alanında yürüttüğü programların müfredatını değiştirmiş ve halkla ilişkiler ve reklamcılık ile ilgili dersleri sürece dahil etmiştir. Avrupa'da stratejik iletişim, genellikle her türlü organizas-

yon için entegre iletişim alanına yönelik bir yönetimsel yaklaşımı belirtmek için kullanılan bir kavramdır. Asya ve Avustralya'da stratejik iletişim; mesleki alanda, eğitimde ve edebiyatta kullanılan bir kavramdır (Mahoney, 2013, s. 2).

Stratejik iletişim; alan yazınında olumsuz veya kötü itibarlı olduğu için kullanılmayan kelimeleri karşılamak için tercih edilen bir terim değildir. Tam aksine tamamlayıcı iç görüler sunan ve disiplinler arası araştırmalar için yeni alanlar açan iletişim sürecine odaklananmayı anlatmak için kullanılır. (Holtzhausen ve Zerfass, 2015, s. 3). Stratejik iletişim süreci; organizasyonların bilgi akışını kontrol etmeleri, kamuoyunu etkilemeleri ve itibarlarını yönetmeleri için kritik bir rol oynamaktadır. O'Rourke ve Smith (2023, s. 89), stratejik iletişimi; organizasyonların belirli hedeflere ulaşmak için tasarladıkları planlı ve düzenli iletişim süreçleri, Hallahan ve diğerleri (2007, s. 1) ise organizasyonların misyonunu genişletmek için amaçlı iletişim sağlanması olarak tanımlamaktadır.

Bu nedenle stratejik iletişim yalnızca bilgi paylaşımını değil, organizasyonların kamuoyuyla olan etkileşimlerini de kapsamaktadır. Stratejik iletişim yönetiminin temel unsurları arasında; hedef belirleme, planlama, uygulama ve değerlendirme süreçleri yer almaktadır. Dijital, geleneksel ve sosyal medya kampanyaları gibi kamuya açık faaliyetlere odaklanmanın yanı sıra stratejik iletişim şu süreçleri içerir:

- E-posta kampanyaları, şirket içi sosyal medya kanalları ve şirket kültürünü oluşturan veya kurumsal değişimi yönlendiren etkinlikler gibi kurumlar içindeki personeli hedefleyen dahili iletişim,
- Çevrimiçi ve sosyal medya reklamları da dahil olmak üzere ürün veya hizmetleri tanıtmak veya satmak için kullanılan entegre pazarlama iletişimleri ve reklam kampanyaları,
- Topluluk katılımı, geri bildirim ve destek almak için insanlarla veya gruplarla bağlantı kurmak için danışma oturumları, haber bültenleri ve anketler,
- Kriz iletişimi: Acil durumlara veya beklenmeyen olaylara yanıt olarak ifadeler yayınlamak ve etkilenen topluluklarla etkileşim kurmak.

Bunlar, kuruluşun itibarını güçlendirmeyi amaçlar ve ayrıca belirli alanlarda kapasite ve destek oluşturabilir (Ward, 2011, s.34).

Stratejik iletişim, organizasyonel faaliyetlerin zaman ve paydaş uyumu içerisinde yürütülmesini öncelikli olarak öne sürdüğü için kurumsal başarılar üzerinde doğrudan etkili olan bir unsur olarak kabul edilmektedir. Bu yaklaşım, yalnızca mesajların kamuya iletilmesini değil, bunların anlamlı ve bütüncül bir çerçevede sunulmasını kapsamaktadır. Stratejik iletişim, mesajların nasıl planlandığı, ne zaman, hangi kanallardan kimlere iletilmesi gerektiği ve iletilen mesajların kamuoyunda nasıl bir etki oluşturduğu ile yakından ilgilidir (Balonas, Ruão ve Carrillo, 2021, s. 78). Bu itibarla organizasyona ilişkin herhangi bir olay ya da mesele mey-

dana gelmeden önce proaktif tedbirler planlanmakta, gerçekleşme esnasında kriz iletişimi bağlamında bilgilendirme ve düzeltme odaklı iletişim sürdürülmektedir. Kriz sona erdiğinde geri dönüşümlerin katkılarını yönetişim süreçlerine katmak için gerekli çalışmalar yapılmaktadır.

Cornelissen (2017, s. 115), stratejik iletişimi, kurumsal ilişkilerdeki önemini vurgulayarak, organizasyonların iç ve dış paydaşlarıyla dengeli bir iletişim kurmalarını sağlayan dinamik bir süreç olarak ifade etmektedir. Bu dinamik yapı, organizasyonların çevreleriyle uyumlu bir şekilde hareket etmelerini ve kriz anlarında etkili iletişim kurmalarını da kolaylaştırmaktadır. Kriz anlarında sürdürülen stratejik iletişim, organizasyonların itibarlarını koruyup kamu güvenini sağlamak açısından kritik bir öneme sahiptir. Büyük çaplı krizlere sebep olan afetler toplum üzerinde derin etkiler bırakan olaylardır. Bu tür durumlarda stratejik iletişim yönetimi, organizasyonların hızlı ve doğru bilgi akışını sağlamaları için kılavuzluk etmektedir.

Afet anında yürütülen stratejik iletişimin, toplumun ihtiyaçlarına uygun şekilde yapılandırılması ve zamanında doğru bilgi akışı sağlayan stratejileri içermesi gerekmektedir (O'Connor, 2019, s. 84). Bunun temel nedeni afetlere ilişkin yayılabilecek bilgi kirliliğinin önlenmesi ve toplumun kurumlara ve çalışmalarına olan güven duygusunun pekiştirilmesidir. Afet anlarında sosyal medya ve dijital iletişim araçları, bilgi akışını sağlamak için önemli bir enstürmandır (Jin ve Austin, 2022, s. 389). Bilhassa sosyal medya, kullanıcılarına afet sonrası bilgi paylaşımında hızlı ve etkili bir platform sunmaktadır. Bunlar, organizasyonların anlık güncellemeler yapabilmesine ve kamuoyunu bilgilendirmesine olanak tanımaktadır.

Büyük krizlerde görev alan kurumların haber aktardığı ve bilgi paylaştığı iletişim kanalları arasında sosyal medya öncelikli olarak görülmektedir. Kurumların halkla doğrudan etkileşim sağladığı sosyal medya platformlarının bulunduğu dijital mecra bu resmiyet kazanan nitelendirme nedeniyle sanal kamusal alan şeklinde değerlendirilmektedir (Kaplan ve Haenlein, 2010, s. 64). Genel bir ifadeyle sanal kamusal alan; sosyal medya platformlarıyla haber ve görüntü aktarımına elverişli tüm uygulamaları kapsayan, bireylerin dijital ortamda etkileşimde bulunduğu ve toplumsal konular üzerine görüş alışverişi yaptığı bir mecra olarak görülmektedir. Dijitalleşmenin yaygınlaşması ve özellikle sosyal medyanın gün geçtikçe etki alanını arttırması, stratejik iletişimde yeni bir dönemin kapılarını açmıştır (Papacharissi, 2015, s. 114). Bundan dolayı sanal kamusal alan, beklenen ve istenen düzeyde olmasa bile, dijital dünyanın merkeziyetsiz ve sınırsız doğasını olay ve konu odaklı görece sınırlandıran ve hesap verilebilir kılan bir dijital anlayışa işaret etmektedir.

Diğer taraftan sanal kamusal alan hem bireylerin hem de kurumların bilgiye hızlı erişimini ve etkileşimde bulunmalarını kolaylaştırırken kriz anlarında toplumun kolektif tepkiler vermesine olanak sağlamaktadır. Schwarz, Seeger,ve Auer (2016, s. 9), sosyal medyanın kriz durumlarında hızlı bilgi paylaşımının yanı sıra,

bireylerin olaylara dair duygusal tepkilerini organize ederek kamusal bir etki alanı oluşturduğunu belirtmektedir. Zira stratejik iletişim, kriz dönemlerinde dijital sosyal medya platformları üzerinden anlık olarak şekillenmekte ve toplumsal algı üzerinde etkili olmaktadır.

Büyük çaplı krizlerde stratejik iletişim, kriz yönetiminin en kritik bileşenlerinden biri olarak kabul edilmektedir. Kriz anında kesintisiz ve doğru bilgi akışının sağlanması, güvenilir iletişim kanallarının korunması ve itibar yönetimi büyük önem taşımaktadır (Heath ve Millar, 2003, s. 75). Kriz anında kamu kurumlarının şeffaf, zamanında ve güvenilir bilgilendirme süreçlerini hayata geçirerek halkın güvenini kazanması gerekmektedir. Kriz sırasında yapılan ilk açıklamalar, kriz yönetiminin başarısını büyük ölçüde etkilediğinden kriz yönetiminin temelini oluşturarak kamuoyunun olaylara bakış açısını şekillendirmektedir.

Sosyal medya, kurumların hedef kitlelerine daha hızlı ve etkili bir şekilde ulaşmasını sağlamakta, toplumun genel bakış açılarını yansıtmaktadır. Sosyal medya, stratejik iletişim için yeni fırsatlar sunmakta ancak bazı riskleri beraberinde getirmektedir. Sosyal medya, kontrolsüz bilgi yayılma riskini artırdığı için organizasyonların stratejik iletişim planlarını sosyal medya dinamiklerine uygun olarak güncellemelerini zorunlu kılmaktadır (Eriksson, 2018, s. 528). Sosyal medya platformları, etkili bir iletişim aracı olmalarının yanı sıra yanlış bilgilerin yayılmasına neden olabilmektedir. Bu sebeple stratejik iletişimde kurumların yerine getirmesi gereken en önemli görevlerden biri; sosyal medya ve diğer dijital iletişim kanallarını proaktif bir şekilde yönetmektir (Ulmer, Sellnow ve Seeger, 2017, s. 81). Bu süreç, yalnızca bilgi paylaşımını değil, kamuoyunun algısını yönlendirme yeteneğini de kapsamaktadır. Kriz anlarında sağlıklı bir iletişim stratejisi geliştirmek; kurumların itibarlarını korumak ve toplumda güven duygusunu pekiştirmek için hayati bir öneme sahiptir.

Kriz İletişimi

İletişim çalışmaları; sağlık iletişimi, siyasî iletişim ve kriz iletişimi gibi çeşitli bağlamları içerir. Sıklıkla kriz iletişimi çalışmalarıyla karıştırılan imaj onarım söylemi, kapsam bakımından kriz iletişimine kıyasla daha sınırlıdır. Kriz iletişimi imaj onarım söylemini içerir, ancak doğa kökenli afetler ve terörizm gibi diğer kriz türleri hakkındaki mesajları da karşılar (Benoit, 2015, s. 305). Genellikle işletme veya kâr amacı gütmeyen kuruluşların merceğinden bakılsa da kriz iletişiminin politikadaki rolü kritiktir (Coombs, 2011, s. 8).

Yukarıda yer verilen bilgilerden hareketle kriz iletişimi, bir organizasyonun karşılaştığı olumsuz olaylar ya da olağanüstü durumlar esnasında bilgi akışını ve kamuoyunu yönetme sürecini ifade etmektedir. Organizasyonların, kriz anlarında halkla iletişim kurma süreçlerini kapsamaktadır. Bunlar, etkili iletişim stratejilerinin geliştirilmesi ve uygulanması ile hem organizasyonun itibarının korunmasına

hem de kamu güveninin sağlanmasına olanak tanımaktadır (Adamu ve Mohamad, 2019, s. 236). Kriz iletişiminin başarılı bir şekilde yürütülmesi için, alan yazınında belirlenen çeşitli tanımlar, büyük çaplı krizlerde organizasyonların alması gereken önlemler, sosyal medyanın rolü, güvenlik açısından iletişim stratejileri ve özellikle kolluk kuvvetlerinin kriz iletişimindeki işlevleri ayrıntılı bir şekilde incelenmelidir.

Kriz iletişimi üzerine yapılan alan yazını incelemeleri, bu alandaki temel tanımları ve yaklaşımları ortaya koymaktadır. Coombs (2014, s. 42), kriz iletişimini; organizasyonun bir kriz sırasında bilgi yönetimi ve kamuoyunu bilgilendirme süreci olarak tanımlamaktadır. Bu süreç, kriz anında organizasyonların mesajlarını etkili bir şekilde iletmesi ve halkın güvenini sağlama amacı taşımaktadır. Sellnow ve Seeger (2013, s. 12) ise kriz iletişimini, bir olayın olumsuz etkilerini azaltmak için bilgi sağlama ve halkın endişelerini giderme süreci olarak açıklamaktadır. Bu tanımlar, kriz anlarında iletişim stratejilerinin geliştirilmesi ve uygulanması gerekliliğini vurgulamaktadır.

Bunun yanında, kriz iletişiminin kapsamını genişleten diğer çalışmalar da iletişim sürecinin şeffaflık, güvenilirlik ve hız gibi unsurlarını öne çıkararak etkili bir kriz yönetimi için kritik unsurları belirlemektedir (Benoit, 1997 s. 178; Wilcox, Cameron ve Reber, 2015, s. 275). İster deprem gibi doğal ister askerî bir saldırı gibi beşerî etkenler yüzünden ortaya çıkmış krizlerde hükûmetin iletişim çabaları, sürecin başarılı bir şekilde yürütülmesi için hayati bir öneme sahiptir. Bu tür çabaların amaçlı ve proaktif olarak geliştirilmesi, bu nedenle stratejik politik iletişime dahil edilmesi önerilmektedir. Temel düzeyde, çoğu bilim insanı krizleri; kriz öncesi, kriz ve kriz sonrası olmak üzere üç başlık altında değerlendirir. (Coombs, 2012, s. 175). Bununla birlikte Coombs (2011, s. 214), siyasî kriz iletişimi ile kurumsal kriz iletişimi arasında benzerlikler olmasına rağmen, büyük farklılıkların kriz yöneticileri, kriz türleri, kriz kısıtlamaları ve başarı göstergelerini tanımlayan şeyler olduğunu ileri sürmüştür.

Büyük çaplı krizler, organizasyonların iletişim stratejilerini gözden geçirmesini zorunlu kılmaktadır. Kriz durumlarında organizasyonların alması gereken tedbirler arasında yer alan proaktif planlama, zamanında bilgilendirme ve çoklu iletişim kanallarının stratejik ve etkili bir biçimde kullanımı, kriz yönetim süreçlerinde hayati bir öneme sahiptir. Proaktif planlama, olası kriz senaryolarının önceden belirlenmesini ve bunlara yönelik hazırlık yapılmasını içermektedir. Heath ve Millar (2003, s. 17), kriz anlarına hazırlıklı olmanın; organizasyonların itibarını korumada önemli bir rol oynadığını ifade etmektedir. Kriz anında hızlı ve doğru bilgi sağlanması, kamuoyunun güveninin korunması açısından son derece önemlidir.

Kriz iletişimi, acil durum yönetimi ile doğrudan ilişkili bir süreçtir. Acil durum yönetimi kapsamında, halkın güvenliği ve refahı için alınacak önlemlerin açık ve anlaşılır bir dille kamuoyuna iletilmesi gereklidir (Macias, Hilyard, ve Freimuth, 2009, s. 18). Organizasyonlar, kriz anlarında karşılaştıkları riskleri en aza indir-

mek için önceden hazırladıkları planları hayata geçirerek kamuoyunun güvenini sağlamak amacıyla bilgi paylaşımı gerçekleştirmektedir. Bu süreçte kriz iletişimi, sadece organizasyonların değil, kamu kurumlarının ve yerel yönetimlerin de kritik rol oynadığı bir alan hâline gelmektedir. Kamu kurumlarının, kriz iletişimi süreçlerinde şeffaflık ve güvenilirlik ilkelerine dayalı stratejiler geliştirerek, halkın doğru ve zamanında bilgiye erişimini sağlamaya özen göstermesi gereklidir.

Coombs (2012, s. 171), kurumların etkili kriz iletişimi stratejilerini, mesajların zamanında iletilmesiyle gerçekleştirilebileceğini vurgulamaktadır. Heath ve O'Hair (2019, s. 16), kriz iletişimini belirsizlik ve tehdit anlarında kurumların alacağı tedbirleri belirlemesi ve iletişim stratejilerini oluşturulması şeklinde açıklamaktadır. Kriz anlarında etkili iletişim sağlamak, yalnızca bilgi akışını değil, kamuoyunun güvenini kazanmayı da gerektirmektedir.

Sosyal medya anlık iletişim olanaklarıyla, kriz anında doğru bilginin edinilmesi ve etkileşim sağlanması amacıyla kullanılan en etkili kanal olarak görülmektedir (Fearn, 2016, s. 45). Sosyal medya platformları, kriz anlarında organizasyonların hızlı bilgilendirme yapmalarına olanak tanıyarak kamuoyunun doğru bilgiye erişimini sağlamaktadır. Bu platformlar halkla doğrudan ve hızlı iletişim kurulmasına olanak sağlarken, aynı zamanda kurumlara kriz iletişim stratejilerini uygulama esnekliği kazandırmaktadır (Apuke ve Tunca, 2018, s. 202). Sosyal medya platformlarında yanlış bilgilerin yayılması, kriz anlarında ciddi sorunlara yol açabilmektedir. (Alexander, 2014, s. 719). Bundan dolayı kurumlar, kriz anında sosyal medya üzerinden aktif iletişim sağlayarak ve yayılan yanlış bilgileri düzelterek kamuoyunun doğru bilgiye erişimini sağlamak için çaba göstermektedirler.

Kriz anlarında doğru bilgilendirme ve etkili iletişim stratejileri, krizlerin olumsuz etkilerini azaltmak ve toplumsal dayanışmayı güçlendirmek için gereklidir. Sosyal medya, kamuoyunun tepkilerini belirleme ve bu tepkilere anında yanıt verme imkânı sunan önemli bir mecra olarak değerlendirilmektedir (Morrow, 2019, s. 4). Günümüzde sosyal medya üzerinden gerçekleştirilen kriz iletişimi, kamuoyunun endişelerini giderme konusunda en etkili yöntemlerden biri olarak öne çıkmakta ve dezenformasyonun önüne geçilmesinde kritik bir rol oynamaktadır. Kriz iletişiminde sosyal medya kullanımı, özel ve kamu kurumları kadar kolluk kuvvetleri için de hayati bir öneme sahiptir.

Kolluk kuvvetlerinin kriz iletişiminde etkin bir şekilde yer alması, toplum güvenliğinin korunması açısından önemlidir. Bu bağlamda, açık ve şeffaf bilgilendirme, sosyal medya platformlarının stratejik kullanımı ve toplumsal iş birliği gibi unsurlar, kriz yönetimi süreçlerinde hayati bir önem taşımaktadır. Kolluk kuvvetlerinin, kriz anlarında kamuoyuna doğru ve net bilgi sunması hem halkın güvenini artırmakta hem de yanlış bilgi yayılımını engelleyerek sosyal kargaşayı önlemektedir (Steele ve Blau, 2023, s. 523). Sosyal medya platformları aracılığıyla kriz anında hızlı ve etkili bir bilgilendirme yapmak, modern kriz iletişiminde önemli bir strateji hâline gelmiştir.

Kolluk kuvvetlerinin sosyal medya platformlarını kriz iletişiminin merkezine koyarak kamuoyuyla etkileşim kurması, yalnızca kriz anında bilgilendirme değil, toplumun kriz sonrası toparlanma sürecine katkıda bulunmasını da sağlamaktadır. Sosyal medya araçlarının bu şekilde stratejik kullanımı, kolluk kuvvetlerinin kriz anlarında güvenli bilgi akışı sağlama ve kamuoyunun güvenini artırma noktasında en etkili yöntemlerinden biri hâline gelmiştir (Jungblut, Kümpel ve Steer, 2024, s. 4651). Kolluk kuvvetlerinin hızlı bilgilendirme ve toplumsal iş birliği stratejilerinde sosyal medya platformları aracılık edebilmekte, güvenlik odaklı kriz iletişimini yönetmelerine katkı sağlamaktadır. Bu bağlamda EGM'nin uyguladığı stratejik iletişim kapsamında gerçekleştirdiği sosyal medya etkinliği, kriz anında kamu güvenliği sağlanması ve toplumu doğru bilgilendirme açısından önemli bir örnektir.

Sosyal Medya Platformları

Kurumların hedef kitlelerine ve kurumsal amaçlarına ulaşmalarında dijital kanallar önemi rol oynamaktadır. Özellikle sosyal medya platformları, etkileşimli doğasıyla kurumlar için vazgeçilmez ve sürdürülmesi gereken yeni iletişim biçimini ortaya çıkarmıştır. Stratejik iletişim yönetimi, hedef kitleyle etkili bir iletişim kurmayı amaçlarken kriz iletişimi bu süreçte kurumların itibarlarını korumayı hedeflemektedir. Sosyal medya platformları, kurumların her iki alanda hızla değişen dinamiklere uyum sağlamaları ve mesajlarını doğru şekilde iletilmesine katkı sağlamaktadır. (Rettberg, 2009, s. 455). Sosyal medya platformları; iletilerin dağıtılmasına, tekrar yayınlanmasına ve beğenilmesine olanak sağlayarak stratejik iletişim yönetimi uygulayıcılarının hedef kitlelerinin tepkilerini anlamalarına ve etkin iletişim sağlamalarına yardımcı olmaktadır (Karsak, Altuntaş ve Demren, 2018, s. 10).

Sosyal medya platformları, stratejik iletişimde etkili bir araç olarak öne çıkmaktadır. X'in yanı sıra Facebook, Instagram ve Linkedin platformları, kurumların geri bildirimlerine hızlı bir şekilde yanıt vermesine, içeriklerini hedef kitleye doğrudan iletmelerine ve marka imajına katkı sağlamaktadır (Lipschultz, 2023, s. 328). Sosyal medya platformları aynı zamanda verilerin toplanmasına olanak tanımakta ve bunlar, iletişim stratejilerinin daha etkili hâle getirilmesinde kullanılmaktadır.

Kriz iletişiminde sosyal medya platformlarının kullanımı, kurumların toplumsal sorumluluklarını yerine getirmelerine ve şeffaflık oluşturmalarına yardımcı olur. Kriz anlarında, bilgi hızla yayılabileceği için sosyal medya platformları, doğru ve zamanında bilgi sunma açısından kritik bir işlevi yerine getirmektedir. Sosyal medya platformları, krizlerin yayıldığı bir ortamda, kamuoyunun tepkilerini hızlı bir şekilde gözlemlemek ve anında yanıt vermek için etkin bir araçtır. Sosyal medya iletilerinin geniş kitlelere anlık olarak ulaşabilmesi, kriz anlarında

kurumların itibar yönetimini zorlaştırabilmektedir (Liu, Austin ve Jin, 2011, s. 347). Bir kriz durumu ortaya çıktığında bilgi kirliliği ve yanlış aktarımlar yayılabilmektedir. Bu nedenle kriz iletişimi sürecinde sosyal medya platformlarının doğru şekilde yönetilmesi büyük bir önem taşımaktadır. Etkili bir kriz yönetimi için, sosyal medyada doğru mesajların ve açıklamaların yapılması, yanlış bilgi yayılmasını önleyebilmekte ve kurumun imajını koruyabilmektedir.

Sosyal medya platformları kriz anlarında geleneksel iletişim yöntemlerine göre daha hızlı ve etkili bir iletişim ortamı sunmasının yanında kurumların gerçek zamanlı olarak doğru bilgi aktarmasını sağlayarak kriz yönetimini daha verimli hâle getirmektedir. Sosyal medya platformları, anında mesajlarla kamuoyuna açıklama yapma, krizle ilgili gelişmeleri aktarma ve izleyici geri bildirimlerine hızla yanıt verme imkânı tanımaktadır. Bu özellik, kurumların kriz sırasında saygınlığını koruyabilmelerine ve kayıplarını azaltmalarına olanak tanımaktadır (Lovejoy ve Saxton, 2012, s. 399). Sosyal medya platformlarının sunduğu anlık etkileşim, kriz iletişiminin başarısını doğrudan etkileyen faktörlerden biridir. Bu sebeple sosyal medya platformları kurumların kriz süreçlerinde toplumsal sorumluluklarını yerine getirmelerinde ve şeffaflıklarını artırmalarında etkilidir.

Emniyet Genel Müdürlüğünün Stratejik İletişim Yöntemleri

EGM, kamu güvenliğini sağlama amacıyla stratejik iletişim yöntemlerini etkili bir şekilde kullanmaktadır. EGM, stratejik iletişim yaklaşımları sayesinde hedef kitle ile olan bağlarını güçlendirmekle yetinmeyerek kriz anlarında da kamuoyunu bilgilendirerek etkili bir iletişim süreci yürütmektedir. Bu amaç için hızlı ve doğru bilgi akışını sağlamak amacıyla yazılı ve görsel tüm medya bileşenleri kullanılmaktadır. Günümüzde çoklu sanal ortamların yoğun kullanımı EGM'nin stratejik iletişim faaliyetlerine yeni bir boyut kazandırmıştır (Çakmak, 2023, s. 181). EGM ve bağlı merkez teşkilatı ile il emniyet müdürlüklerinin resmî internet siteleri, haberleşme uygulamaları ve sosyal medya platformları önemli stratejik iletişim kanallarına dönüşmüştür.

EGM'nin yoğun olarak kullandığı dijital mecralar sanal kamusal alan niteliği taşımaktadır. Bir başka ifade ile EGM gerçek yaşamda uyguladığı kamusal görevleri, sanal ortamlara taşımış ve bu ortamlara özgü yeni bir faaliyet alanı oluşturmuştur. EGM'nin görece daha fazla içerik paylaştığı sosyal medya platformları; kurumsal stratejik iletişim bağlamında önemli ve sürekli izlenen dijital ortamlara evrilmiştir (Su, 2016, s. 18). Sosyal medya üzerinden halkla kurulan etkileşim, EGM'nin şeffaflık ilkesine katkı sağlarken toplumun güvenini de artırmaktadır. EGM, sosyal medya aracılığıyla halkın geri bildirimlerini değerlendirerek stratejilerini sürekli olarak güncellemektedir. Böylelikle sanal kamusal alanlar hem bilgilendirme hem de halkla etkileşim açısından önemli bir platform hâline gelmektedir.

EGM'nin sanal kamusal alan faaliyetleri, gerçek yaşamda meydana gelen olaylarla bağlantılıdır. Bu nedenle, her iki ortamda da güvenlik meselelerinin takibi, proaktif ve reaktif stratejik iletişim faaliyetleri kapsamında gerçekleştirilmektedir. Sosyal medya platformları, bilgi paylaşımı ve halkın tepkilerinin tespit edilmesi açısından kritik bir rol oynamaktadır (Shahbaznezhad, Dolan ve Rashidirad, 2021, s. 54). EGM, fazla takipçisi bulunan Twitter, Facebook ve Instagram platformlarını etkin bir şekilde kullanarak halkla etkileşimi artırmakta ve acil durumlarda anlık güncellemeler yapmaktadır.

Proaktif stratejik iletişim, EGM'nin uzun vadeli hedeflerine ulaşmak için planlı sosyal medya çalışmaları ile halkla iletişim kurmasını içermektedir. EGM, güvenlik sorunlarına yönelik bilinçlendirme çalışmaları düzenleyerek toplumu güvenlik önlemleri hakkında bilgilendirmekte ve halkın duyarlılığını artırmayı hedeflemektedir (Hu ve Lovrich, 2019, s. 655). Bu çalışmalar toplumun güvenlik bilincini artırmakta ve potansiyel tehlikelere karşı hazırlıklı olmalarını sağlamaktadır. Trafik, asayiş, siber güvenlik ile uyuşturucu maddeler ve kitlesel eylemlere yönelik mücadele konularında yapılan sosyal medya çalışmaları, EGM'nin proaktif iletişim stratejilerinin somut örnekleridir.

EGM kriz anlarında reaktif stratejik iletişime başlamakta ve halkın bilgi ihtiyacını karşılamak amacıyla hızlı bir kriz iletişim süreci yürütmektedir. Bu süreçte EGM'nin öncelikli hedefi, kriz durumlarında halkı doğru bir şekilde bilgilendirmek ve yanlış bilgilerin yayılmasını önlemektir. Sosyal medya kanalları üzerinden aktif bir şekilde yapılan güncellemelerle, EGM toplumun krizle ilgili endişelerini azaltmayı ve güvenliği sağlamak için gerekli bilgileri paylaşmayı amaçlamaktadır. Zamanında yapılan açıklamalar ve doğru bilgi aktarımı, kriz dönemlerinde halkın güven duygusunu pekiştirmekte ve kamuoyunun bilgi ihtiyacını karşılayarak olası yanlış anlaşılmaların önüne geçmektedir (Pang, 2013, s. 312). Bu bağlamda sosyal medya platformları, reaktif stratejik iletişimin en önemli unsurlarından biri olarak öne çıkmakta, halkla anlık ve doğru bilgi paylaşımı sağlanmaktadır.

Büyük çaplı krizler reaktif stratejik iletişimi gerektirmektedir. Doğal afetler, kitlesel eylemler, terör saldırıları ve kamuoyunu derinden etkileyen kapsamlı olaylar EGM'nin görev alanına giren büyük çaplı krizlere işaret etmektedir. Büyük çaplı krizlerde EGM sosyal medya aracılığıyla doğru ve hızlı bilgi akışı sağlayarak yanlış bilgilerin yayılmasını engellemeye çalışmaktadır. Bu kapsamdaki reaktif stratejik iletişim, kamu düzeninin korunması, toplumsal güvenliğin sağlanması ve bilgi kirliliğinin önlenmesine odaklanan bir yaklaşım olarak öne çıkmaktadır (Steyn, 2004, s. 173). Bu çalışmalar sosyal medyada yayılan provokatif paylaşımların ve hesapların tespit edilmesi, sorumlular hakkında yapılan işlemlerin kamuoyu ile paylaşılması olası panik ve kaos ortamlarının önüne geçilmesi açısından büyük önem taşımaktadır.

EGM'nin reaktif stratejik iletişim temelinde büyük çaplı krizlere yönelik önemle takip ettiği diğer önemli bir sorun da sosyal medya dezenformasyonla-

rıdır. Dezenformasyon bilinçli ve kasten üretilen, sosyal medya platformlarında paylaşılan ve yaygınlaştırılan yanlış bilgileri içermektedir (Fallis, 2015, s. 405). Kötü amaçlı ve zarar verici iletilerden oluşmaktadır. Bununla birlikte sosyal medyada paylaşıma sunulan dezenformasyon iletileri, kullanıcılar tarafından tekrar paylaşılarak mezenformasyona evrilmektedir. EGM'nin reaktif stratejik iletişiminde öncelikli olarak değerlendirdiği mezenformasyon, dezenformatik içeriğin yanlış ve yanıltıcı olduğunun farkında olmadan tekrar iletilmesidir (Muhammed ve Mathew, 2022, s. 275). Bu iletiler doğruluğu teyit edilmeden ve yeteri kadar araştırılmadan kasıtsız olarak paylaşılmakta ancak dezenformasyonun yayılmasına yol açmaktadır.

Buna ilaveten EGM'nin büyük çaplı krizlerde özenle takip ettiği diğer ileti döngüsü de malenformasyon içerikli paylaşımlardır. Doğru bilginin zarar vermek amacıyla sosyal medyada paylaşılması malenformasyonu oluşturur. Gizli ya da özel kalması gereken gerçek bilgi, kötü amaçlı olarak sosyal medyada paylaşılmaktadır (Eskicioğlu, 2023, s. 24). EGM; dezenformasyon, mezenformasyon ve malenformasyon tespitlerinde ilgili hesaplar hakkında gerekli işlemleri yapmakta, bilgi düzeltmeleri de dahil olmak üzere sürdürdüğü çalışmalarını sosyal medya platformlarında paylaşmaktadır. Büyük krizlere ilişkin sosyal medyada dolaşıma sunduğu basın açıklamalarıyla düzenli bilgi akışı sağlamakta kasıtlı, yanlış ve kötücül paylaşımların yayılmasını engellemektedir. Sosyal medya platformları üzerinden yürütülen reaktif stratejik iletişim; anlık güncellemelerle toplumun bilgi ihtiyacını karşılayarak kriz iletişimi sürecine önemli katkılar sağlamaktadır.

EGM'nin kriz iletişimi parametrelerini içeren stratejik iletişim yöntemleri; kamusal tehdit oluşturan sosyal medya paylaşımlarının ve iletilerin yayılma biçimlerinin tespit edilip sorumlular hakkında gerekli çalışmaların yapılarak kamuoyunun aydınlatılması süreçlerini kapsamaktadır. Büyük çaplı krizlerde ihlal edilen sanal kamusal alanın muhafazası için stratejik iletişim çalışmalarını sürdüren EGM, sosyal medya paylaşımlarıyla faaliyetlerini duyurmaktadır. Bu bağlamda EGM'nin stratejik iletişim yöntemlerini uyguladığı ve kriz iletişimi yaklaşımıyla kamuoyunu düzenli olarak bilgilendirdiği X platformu araştırmanın temel çerçevesini oluşturmaktadır.

Yöntem

Bu çalışmanın temel araştırma sorusu, "*EGM'nin 6 Şubat 2023 tarihinde meydana gelen Kahramanmaraş depremleri sonrasında stratejik iletişim yöntemleri ve kriz iletişim çalışmaları bağlamında kamuoyunu bilgilendirmek, kasıtlı ve yanlış bilgilere karşı korumak, proaktif ve reaktif stratejilerle toplumu aydınlatmak için sürdürdüğü faaliyetler nelerdir*?" şeklinde ifade edilebilir. Çalışma, nitel araştırma yöntemlerinden betimsel analiz ile gerçekleştirilmiştir. Betimsel analiz, araştırma bulgularının sistematik bir şekilde incelenmesini ve kategoriler altında or-

ganize edilmesini sağlayarak elde edilen verilerin daha anlaşılır ve yorumlanabilir olmasına katkıda bulunmaktadır (Creswell, 2013, s. 121). Nitel betimsel analiz, özellikle karmaşık sosyal olguların incelenmesinde önemli bir yaklaşım olarak kullanılmaktadır ve araştırmacıların mevcut verilerden anlamlı temalar çıkarmasına olanak tanımaktadır (Miles ve Huberman, 1994, s. 173; Patton, 2002, s. 431). Dezenformasyon, mezenformasyon ve malenformasyon içerikli iletilerin en fazla görüldüğü alan dijital mecra olduğu için çalışmanın evrenini sosyal medya oluşturmaktadır. EGM' nin stratejik iletişim çalışmalarında ve kriz yönetiminde öncelikli olarak tercih ettiği ve diğer sosyal medya platformlarında paylaşılan iletileri kapsadığı için X araştırmanın örneklemi olarak belirlenmiştir.

Bu çalışmada; Kahramanmaraş depremlerinin meydana geldiği 6 Şubat-31 Mart 2023 tarihleri arasında X platformunda, EGM tarafından dolaşıma sunulan 161 paylaşım, stratejik iletişim yöntemleri bağlamında değerlendirilmektedir. Çalışma, sosyal medya platformu X üzerinden EGM'nin Kahramanmaraş depremleri sonrasında gerçekleştirdiği önleyici tedbirleri ve yardım çalışmaları ile provokatif paylaşımlara ve dijital dolandırıcılığa yönelik sürdürdüğü faaliyetleri yedi farklı başlıkta toplanmıştır. EGM'nin gerçekleştirdiği çalışmalar hakkında kamuoyunu bilgilendirmek, kasıtlı ve yanlış bilgilere karşı korumak, proaktif ve reaktif aktivitelerden toplumu aydınlatmak amacıyla sürdürdüğü faaliyetler, stratejik iletişim yöntemleri ve kriz iletişim çalışmaları kapsamında incelenmiştir.

Bulgular

EGM, Kahramanmaraş depremleri sırasında X platformunu etkin bir şekilde kullanarak hem proaktif hem de reaktif stratejik iletişim yöntemleriyle kriz iletişimi sağlamıştır (Cheng, 2018, s. 59). EGM'nin proaktif stratejik iletişim kapsamında, deprem bölgesine kurtarma çalışmaları ve önleyici faaliyetler için acil olarak takviye personel ulaştırdığı, gıda, giyecek ve sıcak yemek tedarik ettiği X platformundaki etkileşimlerinden anlaşılmaktadır. Asayişin ve kamu düzeninin sağlanmasına yönelik çalışmalarını reaktif stratejik iletişim çerçevesinde sürdürerek X platformunda basın açıklaması teması ile paylaşarak kamuoyunu bilgilendirdiği gözlenmektedir.

Proaktif İletişim Stratejisinin Uygulanması

EGM' nin X platformunda Kahramanmaraş depremlerine yönelik paylaşımlarının etki düzeyi Tablo 1'de belirtildiği gibi asayiş olayları, basın açıklamaları, deprem bölgesinde bulunan personel sayısı, kurtarma faaliyetleri, mobil mutfak ve sıcak yemek dağıtımı, depremzede aile ve çocuklara sosyal destek ile gıda ve giyecek yardımı olmak üzere yedi ayrı başlık altında 161 gönderi incelenmiştir. Tablo 1'de EGM'nin X platformunda Kahramanmaraş depremlerine yönelik paylaşımlarının etki düzeyine yer verilmiştir.

Tablo 1. EGM' nin X Platformunda Kahramanmaraş Depremlerine Yönelik Paylaşımların Etki Düzeyi

TEMA	GÖNDERİ SAYISI	GÖRÜNTÜLEME	YENİDEN YAYINLAMA	BEĞENİ	YORUM
Depremzede Aile ve Çocuklara Sosyal Destek	70	10.740.604	22.931	201.220	1.940
Kurtarma Faaliyetleri	34	9.000.700	21.952	158.030	2.201
Asayiş Olayı	15	2.576.100	3.889	33.473	413
Mobil Mutfak ve Sıcak Yemek Dağıtımı	14	2.853.700	6.465	40.600	469
Gıda ve Giyecek Yardımı	11	1.549.200	3.720	28.000	294
Deprem Bölgesi Personel Sayısı	9	2.458.000	5.506	41.400	733
Basın Açıklaması	8	2.787.800	7.248	27.185	909

(Tablo 1 Yazar tarafından oluşturulmuştur.)

EGM'nin X platformunda dolaşıma sunduğu "depremzede aile ve çocuklara sosyal destek" ile "kurtarma faaliyetleri" temalarının beğeni, tekrar yayınlama ve yorumlanma sayısının diğer temalara göre daha çok dolaşımda kaldığı Tablo 1'de görülmektedir. Etkileşimin sıklığı, EGM'nin faaliyetlerinin yakından gözlemlendiğine işaret etmektedir. Gönderi sayısı yüksek olan diğer temalar sırasıyla "asayiş olayı", "mobil mutfak ve sıcak yemek dağıtımı", "gıda ve yiyecek yardımı", "deprem bölgesi personel sayısı" ve "basın açıklaması"dır. Belirlenen temaların X platformunda yüksek oranda yeniden yayınlanması, beğeni oranı ve yapılan yorum sayısı dikkate alındığında EGM'nin Kahramanmaraş depremleri sonrasında stratejik iletişim kapsamında proaktif olarak gerçekleştirdiği önleyici tedbirlerin ve yardım çalışmalarının kamuoyunda karşılık bulduğu ifade edilebilir.

Reaktif İletişim Stratejisinin Uygulanması

EGM'nin deprem bölgesinde X platformu üzerinden asayiş olayları ve basın açıklamaları olmak üzere iki başlık altında faaliyetlerini gerçekleştirdiği görülmektedir. Asayişe müessir olaylarda EGM'nin paylaştığı 15 gönderi takipçiler tarafından yüksek oranda görüntüleme ve beğeni sayısına ulaşmıştır (Bkz. Tablo 1). EGM'nin deprem bölgesinde gerçekleştirdiği asayişe ilişkin uygulamalarının

sosyal medya aracılığıyla halka aktarılması ve bahsi geçen paylaşımların etkileşim yüksekliğinin EGM'nin kurumsal imajını güçlendirmesine katkı sağladığı söylenebilir.

EGM'nin reaktif iletişim stratejisi bağlamında en fazla dikkat çeken teması "basın açıklaması" başlığı altında Tablo 2'de yer almaktadır. 6 Şubat-31 Mart 2023 tarihleri arasında EGM, özel olarak hazırlanan basın açıklaması başlığı ile sekiz gönderi paylaşmıştır. Gönderiler, Kahramanmaraş depremlerine yönelik provokatif paylaşımlar ile dijital dolandırıcılık faaliyetlerine ilişkin basın açıklamalarını içermektedir. Basın açıklamalarında "*EGM Siber Suçlarla Mücadele Daire Başkanlığınca kanunların verdiği yetki çerçevesinde suç ve suçlularla mücadele amacıyla internet ortamında 7/24 esasına göre sanal devriye faaliyetleri yürütülmektedir*" ifadeleri kullanılarak EGM'nin reaktif iletişim stratejilerini kararlılıkla sürdürdüğünü betimlemektedir.

Diğer taraftan Siber Suçlarla Mücadele Daire Başkanlığı adının basın açıklamasında yer alması, EGM tarafından gerçekleştirilen faaliyetlerin ciddiyetini ve kesintisizliğini ortaya koymaktadır. EGM'nin yetki devri kapsamında yürüttüğü bu faaliyetlerin, toplumsal güvenin inşasında da önemli rol oynama potansiyeli bulunmaktadır.

X platformunda yayınlanan basın açıklamalarında üzerinde önemle durulan başka bir husus sanal devriye faaliyetleridir. Aralıksız olarak sürdürülen bu görev, gerçekleşmekte olan ya da gerçekleşmiş suçlarla etkin mücadeleyi kapsamaktadır. (Hughes ve Love, 2004, s. 609) EGM, Kahramanmaraş depremleri odaklı yasadışılıkları, sanal kamusal alan suçu bağlamında değerlendirerek takip etmektedir. Bu yaklaşım, EGM'nin yalnızca gerçek dünyada işlenen suçlarla değil, dijital ortamdaki suçlar konusunda da yetkin olduğunu ve bu alandaki mücadelesini kararlılıkla sürdürdüğünü göstermektedir. X platformu üzerinden bu yetki ve kabiliyetlerini kamuoyuna duyurması, EGM'nin paydaş etkileşimine ve kitle iletişim stratejilerine verdiği önemi açıkça ortaya koymaktadır.

Tablo 2. EGM' nin Kahramanmaraş Depremlerine Yönelik Provokatif Paylaşımlar Hakkında Yaptığı İşlemlere İlişkin Basın Açıklamaları

TEMA	**PROVOKATİF PAYLAŞIMLARA YÖNELİK FAALİYETLER**			
BASIN AÇIKLAMASI	Provokatif Paylaşım Yapan Hesaplar	Adli İşlem Yapılan Hesap Yöneticileri	Gözaltına Alınan Hesap Yöneticileri	Tutuklanan Hesap Yöneticileri
8	3.531	1.936	527	99

(Tablo 2 Yazar tarafından oluşturulmuştur.)

EGM'nin X platformunda paylaştığı basın açıklamalarında Kahramanmaraş depremlerine yönelik yayılan provokatif paylaşımları takip ederek uyguladığı hukukî işlemlere yer verilmektedir. Siber Suçlarla Mücadele Daire Başkanlığı görevlileri ve yetki verilen diğer birimler, Tablo 2'de gösterildiği gibi provokatif paylaşım yapan hesapları tespit etmektedir. Hesap yöneticileri hakkında adli işlem başlatılarak adli makamların uygun gördüğü hesap yöneticileri gözaltına alınıp mahkeme kararı ile suçu sabit görülenler tutuklanmaktadır (Bkz. Tablo 2).

Basın açıklamalarında yer verilen provokatif paylaşımlar, kitlesel eylemleri meydana getirebilecek nitelikte yanlış, kasıtlı ve taraflı iletilerden oluşmaktadır. X platformunda Kahramanmaraş depremlerine yönelik kasıtlı olarak yapılan dezenformasyon paylaşımlarının yanı sıra, dezenformatik iletilerin dolaşıma girmesine olanak sağlayan mezenformasyonun yayılmasına da sıklıkla tanık olunmuştur. Bunlardan başka X platformunda Kahramanmaraş depremlerine ilişkin özel olarak kalması gereken doğru bilginin, zarar vermek amacıyla sanal kamusal alana taşıyan malenformasyona da rastlanmıştır. Örneğin, "*Deprem Sonrası Malatya'da Kızılay Bölge Kan Merkezi Tamamıyla Yıkıldı*" başlıklı sosyal medya iletisi dezenformasyon; "*Deprem Sonrasında Atatürk Barajı'nda Çatlaklar Oluştu*" başlıklı ileti mezenformasyon; "*HDP'li Ağrı Patnos Belediyesi'nin Deprem Bölgesine Ulaştırmaya Çalıştığı Yardım Aracına Kaymakamlık Tarafından El Konuldu*" ve "*Afet Bölgesine Giden İş Makinaları Engelleniyor*" başlıklı iletiler ise sosyal medya üzerinden zarar verme amacıyla yayılan malenformasyona örnek olup İletişim Başkanlığının yayımladığı resmî raporda da yer almıştır (İletişim Başkanlığı, 2023).

EGM'nin yetkili birimleri tarafından 6 Şubat-31 Mart 2023 tarihleri arasında gerçekleştirilen çalışmalarda, 3.531 provokatif paylaşım yapan hesabın tespit edilmesi ve sanal suçların sorumlularını belirlemedeki zorluklara rağmen 99 hesap yöneticisinin tutuklanması, EGM'nin bu alandaki kurumsal başarı ve etkinliğini göstermektedir (Tablo 2). Bu tür dijital tehditlerle mücadelede sergilediği performans, EGM'nin siber güvenlik alanındaki yetkinliğini göstermesi bakımından önemlidir.

EGM'nin X platformunda paylaştığı bir diğer önemli husus, Kahramanmaraş depremleri sonrası dijital dolandırıcılık girişimlerine karşı yürütülen çalışmaları ortaya koyan basın açıklamalarıdır. Bu açıklamalarda, özellikle oltalama yöntemiyle gerçekleştirilen resmî kurumlara ait internet sitesi ve sosyal medya dolandırıcılıklarına dikkat çekilmektedir (Tablo 3). EGM'nin bu tür dijital dolandırıcılık faaliyetlerine karşı vatandaşları bilgilendirmek ve farkındalık oluşturmak amacıyla önemli çalışmalar yaptığı anlaşılmaktadır.

Tablo 3. EGM' nin Kahramanmaraş Depremlerine Yönelik Dijital Dolandırıcılık Faaliyetlerine İlişkin Basın Açıklamaları

TEMA	**DİJİTAL DOLANDIRICILIK FAALİYETLERİ**		
BASIN AÇIKLAMASI	Oltalama Yöntemiyle Resmi Kurum İnternet Sitesi Dolandırıcılığı	Oltalama Yöntemiyle Resmi Kurum Sosyal Medya Dolandırıcılığı	Deprem Yardımı Talep Edilerek Dijital Para Dolandırıcılığı
8	81	15	6

(Tablo 3 Yazar tarafından oluşturulmuştur.)

Kahramanmaraş depremleri sonrası yardım talebiyle gerçekleştirilen dijital para dolandırıcılığı girişimleri, bu süreçte tespit edilmiş ve bu durumun afet sonrası dönemde artan bir tehdit unsuru oluşturduğu vurgulanmıştır. EGM'nin sürdürdüğü çalışmalar, oltalama yöntemiyle resmî kurumlara ait internet siteleri ve sosyal medya hesapları üzerinden yapılan dolandırıcılık faaliyetlerini önlemeye yönelik kapsamlı bir müdahaleyi içermektedir. Tablo 3'te belirtildiği üzere, EGM tarafından tespit edilen oltalama yöntemleri arasında 81 sosyal medya, 15 internet sitesi ve 6 dijital para dolandırıcılığı olayı yer almaktadır.

EGM dolandırıcılık girişimlerine karşı uyguladığı reaktif stratejik iletişim faaliyetleriyle hem mağdur edilmek istenen bireylerin korunmasında hem de kamu güvenliğinin sağlanmasında kritik bir işlev üstlenmektedir. Kahramanmaraş depremleri sonrası artan bu tür dijital dolandırıcılık faaliyetlerine yönelik yürütülen stratejik iletişim, toplumda farkındalık oluşturmanın yanı sıra, dijital güvenlik ve bilinç düzeyinin artırılmasına da katkıda bulunmaktadır.

Sonuç

Doğal afetler gibi büyük çaplı krizler, kurumların kriz yönetim yeteneklerini ve iletişim becerilerini sınarken stratejik iletişim, kriz dönemlerinde kamu kurumlarının kamuoyuyla olan ilişkilerini yönetmede hayati bir rol oynamaktadır. Bu bağlamda, Kahramanmaraş depremleri, EGM'nin stratejik iletişim kabiliyetlerini ve dijitalleşen dünyada kriz anındaki iletişim yönetimini değerlendirmek bağlamında anlamlı bir örnek teşkil etmektedir. Bu çalışma, EGM'nin sosyal medya platformu X aracılığıyla gerçekleştirdiği stratejik iletişim faaliyetlerini analiz ederek kriz dönemlerinde sosyal medya kullanımındaki etkinliğini ortaya koymaktadır.

Bu kapsamda, 6 Şubat-31 Mart 2023 tarihleri arasında EGM'nin sosyal medya platformunda gerçekleştirdiği toplam 161 paylaşım, betimsel analiz yöntemi kullanılarak incelenmiştir. İncelenen paylaşımlar, Kahramanmaraş depremleri süresince EGM'nin kriz yönetimi süreçlerine ve bilgi akışını sağlama strateji-

lerine dair önemli veriler sunmaktadır. Analiz edilen içerikler yedi temel tema etrafında gruplandırılmıştır. Bu temalar doğrultusunda gerçekleştirilen analizler, EGM'nin stratejik iletişim sürecinde karşılaştığı zorlukları ve kriz dönemlerinde sosyal medya aracılığıyla kamuoyunu bilgilendirme çabalarının önemini vurgulamaktadır.

EGM'nin kriz döneminde sosyal medya üzerinden gerçekleştirdiği faaliyetler, kriz iletişimi alan yazınında vurgulanan temel ilkelerle büyük ölçüde örtüşmektedir. Coombs (2014, s. 41), kriz anında kamu kurumlarının şeffaf ve güven verici iletişim stratejileri benimsemelerinin, halkın güvenini tazeleyen en önemli faktörlerden biri olduğunu belirtmektedir. EGM'nin deprem sonrası hızlı ve şeffaf bilgi paylaşımını ön planda tutarak asayiş olaylarının da ötesinde "mobil mutfak ve sıcak yemek dağıtımı" "kurtarma çalışmaları" ve "personel sayısı" konularında kamuoyunu bilgilendirmesi, bu bağlamda kriz iletişimi stratejilerini etkin bir biçimde uyguladığına dikkati çekmektedir.

EGM, depremin hemen ardından faaliyetlerine yönelik paylaştığı iletilerle, oluşan kriz hakkında kamuoyunu düzenli olarak bilgilendirmiş ve kurumsal güvenin tesis edilmesine katkı sağlamıştır. Bununla birlikte Veil vd.'lerinin (2011, s. 114) de işaret ettikleri üzere hızlı bilgi paylaşımının yanlış anlamalara yol açabilecek riskler barındırdığı da gözlemlenmiştir. Bu nedenle sosyal medya gibi hızlı ve geniş kitlelere ulaşan platformlarda bilginin doğruluğunu sağlamak, EGM'nin stratejik iletişim perspektifinin temel unsuru olarak nitelendirilmektedir. Bilhassa asayiş olaylarına yönelik hızlı ve bilgilendirici paylaşımları bu görüşü destekler niteliktedir.

Bu çalışma, EGM'nin Kahramanmaraş depremleri süresince X platformu aracılığıyla gerçekleştirdiği kriz iletişim faaliyetlerinin, kamuoyuyla etkin bir etkileşim kurma ve dezenformasyona karşı önleyici tedbirler alma açısından başarılı olduğunu göstermektedir. Öte yandan sosyal medyada bilginin anlık ve kesintiye uğramadan yayılma potansiyeli, dezenformasyonun da benzer bir hızla yayılabileceğini göstermiştir (Dan vd., 2021, s. 645). Bu durum, EGM'nin sosyal medya stratejilerini daha dikkatli ve özenli bir şekilde yürütmesi gerektiğine işaret etmektedir. Dijital medya çağında sosyal medya platformlarının kriz yönetiminde giderek daha fazla önem kazanması, EGM'nin bu alanlardaki yetkinliklerini artırmasını zorunlu kılmaktadır.

EGM'nin stratejik iletişim faaliyetlerinin kapsamlı bir analizi, kriz yönetimi süreçlerinde ve dijital platformlarda stratejik iletişimin etkili bir biçimde uygulanmasına dair dikkate değer bulgular ortaya koymaktadır. Bilhassa yardım talebiyle gerçekleştirilen dijital para dolandırıcılığı girişimlerine yönelik EGM'nin halkı doğru bilgilendirme çalışmaları ve basın açıklamaları yoluyla yanlış bilgilendirmeleri önleme çabaları kriz anında anlaşılmamakta, stratejik iletişim faaliyetleri açıklık ve güvenilirlik oluşturma konusunda kritik bir rol oynamaktadır. Sosyal medya platformlarının dinamik yapısı göz önünde bulundurulduğunda EGM'nin iletişim stratejilerinin sürdürülebilirliğinin ve kriz sonrası süreçlerde de etkinliği-

nin devam etmesi kaçınılmaz bir gereklilik olarak karşımıza çıkmaktadır. Bu nedenle kriz sonrasında halkın güvenini koruyabilmek ve gelecekteki krizlere daha hazırlıklı olabilmek için stratejik iletişim çalışmalarının kesintisiz bir şekilde sürdürülmesi gerekmektedir.

Yapılacak çalışmalarda, EGM'nin sosyal medya üzerinden yürüttüğü kriz iletişimi faaliyetlerinin nasıl daha sistematik ve etkili hâle getirilebileceğinin incelenmesi ve bu süreçlerde dezenformasyonun önlenmesine yönelik proaktif stratejiler geliştirilmesine odaklanılması önemlidir. Bunun yanında, bu çalışmalar sırasında sosyal medya platformlarının değişken doğası ve kullanıcı etkileşimlerinin dinamikleri göz önünde bulundurulmalıdır. Bu sayede kriz anında kamuoyuyla daha etkili bir iletişim sağlamak için yenilikçi yaklaşımlar ve teknolojik çözümler ortaya çıkarılabilir. EGM'nin kriz iletişim stratejilerinin güçlendirilmesi, yalnızca mevcutların yönetimi için değil, aynı zamanda gelecekteki olası krizlere karşı daha hazırlıklı bir yaklaşım geliştirilmesi açısından da büyük önem taşımaktadır.

Kaynakça

Adamu, A. A. ve Mohamad, B. (2019). Developing a strategic model of internal crisis communication: Empirical evidence from Nigeria. *International Journal of Strategic Communication*, *13*(3), 233-254.

Alexander, D. E. (2014). Social media in disaster risk reduction and crisis management. *Science and Engineering Ethics*, *20*, 717-733.

Apuke, O. D. ve Tunca, E. A. (2018). Social media and crisis management: A review and analysis of existing studies. *LAÜ Sosyal Bilimler Dergisi*, *9*(2), 199-215.

Balonas, S., Ruão, T. ve Carrillo, M. V. (2021). *Strategic communication in context: Theoretical debates and applied research*. Coimbra University Press.

Benoit, W. L. (1997). *Image repair discourse and crisis communication*. *Public Relations Review, 23*(2), 177-186.

Benoit, W. L. (2015). Image repair theory in the context of strategic communication. In Holtzhausen, D. ve Zerfass A. (Eds.), *The Routledge handbook of strategic communication*. Oxon: Routledge.

Buhmann, A. ve Likely, F. (2018). Evaluation and measurement in strategic communication. *The international encyclopedia of strategic communication*, *1*, 625-640,

Cheng, Y. (2018). How social media is changing crisis communication strategies: Evidence from the updated literature. *Journal of contingencies and crisis management*, *26*(1), 58-68

Coombs, W. T. (2014). *Ongoing crisis communication: Planning, managing, and responding*. Thousand Oaks, CA: SAGE Publications.

Coombs, W. T. (2011). Political public relations and crisis communication: A public relations perspective. In J. Strömbäck & S. Kiousis (Eds.), *Political public relations: Principles and applications* (pp. 214–234). New York: Routledge.

Coombs, W. T. (2012). *Ongoing crisis communication: Planning, managing, and responding* (3rd ed.). Thousand Oaks, CA: Sage.

Cornelissen, J. (2017). *Corporate communication: A guide to theory and practice*. SAGE

Creswell, J. W. (2013). *Qualitative inquiry and research design: Choosing among five approaches* (3rd ed.). SAGE Publications.

Çakmak, V. (2023). Kriz iletişim stratejileri ve sosyal medya kullanımına yönelik sistematik bir değerlendirme. *Middle Black Sea Journal of Communication Studies*, *8*(2), 179-194.

Dan, V., Paris, B., Donovan, J., Hameleers, M., Roozenbeek, J., van der Linden, S. ve von Sikorski, C. (2021). Visual mis-and disinformation, social media, and democracy. *Journalism and Mass Communication Quarterly*, *98*(3), 641-664

Eriksson, M. (2018). Lessons for crisis communication on social media: A systematic review of what research tells the practice. *International Journal of Strategic Communication*, *12*(5), 526-551.

Eskicioğlu, Y. C. (2023). İnfodemi, korku ve dezenformasyon: Pandemi döneminde sosyal medyada islamofobi. *Journal of Migration and Political Studies*, *1*(1), 17-34

Fallis, D. (2015). What is disinformation?. *Library Trends*, *63*(3), 401-426.

Farwell, J. P. (2012). *Persuasion and power: the art of strategic communication*. Washington, DC: Georgetown University Press.

Fearn, B. K. (2016). *Crisis communications: A casebook approach*. Routledge.

Gündoğan, A. A. ve Karimzadeh, S. (2019). Kuzey Anadolu fay hattı üzerinde olası deprem senaryoları için benzeştirilmiş bir kuvvetli yer hareketi veri tabanı. *Türk Deprem Araştırma Dergisi*, *1*(1), 76-97.

Hallahan, K., Holtzhausen, D., Van Ruler, B., Verčič, D. ve Sriramesh, K. (2007). Defining strategic communication. *International journal of strategic communication*, *1*(1), 3-35.

Heath, R. L. ve Millar, D. P. (2003). *Responding to crisis: A rhetorical approach to crisis communication*. Routledge.

Heath, R. L. ve O'Hair, H. D. (2019). *Handbook of Risk and Crisis Communication*. Routledge.

Hu, X. ve Lovrich, N. P. (2019). Social media and the police: A study of organizational characteristics associated with the use of social media. *Policing: An International Journal*, *42*(4), 654-670.

Holtzhausen, D. ve Zerfass A. (Eds.) (2015). *The Routledge handbook of strategic communication*. Oxon: Routledge.

Hughes, V. ve Love, P. E. (2004). Toward cyber centric management of policing: back to the future with information and communication technology. *Industrial Management & Data Systems*, *104*(7), 604-612.

İletişim Başkanlığı (2023). Yaşanan asrın felaketi sürecinde yapılan dezenformasyonlara karşı yayımladığımız günlük "deprem dezenformasyon" bültenleri 6 Şubat – 20 Şubat. İletişim Başkanlığı Dezenformasyonla Mücadele Merkezi.

Jin, Y. ve Austin, L. L. (2022). *Social media and crisis communication*. Routledge.

Jungblut, M., Kümpel, A. S. ve Steer, R. (2024). Social media use of the police in crisis situations: A mixed-method study on communication practices of the German police. *New Media and Society*, *26*(8), 4647-4668.

Kaplan, A. M. ve Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons*, *53*(1), 59-68.

Karsak, B., Altuntaş, E. Y. ve Demren, G. A. S. (2018). Stratejik iletişim yönetiminde dijital kanalların önemi: Halkla ilişkiler uygulayıcılarının dijital kanal kullanımlarına yönelik niteliksel bir araştırma. *Uluslararası Halkla İlişkiler ve Reklam Çalışmaları Dergisi*, *1*(1), 6-17.

Kaya, İ. ve Şahan, C. (2023). Depreme karşı okul binalarında yapısal olmayan tehlikelere alternatif mobilya tasarım önerileri. *Ordu Üniversitesi Sosyal Bilimler Enstitüsü Sosyal Bilimler Araştırmaları Dergisi*, *13*(2), 1907-1928.

Khang, H., Ki, E. J. ve Ye, L. (2012). Social media research in advertising, communication, marketing, and public relations, 1997–2010. *Journalism & Mass Communication Quarterly*, *89*(2), 279–298.

Lovejoy, K. ve Saxton, G. D. (2012). Information, community, and action: How nonprofit organizations use social media. *Journal of computer-mediated communication*, *17*(3), 337-353

Lipschultz, J. H. (2023). *Social media communication: Concepts, practices, data, law and ethics*. Routledge.

Liu, B. F., Austin, L. ve Jin, Y. (2011). How publics respond to crisis communication strategies: The interplay of information form and source. *Public Relations Review*, *37*(4), 345-353.

Macias, W., Hilyard, K. ve Freimuth, V. (2009). Blog functions as risk and crisis communication during Hurricane Katrina. *Journal of Computer-mediated Communication*, *15*(1), 1-31.

Mahoney, J. (2013). *Strategic communication: Principles and practices*. Oxford University Press.

Miles, M. B. ve Huberman, A. M. (1994). *Qualitative Data Analysis: An Expanded Sourcebook* (2nd ed.). Sage Publications.

Morrow, S. (2019). Social and news media's effects on law enforcement. *Global Journal of Forensic Science and Medicine*, *1*(4), 1-6.

Muhammed T, S. ve Mathew, S. K. (2022). The disaster of misinformation: a review of research in social media. *International journal of data science and analytics*, *13*(4), 271-285.

O'Connor, R. (2019). *Crisis communication: A case study approach*. Routledge.

O'Rourke, A. ve Smith, J. (2023). *Strategic crisis communication.* SAGE Publications.

Pang, A. (2013). Social media hype in times of crises: Nature, characteristics and impact on organizations. *Asia Pacific Media Educator*, *23*(2), 309-336.

Papacharissi, Z. (2015). *Affective publics: Sentiment, technology, and politics*. Oxford University Press.

Patton, M. Q. (2002). *Qualitative research and evaluation methods*. Routledge.

Paul, C. (2011). Strategic communication: Origins, concepts, and current debates. Praeger Security International.

Rettberg, J. W. (2009). Freshly generated for you, and Barack Obama' how social media represent your life. *European Journal of Communication*, *24* (4), 451-466.

Reynolds, B. ve M. W. Seeger, (2005). Crisis and emergency risk communication as an integrative model. *Journal of Health Communication*, *10*(1), 43-55.

Schwarz, A., Seeger, M.W. ve Auer, C. (2016). *The Handbook of International Crisis Communication Research.* Wiley

Sellnow, T. L. ve Seeger, M. W. (2013). *Theorizing crisis communication*. Malden, MA: Wiley-Blackwell

Shahbaznezhad, H., Dolan, R. ve Rashidirad, M. (2021). The role of social media content format and platform in users' engagement behavior. *Journal of Interactive Marketing*, *53*(1), 47-65.

Snoussi, T. (2020). Social media for crisis communication management. *International Journal of Business and Management Research*, *8*(3), 64-72.

Stein, S. ve Wysession, M. (2003). *An introduction to seismology, earthquakes, and earth structure*. Wiley.

Steele, J. L. ve Blau, N. (2023). An analysis of police department crisis communication via social media. *Police Quarterly*, *26*(4), 520-544.

Steyn, B. (2004). From strategy to corporate communication strategy: A conceptualisation. *Journal of communication management*, *8*(2), 168-183.

Su, W. (2016). A virtual public sphere and its limitations–microblog, online civic engagement in China and its interplay with the state. *The journal of international communication*, *22*(1), 1-21.

Telford, J. W. ve Cosgrave, J. (2006). *Joint evaluation of the international response to the Indian Ocean tsunami: Synthesis report*. Tsunami Evaluation Coalition.

Ulmer, R. R., Sellnow, T. L. ve Seeger, M. W. (2017). *Effective crisis communication: Moving from crisis to opportunity* (4th ed.). SAGE Publications.

USGS. United States Geological Survey (2020). *Great Chilean earthquake of 1960*.

https://earthquake.usgs.gov/earthquakes/eventpage/official19600522191120_30/executive(E.T.07 Ekim 2024).

Veil, S. R., Buehner, T., & Palenchar, M. J. (2011). A work in process literature review: Incorporating social media in risk and crisis communication. *Journal of Contingencies and Crisis Management*, *19*(2), 110-122.

Ward, W.E. (2011). Strategic communication at work. *Leader to leader*, *59*, 33-38.

Wilcox, D. L., Cameron, G. T. ve Reber, B. H. (2015). *Public relations: Strategies and tactics*. Pearson.

Zheng, B., Liu, H., & Davison, R. M. (2018). Exploring the relationship between corporate reputation and the public's crisis communication on social media. *Public Relations Review*, *44*(1), 56-64.

Turkish Journal of Security Studies

ISSN: 2148-6166
Year: 26 Volume: 26 Issue: 2 December 2024 p.180-199 Article Type: Review
Received Date: 03.10.2024 Accepted Date: 26.12.2024

What Makes Civil Wars Protracted? A Review of Systemic, Organizational & Individual-Level Factors*

Yunus ÖZTÜRK**

Abstract: This study investigates the factors behind the increasing prevalence of intrastate conflicts since World War II, contrasting with the global decline in interstate wars, particularly in the developing world. While advancements in technology, society, and economy have facilitated a reduction in interstate conflicts, intrastate wars have persisted due to a decline in their terminations rather than an increase in their onsets. The study attributes this prolongation to systemic, organizational, and individual-level factors. At the systemic level, processes such as decolonization, Cold War interventions, and the post-Cold War multipolar order has established conditions that foster civil wars, often exacerbated by external interventions driven by power dynamics and competitive interests. Additionally, neoliberal economic policies have fragmented the global economy and marginalized the Global South, fostering the emergence of "regional conflict complexes" reliant on illicit economies. Organizationally, factors such as state capacity, geographical features, and resource availability enhance the resilience of rebel groups, particularly in rugged, resource-rich territories near international borders that facilitate contraband access and enable evasion of state control. Furthermore, the quality of leadership and cohesion within insurgent groups significantly affect conflict duration, as elite manipulation and factionalism can obstruct peace efforts. Lastly, at the individual level, motivations shaped by grievances associated with ethnic, political, or economic marginalization, alongside economic incentives for private gain, largely sustain involvement in armed conflicts. The study concludes that a comprehensive understanding of these complex factors is crucial for developing effective policy strategies to reduce conflict durations, advancing theoretical and practical approaches to civil war resolution.

Keywords: Intrastate Conflicts, Civil Wars, Civil War Durations, Persistent Civil Wars, Conflict Resolution

* This study is derived from the author's doctoral dissertation, "Droughts in the Midst of Conflicts: A Mixed-Method Analysis of Water Insecurity & Civil War Duration and Outcomes," completed at the University of Delaware (USA) in 2024.

** Lecturer Dr., Recep Tayyip Erdogan University, Faculty of Economics and Administrative Sciences, Department of International Relations, Division of Political History, Rize/Turkey, ORCID: 0000-0002-6274-5230, e-mail: y.ozturk@erdogan.edu.tr

Güvenlik Çalışmaları Dergisi

ISSN: 2148-6166
Yıl: 26 Cilt: 26 Sayı: 2 Aralık 2024 s.180-199 Makale Türü: Derleme
Makalenin Geliş Tarihi: 03.10.2024 Makalenin Kabul Tarihi: 26.12.2024

İç Savaşları Uzatan Nedir? Sistemsel, Örgütsel ve Bireysel Düzeydeki Faktörlerin Bir Değerlendirmesi[*]

Yunus ÖZTÜRK[**]

Öz: Bu çalışmada, İkinci Dünya Savaşı'ndan bu yana, özellikle gelişmekte olan ülkelerde, devletlerarası savaşlardaki küresel düşüşün aksine, devlet içi çatışmaların artan yaygınlığının ardındaki faktörler araştırılmaktadır. Teknolojik, toplumsal ve ekonomik ilerlemeler devletlerarası çatışmaların azalmasını kolaylaştırırken devlet içi savaşlar, meydana gelmelerindeki artıştan ziyade sonlandırılmalarındaki düşüş nedeniyle yaygınlığını korumaktadır. Çalışma, iç savaşların uzamasını sistemsel, örgütsel ve bireysel düzeydeki faktörlere bağlamaktadır. Sistemsel düzeyde, dekolonizasyon, Soğuk Savaş müdahaleleri ve Soğuk Savaş sonrası çok kutuplu düzen gibi süreçler, genellikle güç dinamikleri ve rekabetçi çıkarlar tarafından yönlendirilen, sıklıkla dış müdahalelerle şiddetlenen, iç savaşları teşvik eden elverişli koşullar yaratmıştır. Buna ek olarak neoliberal ekonomi politikaları, küresel ekonomiyi parçalamış ve Küresel Güneyi marjinalleştirerek yasadışı ekonomilere dayanan "bölgesel çatışma komplekslerinin" ortaya çıkmasına yol açmıştır. Organizasyonel olarak devlet kapasitesi, coğrafi özellikler ve kaynak mevcudiyeti gibi faktörler, özellikle kaçakçılığa erişimi kolaylaştıran ve devlet kontrolünden kaçmayı mümkün kılan, uluslararası sınırlara yakın engebeli, kaynak zengini bölgelerde isyancı grupların direncini arttırmıştır. Ayrıca elit manipülasyonu ve hizipçilik, barış çabalarını engelleyebileceğinden isyancı gruplar içindeki liderlik ve uyum kalitesi çatışma süresini önemli ölçüde etkilemiştir. Son olarak bireysel düzeyde, kişisel çıkarlara dönük ekonomik teşviklerin yanı sıra etnik, siyasi veya ekonomik marjinalleşmeyle ilişkili şikâyetlerle şekillenen motivasyonlar, silahlı çatışmalara katılımın sürdürülmesini büyük ölçüde etkilemiştir. Çalışma, bu karmaşık faktörlerin kapsamlı bir şekilde anlaşılmasının çatışma sürelerini azaltmaya yönelik etkili politika stratejileri geliştirmek ve iç savaş çözümüne yönelik hem teorik hem de pratik yaklaşımları ilerletmek için önemli olduğu sonucuna varmaktadır.

Anahtar Kelimeler: Devlet İçi Çatışmalar, İç Savaşlar, İç Savaş Süreleri, Kalıcı İç Savaşlar, Çatışma Çözümü

[*] Bu çalışma, yazarın "Çatışmaların Ortasında Kuraklıklar: Su Güvensizliği & İç Savaş Süresi ve Sonuçları Üzerine Karma Yöntemli Bir Analiz" başlıklı doktora tezinden türetilmiş olup 2024 yılında Delaware Üniversitesi'nde (ABD) tamamlanmıştır.

[**] Öğretim Görevlisi Dr., Recep Tayyip Erdoğan Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Uluslararası İlişkiler Bölümü, Siyasi Tarih Anabilim Dalı, Rize/Türkiye, ORCID: 0000-0002-6274-5230, e-posta: y.ozturk@erdogan.edu.tr

Introduction

Since the conclusion of World War II, the global landscape has witnessed two concurrent trends in conflict dynamics. While interstate wars have become increasingly rare, mainly due to various social, economic, political, and technological transformations (see Gat (2017), Mandelbaum (1998), Mueller (2001), Pinker (2011)), intrastate wars have experienced a notable surge, particularly in the developing world (Rustad, 2024). In the period following the Cold War, scholarly debates have centered on identifying the factors contributing to these contrasting trends in interstate and intrastate wars. Particularly, the ongoing Ukrainian War has prompted a reexamination of the proposition that interstate wars are a relic of a bygone era. Consequently, some scholars have argued that conventional interstate wars remain a feature of the contemporary world (e.g., Biddle (2023), Robinson (2022)). Undoubtedly, armed conflicts in the Middle East, Africa, and Eastern Europe, coupled with the warnings of world leaders that a new potential world war may be imminent, have reignited these debates (Overy, 2024; Racker, 2023; Rustad, 2024). Despite the renewed focus on interstate wars, intrastate wars remain a more significant concern for international peace and security due to their increased prevalence, intensity, and duration. Notably, such conflicts have resulted in higher civilian casualties, displacement, and external interventions (Einsiedel et al., 2014; 2017).

The rise in intrastate conflicts can be attributed to a range of factors, including weak state capacity, contentious national identities, illegitimate and/or authoritarian governments, territorial disputes, and the enduring legacies of colonialism (Holsti, 2004; Kennedy & Waldman, 2014; Newman, 2014; Rice, 1990). Although these explanations offer insights into the root causes of intrastate conflicts, they fall short of fully accounting for the distinctive characteristics of contemporary wars. Contemporary intrastate wars, for instance, are significantly more protracted and resistant to decisive military resolutions. This is largely due to the proliferation of external interventions, the rise of criminal networks, and the expansion of extremist groups (Einsiedel et al., 2014; 2017; Walter, 2017). Specifically, while post-World War II civil wars were typically class-based conflicts aiming to incite revolutions by mobilizing the masses, post-Cold War civil wars have primarily been driven by ethnic separatism. Since the turn of the millennium, however, the global landscape has witnessed a new wave of civil wars, where religious or sectarian identities, combined with technological advancements in weaponry, have played a pivotal role. As Walter (2017, p. 470) observes that most post-millennium civil wars have occurred in Africa, East Asia, and the Middle East, where radical religious groups have pursued transnational objectives, namely the unification of the *Ummah* under a *Khalifa*.

While these arguments clarify the underlying causes of intrastate wars and illustrate their evolving trends and characteristics, they are insufficient in identifying the factors behind the steady rise in the global prevalence of civil wars since the end of World War II. Put differently, the question remains: What factors have contributed to the sustained incidence of civil wars, particularly in the post-World War II era? Collier et al. (2004) and Fearon (2004) propose that the increased incidence of civil wars is more closely linked to a decline in terminations rather than an increase in onsets. In other words, while the number of civil wars onsets remains relatively stable at approximately 2.2 per year, the rate of civil war terminations has dropped to around ~1.7 per year, leading to the protraction of intrastate conflicts. Notably, the average duration of civil wars has exceeded 20 years during the post-World War II period (Collier et al., 2003, pp. 93–97; Fearon, 2004, pp. 275–276). In brief, the growing prevalence of civil wars since 1945 can be attributed to the increasing protraction of these conflicts, as the interval between the onset and termination has progressively lengthened over time despite fluctuations in the broader international context.

In this context, the objective of this study is to provide a comprehensive review of the extant literature on the factors contributing to the prolongation of civil wars. This study specifically investigates systemic, organizational, and individual-level factors to offer a holistic understanding of the phenomenon under review. By examining protracted civil wars from a three-dimensional perspective, this study concludes that a thorough analysis of these prolongation factors is essential to comprehend the reasons behind the increased persistence of intrastate wars, particularly in the post-World War II era. Such a study would contribute significantly to academic research and policy-making efforts in three key ways (Brandt et al., 2008; Hegre, 2004).

First, in addition to the prevention of new conflicts, the resolution or shortening of protracted civil wars has become a crucial task for policymakers, given the detrimental impacts these wars have on human, state, and international security (Collier et al., 2003; Iqbal, 2006; Kang & Meernik, 2005; Thyne, 2016). Second, since the prevalence of civil wars is more closely related to their protracted nature than to their increased onsets, the earlier termination of such conflicts would lead to a decline in the overall number of civil wars, and consequently, a reduction in the total number of armed conflicts worldwide (Collier et al., 2003; Fearon, 2004; 2017; Fearon & Laitin, 2003). Finally, investigating the duration of civil wars offers insights into the potential outcomes of these conflicts, thereby facilitating the identification of the most effective policy strategies for ending ongoing civil wars (Brandt et al., 2008; DeRouen Jr. & Sobek, 2004; Mason et al., 1999; Mason & Fett, 1996).

The paper is structured as follows: The initial section examines international, regional, and local factors contributing to prolonging civil wars. The second section explores organizational factors, focusing on both rebel/insurgency groups

and states/governments. The third section builds upon the preceding analysis by investigating the individual-level factors that contribute to the persistence of civil wars. The final section critically assesses the factors discussed, offering critiques, policy suggestions, and concluding remarks.

Systemic Factors: International, Regional & Local Levels

The study of civil wars typically approaches factors contributing to their dynamics -onset, duration, and termination- from an individual or organizational/group perspective. The least studied area, however, pertains to international, regional, and local factors. In this context, Gleditsch (2007, p. 305) emphasizes international factors in understanding civil war dynamics and prospects for their resolution. This sub-section thus comprehensively examines systemic factors at the international, regional, and local levels. Specifically, the following factors are subjected to detailed examination: (i) shifts in the international system and the increased third-party interventions, (ii) changes in the international economic system and the advent of regional conflict complexes, and (iii) the local agendas and activities of rebel groups.

International Political System & Third-Party Interventions

From a macro perspective, Hironaka (2005) argues that the surge in civil wars in the post-World War II era can be attributed to shifts in the international system. The decolonization process between 1945 and 1960 led to the admission of numerous weak African and Asian states into the international system as *de jure* sovereign equals. However, most of these states were highly dependent on foreign aid and military assistance. During the Cold War, most of these newly independent states aligned themselves with the US or the USSR, contingent on their ideological leanings. This great power competition resulted in increased financial, technical, and military support or intervention on behalf of governments or rebel factions, thereby altering the balance of power between warring parties. Consequently, neither side achieved a decisive victory, leading to protracted and intractable conflicts (Hironaka, 2005, pp. 20–28).

The Cold War period, however, was not the sole factor responsible for prolonging domestic conflicts; the post-Cold War context also played a significant role. Contrary to the expectations of those with a liberal outlook (see Fukuyama (1989)), the end of the bipolar Cold War international system, particularly following the “unipolar moment” of US hegemony during the early 1990s (see Krauthammer (1990; 2002)), led to the emergence of multiple middle powers, each competing for relative advantage. As Posen (2017, pp. 171–172) observes, in the post-Cold War multipolar world, the primary concern of major powers was to

maintain the balance of power against the rise of regional powers. Particularly, the lack of consensus on why, when, and how the international society should intervene in intrastate wars had created a political vacuum in which external interventions through the "responsibility to protect" (R2P) norm/doctrine were increasingly viewed as a way to fill that gap. In short, the pursuit of relative advantage within a multipolar world gave rise to what Posen (2017) terms "competitive interventions." These interventions, often backed by external actors, led to persistent efforts by warring parties to maintain military activities in the expectation that external assistance would ultimately guarantee victory (Posen, 2017, p. 176).

It is evident that the primary factor contributing to the prolongation of civil wars during both the Cold War and the post-Cold War periods was the increased frequency of external interventions, whether financial, technical, or military. Third-party interventions have been shown to extend the duration of civil wars in ethnically polarized societies by reducing the coordination costs for rebel groups (Elbadawi & Sambanis, 2000). Moreover, the mere anticipation of external assistance can foster an environment conducive to protracted conflicts. Warring parties may persist in their military efforts until such assistance arrives or refrain from settling the conflict until they have exhausted their existing resources (Akcinaroglu & Radziszewski, 2005). Although the intentions behind third-party interventions, whether neutral or biased, are critically important, it is argued that third-party interventions are more likely to prolong civil wars (Balch-Lindsay & Enterline, 2000; Regan, 2002). Because of the importance of the intervenors' impartiality, biased interventions make it less likely that belligerents will seek to terminate civil wars promptly. The partiality of external intervenors reduces the likelihood that the warring parties will see the cessation of hostilities as being in their interest.

The strategic competition among intervenors also plays a crucial role in determining the duration of civil wars (Anderson, 2019). While the intervenors endeavor to ensure that their proxies are sufficiently robust to achieve a decisive military victory through aid and assistance, they simultaneously seek to avoid provoking other external actors into intervening or escalating the conflict. In such a context, intervenors may perceive the continuation of the conflict as a more favorable outcome than its premature conclusion. Nevertheless, intervenors from democratic regimes are inclined to support would-be victorious parties in conflicts due to the constraints and obligations inherent to their democratic systems, particularly those related to accountability and transparency (Norrevik & Sarwari, 2021). In addition to competition and regime types, the specific intervention tools employed -whether sanctions or military deployment- are significant determinants of conflict dynamics. For example, economic sanctions have been shown to reduce conflict duration more effectively than arms embargoes (Escribà-Folch, 2010). In the context of military interventions, however, larger military deployments in conflict zones have been associated with shorter civil wars (Kathman & Benson, 2019).

International Economic System & *Regional Conflict Complexes*

It is important to note that systemic factors are not inherently political. Following the 1970s, alterations to the global economic system through the implementation of neoliberal policies, including deregulation and privatization, have resulted in a significantly more fragmented global capitalist system, contrary to the anticipated outcomes of globalization. Adopting neoliberal policies has led to a clear distinction between the North and South in the global economic landscape, with the former occupying the core and the latter situated at the periphery of the global economy. This fragmented economic system has resulted in the formation of an exclusionary global economy. While the North has intensified its interdependent economic relations, the South has been excluded from the emerging Northern informational economy. Consequently, the South was compelled to turn towards extra-legal networks, including transnational criminal networks and war economies (Duffield, 2001, pp. 2–7).

For Duffield (2000; 2001), the prevailing economic system exerts a profound influence on the conflict dynamics. The advent of market deregulation has precipitated a surge in parallel and transborder trade, facilitating the formation of local-global networks and shadow economies. These serve as conduits for asset realization and self-provisioning, particularly in the context of armed conflicts (Duffield, 2001, p. 14). Moreover, besides being excluded from the Northern economic network, the South lacked financial aid, technical support, and military assistance from their patrons in the post-Cold War era. Those in positions of power in the South, whether ruling elites or rebel leaders, have become significantly more inclined to pursue alternative sources of financial stability, primarily through extra-legal economic networks. As Duffield (2000, pp. 72–73) succinctly states, "market deregulation and declining nation-state competence [due to globalization] have not only allowed the politics of violence and profit to merge, but also underpin the regional trend toward protracted instability, schism, and political assertiveness in the South."

Such a transformation in the international economic system led to the advent of regional war economies in the South. In this regard, Armstrong & Rubin (2002) and Studdard (2004) present a compelling argument for the role of "regional conflict complexes/formations," namely war economies, in shaping conflict dynamics. The term "regional conflict complex" refers to actors' social, economic, military, and political networks within particular regions. These networks facilitate the movement of "people, goods, and arms [move] back and forth across borders and among 'internal' conflicts, prolonging regional conflict and preventing [a] peaceful resolution" (Armstrong & Rubin, 2002, p. 4). Notable regional conflict complexes include West Africa, Southern Central Asia, the Andean region, the Middle East, the Great Lakes region, and the Balkans. These regions are characterized by the frequent occurrence of smuggling networks, illicit trafficking in

humans, drugs, and arms, transborder armed groups, mercenaries, and refugee flows (Armstrong & Rubin, 2002, pp. 5–7).

Local Dynamics & Agendas of Warring Parties

In addition to international and regional factors, local dynamics also play a role in determining the duration of conflicts. Autesserre (2009; 2010) emphasizes the significance of rebel groups' local agendas, particularly territorial/land issues, in prolonging civil wars. A comprehensive analysis of the Congolese Civil War demonstrates that an excessive focus on the broader discourse of intervenors in the context of regional or national initiatives to terminate civil wars leads to the neglect of rebel groups' local agendas and activities by peacebuilders. Such a "peacebuilding culture" diverts the attention of scholars and policymakers from the local causes of warfare, thereby contributing to the failure of peace missions and the prolongation of conflicts between belligerents.

Organizational Factors: State Capacity & Group Cohesion

Undoubtedly, an exclusive focus on international, regional, and local-level factors is insufficient for a comprehensive understanding of the prolonged intrastate wars in the post-WWII era. The role of individual and organizational dynamics in this phenomenon is worthy of consideration as these factors are central to understanding why conflicts persist. The key explanatory variables are the timing and duration of the initial uprising by the oppressed and the continuation of insurgent warfare by rebel groups against mighty governments. Before examining why would-be rebels engage in armed conflict with formidable armed forces, this sub-section addresses the factors contributing to the resilience of rebel/insurgent groups in the face of significant challenges. From an organizational perspective, rebel/insurgent groups tend to maintain their military operations for as long as they possess (i) the opportunity and (ii) strong leadership and group cohesion necessary for their warfighting efforts against formidable government forces.

Opportunity Structure & State Capacity

While the literature on civil wars emphasizes the significance of "greed *versus* grievance" arguments in understanding the outbreak and persistence of intrastate conflicts, some scholars (e.g., Berdal (2005), Hoeffler (2011), Humphreys & Weinstein (2008), Keen (2011)) challenge the simplicity of this perspective in explaining a complex social phenomenon like civil wars. Rather, they propose a more sophisticated approach that extends beyond the simplistic dichotomy of greed versus grievance, which often posits "opportunity" for conflict as a key *explanans*. In this regard, Fearon & Laitin (2003, p. 75) argue that "the main factors

determining [intrastate wars] are not ethnic or religious differences or broadly held grievances but, rather, conditions that favor *insurgency*." Similarly, Collier et al. (2008) emphasize the importance of "feasibility" in the outbreak of conflicts (see also Collier (2000), Collier & Hoeffler (1998; 2004)). The opportunity or feasibility argument posits that the outbreak of conflicts by political entrepreneurs is contingent upon the existence of a militarily and financially conducive environment with a low opportunity cost and high utility of participation. Such environments allow would-be rebels to participate in armed groups in pursuit of private gains. It is evident that this line of reasoning offers a more comprehensive perspective on the circumstances under which would-be rebels are likely to take up arms and continue their participation in armed groups. The motivational arguments, which are typically framed in terms of greed *versus* grievances, are typically employed to elucidate the initial impetus behind collective violence, namely why people riot in the first place.

From the opportunity structure perspective, geographical factors, state capacity, and the balance of power between warring parties are identified as the key variables. Specific geographical features, such as rough/mountainous terrain, resource-rich lands, distance from city centers, proximity to international borders, *et cetera*, are regarded as primary contributors to prolonged conflicts, as they enhance rebel capacity against formidable government forces. The presence of rugged terrain allows rebels to conceal themselves from government forces, particularly when they are comparatively weaker and seek to achieve a balance of power through military means. Similarly, government forces are required to possess local knowledge of the terrain for logistical reasons, which is often not readily available to armed forces (Buhaug et al., 2009; Buhaug & Gates, 2002; Rustad et al., 2008). In the same way, resource-rich areas offer rebels the opportunity to extract valuable resources or engage in contraband activities, which can bolster their war effort. By raiding cultivated lands and farms for subsistence products or extracting precious gems and natural resources, such as diamonds, timber, and oil, for contraband and illicit markets, armed groups may maintain their existence through financial well-being even when confronted with mighty government forces. Moreover, the proximity of rebel groups to international borders allows them to receive external support and/or establish a haven outside of their operational area/country, thus enabling them to maintain their existence and warfighting capacity (Bagozzi et al., 2017; Buhaug et al., 2009; Buhaug & Gates, 2002; Koren & Bagozzi, 2017).

The state capacity variable is of paramount importance in determining whether rebel/insurgent groups could initiate and maintain their warfare. In her analysis of state capacity, Skocpol (1985; 2008) builds upon the formulations of Weber (1946) and Tilly (1985) to elucidate the role of state capacity in understanding why some states experience civil wars that result in social revolutions while others do not. Similarly, Tilly (1978) underscores state capacity in explaining when rebellion as a form of social mobilization could be a viable option for would-

be rebels. According to this line of reasoning, the likelihood of rebel/insurgent groups successfully pursuing a rebellion is diminished when they are likely to be repressed or accommodated by the state. In other words, the requisite time for a decisive military victory is reduced if the state possesses an effective bureaucratic apparatus and/or a powerful military force, thereby shortening the duration of conflicts (DeRouen Jr. & Sobek, 2004). Conversely, when states lack the capacity and/or resources to respond effectively, decision-makers are more likely to pursue a containment strategy against rebel groups, which can result in protracted conflicts (Fearon, 2004; Fearon & Laitin, 2003; Mukherjee, 2014). Nevertheless, it is important to note that indications of robust, strong state capacity, particularly in rural areas, such as infrastructure like roads, hospitals, schools, and police stations, are more likely to be targeted by rebel groups as a means of demonstrating their resilience and power (Koren & Sarbahi, 2018).

Leadership & Group Cohesion

Clearly, the arguments about state capacity provide insight into the power dynamics between rebel/insurgent groups and governments, influencing the duration and outcomes of civil wars. However, this does not imply that civil wars are exclusively related to the capacity of states. For instance, the concessions made by governments to strong rebel groups are typically accepted within a relatively short period, leading to a shorter duration of civil wars, or *vice versa* (Cunningham et al., 2009). Evidently the pivotal elements in this context are not solely the states but also the rebel groups, particularly in terms of their (i) leadership and (ii) organizational strength. In this regard, theories of social mobilization and contentious politics offer valuable insights into the significance of rebel groups' organizational capacity beyond feasibility/opportunity structure in civil war dynamics (see McAdam et al. (2004; 2008), Tilly (1978), Tilly & Tarrow (2015)). As Kaufman (2015) succinctly notes, the role of elites in framing issues in a specific way -a.k.a. the "air war"- is to mobilize masses for conflicts underpinned by leadership. In contrast, the organizational strength emphasizes the structures through which participants are controlled and directed in the context of the "ground war."

Political leaders/elites play a pivotal role in shaping the discourse surrounding contentious issues, thereby manipulating public opinion and sustaining mass participation in protracted armed conflicts. Moreover, the competition among rebel/insurgent groups to control mass movements or human resources also contributes to the dynamics of civil wars. In examining the potential for the demise of terrorist organizations, for instance, Cronin (2009) identifies six different strategies, with the "decapitation" of leadership being the most crucial. This is because leaders are regarded as the "propagandist in chief," and their removal can have a significant adverse impact on the organization's ability to disseminate and promote its message/cause.

Nevertheless, despite the conventional wisdom that civil wars are inherently dyadic, a more accurate description is that they are extra-dyadic. In such conflicts, multiple rebel leaders/groups may compete with the government or with each other for a superior position. Particularly in the context of peace processes, the presence of "spoilers" - those who perceive a potential peace agreement as disadvantageous to their parochial goal, whether total, limited, or greedy - can impede the ongoing peace process in order to secure their preferences and interests in the post-conflict environment (Stedman, 1997; 2003). For such spoilers, the continuation of hostilities is preferable to a swift conclusion of the war. Moreover, the spoiler problem is not confined to the context of peace negotiations. Actors may also struggle for dominance before, during, and after peace talks. This phenomenon has been frequently observed in the Palestinian issue, where the lack of cohesion among Palestinian actors has resulted in armed conflicts within and between groups for control and leadership (see Pearlman (2009; 2011; 2012)). In short, the greater the number of conflicting actors engaged in struggles for dominance, the more probable it is that armed conflict will persist as multiple "veto players" seek to advance their parochial interests and/or preferences in the looming post-conflict environment (Cunningham, 2006; Pearlman & Cunningham, 2012).

Last but not least, the type of warfare employed by rebel/insurgent leaders/groups is also a significant factor in understanding the conflict dynamics. For instance, states are reluctant to compromise for a negotiated settlement with secessionist insurgent groups, as any concession is more likely to be perceived as a sign of weakness by other rebel groups. Consequently, as Walter (2006) illustrates, states typically engage in protracted conflicts against such rebel/insurgent groups to establish a reputation for their deterrent capabilities. Nevertheless, this line of reasoning cannot be applied to rebel/insurgent groups that demand decentralization and/or power-sharing, as these actors are more inclined to compromise and conclude ongoing conflicts in a shorter time. Similarly, "irregular warfare" frequently results in protracted conflicts that conclude with government victories, as rebel/insurgent groups require time to organize for public support and to develop military effectiveness compared to the capabilities of the armed forces (Balcells & Kalyvas, 2012).

Individual-Level Factors: Emotions & Interests

One area that has yet to be sufficiently examined in this analysis is the underlying motivation of individuals driven to engage in armed conflicts on the side of rebels/insurgents. The analysis has thus far concentrated on systemic and organizational factors in order to gain insight into the international, regional, and local conditions that gave rise to protracted conflicts, as well as the organizational structures that enable rebel/insurgent groups to sustain their involvement in armed conflicts.

Nevertheless, these arguments are inadequate for comprehending why individuals would engage in armed conflict with formidable armed forces, even at the risk of their own lives. Given that rebel/insurgent groups require a consistent supply of personnel to engage in combat (a.k.a. recruitment), it becomes evident why exploring the motivation of would-be rebels/insurgents for participating in armed groups is a crucial element in the analysis.

"What motivates individuals to engage in risky actions, even at the cost of their own lives?" is the central question that one is required to answer in order to understand the radicalization of individuals and the sustenance of rebel/insurgent groups through recruitment. The extant literature has thus far addressed this question from two distinct perspectives: the emotional motivations (grievances) associated with a sense of injustice and the economic incentives (greed) that drive individuals to pursue material gain (e.g., Cederman et al. (2011; 2013), Collier (2000), Collier & Hoeffler (1998; 2004), Gurr (2010), Keen (2000; 2011), Reno (2000), Soysa (2000), Stewart (2008)). Given that these two perspectives analyze the phenomenon in a limited fashion, a more holistic approach, including both emotions and incentives, is necessary to fully comprehend the motivations underlying the decision to risk one's life for a cause (see Berdal (2005), Berdal & Malone (2000), Collier et al. (2008)).

In fact, emotional or incentive-based factors that prompt individuals to engage in armed conflicts against formidable governments are directly related to Mancur Olson's (2002) argument regarding the "collective action problem." As Olson (2002, p. 116) observes, individuals are more likely to engage in "free-riding" behavior when they benefit from public goods without any associated risks or costs and when others are willing to assume the responsibility and bear the cost on their behalf. In light of the cost-free benefits inherent in civil wars, the question of why some individuals, but not others, take up arms against armed forces at the cost of their lives becomes a significant conundrum. On the one hand, some scholars (e.g., Cederman et al. (2013), Gurr (2010), McLauchlin (2018), Montalvo & Reynal-Querol (2010), Østby (2008), Stewart (2008), Wucherpfennig et al. (2012)) posit that individuals are more likely to engage in armed conflicts when they have specific grievances, such as experiencing economic inequality, political discrimination, ethnic, religious or sectarian polarization, cultural exclusion, *et cetera*. In contrast, others (e.g., Bagozzi et al. (2017), Collier (2000a; 2000b), Collier & Hoeffler (1998; 2004), Keen (2000; 2011), Koren & Bagozzi (2017), Reno (2000), Shearer (2000), Soysa (2000)) claim that people primarily join in armed groups for personal gain, including through external support, natural resource extraction, looting, pillaging, plundering during armed conflicts, et cetera.

Emotional Motivation or *Grievances*

In particular, Stewart (2008) proposes that the existence of "horizontal inequalities" in economic, social, and cultural spheres is the underlying cause of violent conflicts among social groups. In this line of reasoning, the intensification of grievances at the leadership and mass levels due to the perception of "relative deprivation" among social groups and the occurrence of systematic discrimination by states against specific social groups result in individuals resorting to rioting against governments in pursuit of a more favorable set of conditions (see also Gurr (2010)). Moreover, compared to economic discrimination, social, political, and cultural exclusion have been identified as the most significant factors in mass mobilization for armed conflicts (Cederman et al., 2011; 2013; Østby, 2008). Exclusionary state policies directed at specific social groups, whether ethnic, religious, or sectarian, are likely to contribute to the persistence of armed conflicts. Such policies exacerbate the existing grievances among would-be rebels, thereby providing the requisite human resources for protracted conflicts (Montalvo & Reynal-Querol, 2010; Wucherpfennig et al., 2012). Moreover, the implementation of exclusionary policies or selective promotions results in the social groups supported by such policies becoming more loyal to the regime. This inevitably gives rise to assurance problems for rebels attempting to negotiate a peace process (McLauchlin, 2018).

Economic Incentives or *Greed*

In light of the pervasiveness of social, political, and cultural grievances inherent across diverse societies, some scholars (e.g., Collier (2000a; 2000b), Collier & Hoeffler (1998; 2004)) contend that economic incentives for private gains offer a more compelling rationale for the mass participation of individuals in armed conflicts. Collier (2000b) and Collier & Hoeffler (1998), in particular, elucidate the tendency for individuals to be more responsive to economic incentives than socio-political motivations, rendering the accumulation of personal wealth a more probable motive for would-be rebels. In other words, individuals are more likely to engage in rebel activities if they perceive the potential for personal gain during the conflict or a favorable outcome at its conclusion. Collier et al. (2004) demonstrated in their renowned quantitative analysis that economic inequality and *per capita* income are the most significant factors in prolonging civil war by lowering the opportunity cost for would-be rebels. Put differently, individuals are more likely to engage in armed conflicts when they face high income inequality and when the cost of participation is low, whereas the potential rewards of rebellion are comparatively high. In such circumstances, rebellion is regarded as a commercial venture or "business" for most would-be rebels rather than an "investment" in addressing their existing grievances.

In line with this reasoning, violence is not an irrational act perpetrated by the masses; rather, it is a deliberate and strategic action undertaken by political elites to maintain their privileged position by manipulating the masses to engage in armed conflict against rivals. Moreover, lay people also engage in rebel activities for reasons related to security, survival, and, when feasible, economic gain through plundering, pillaging, raiding, and other forms of criminal activity. From this perspective, warring parties, whether political elites or rebel leaders, are not regarded as dedicated actors striving to overcome their grievances through armed conflict. Instead, they are considered bandits or pirates, driven by a desire to loot and exploit economic and political resources (Reno, 2000; Soysa, 2000). In such circumstances, the ultimate aim of warfare is not to achieve a decisive victory on the battlefield, as is the case in conventional wars, but rather to prolong an ongoing conflict in order to accumulate wealth and sustain privileged positions (Aliyev, 2020; Keen, 2000; 2011).

It is important to note that the financial resources of rebel/insurgent groups are not solely dependent on natural resource extraction. Rebel groups employ a variety of income-generating activities, including the raiding of aid convoys, participation in illicit trade and trafficking networks, and the looting of agricultural lands and farms for sustenance (Bagozzi et al., 2017; Koren & Bagozzi, 2017; Shearer, 2000). Moreover, the erosion of states' territorial integrity and sovereignty through globalization and neoliberal policies (e.g., privatization, marketization) since the 1970s has created an environment conducive to warring parties engaging in international criminal activities without robust state surveillance for wealth accumulation through smuggling and trafficking (Duffield, 2000; 2001). As Keen (2000, p. 24) succinctly states:

> "Conflicts have seen the emergence of war economies (often centered in particular regions controlled by rebels or warlords and linked to international trading networks). Members of armed gangs have profited from looting and other forms of violent economic activity. […] These developments add to the difficulties of bringing violence to an end, […] because many have a vested interest in prolonging violence […]."

Conclusion

Since the end of World War II, the global landscape has witnessed a notable increase in intrastate conflicts, particularly in comparison to the global reduction in interstate wars. While technological and socio-economic advancements have mitigated interstate conflicts, intrastate wars persist not because of an increase in the incidence of such conflicts but due to decreased rates at which they are concluded. After a comprehensive review of existing literature, this study identifies three key levels of contributing factors to the prolongation of civil wars: (i) systemic, (ii) organizational, and (iii) individual.

Systemic factors essentially point to the legacy of decolonization, Cold War interventions, and the post-Cold War multipolar world order, in which these processes create conditions conducive to civil wars. In many instances, external or third-party interventions have contributed to intensifying ongoing conflicts through geopolitical competition. The proliferation of neoliberal policies, particularly since the 1970s, has contributed to the global economy's further fragmentation, resulting in the Global South's economic marginalization and the emergence of "regional conflict complexes" that are dependent on illicit economies for sustenance.

At the organizational level, factors such as state capacity, geographical features, and resource availability play a crucial role in the resilience of rebel groups. The capacity of states to exert control over territory is frequently constrained by several factors, including the presence of rugged terrain and the proximity of rebel groups to international borders and resource-rich areas. These conditions permit rebels/insurgents to evade strict state control and gain access to illicit markets, thereby prolonging conflicts. Moreover, the quality of leadership and group cohesion within insurgent groups considerably impact on the duration of conflicts in which elite manipulation and factional competition within rebel groups create additional obstacles (e.g., spoilers) to peace processes.

Last, the continued involvement of rebel groups in armed conflict can also be attributed to individual-level factors. The decision to engage in armed conflicts is driven by a complex interplay of individual motivations, including grievances and economic incentives. Marginalization in social, economic, or political arenas exacerbates grievances, whereas the presence of economic opportunities within conflict zones incentivizes continued involvement among would-be rebels. This dual motivation (a.k.a. *greed* & *grievances*) sustains individual participation, thereby rendering ongoing conflicts more resistant to resolution.

In brief, this study highlights the importance of a comprehensive approach to understanding and addressing the increasing prevalence and prolongation of civil wars. By examining these multifaceted factors – systemic, organizational, and individual, the research contributes to both the academic literature and the formulation of policy strategies aimed at reducing conflict durations and thus achieving sustainable peace. To this end, the study puts forth the following ten policy recommendations for decision-makers to curtail the duration of intrastate conflicts: (i) reducing third-party interventions either through impartial meditation and/or negotiation mechanisms under the auspices of neutral international organizations; (ii) increasing economic aid and investments to marginalized regions in the Global South to mitigate their reliance on illicit and/or war economies; (iii) enhancing international cooperation to dismantle transnational criminal networks through the strict border controls and international monitoring; (iv) providing technical and financial assistance to conflict-prone states to improve their control capacity, particularly in contested areas; (v) employing strategies to undermine rebel/insurgent group cohesion through incentivizing defections and fostering splinter

groups; (vi) using targeted sanctions or diplomatic pressures on rebel/insurgent factions to reduce their adverse impacts on peace processes; (vii) designing peace agreements that account the preferences of potential spoilers for power-sharing and resource distribution; (viii) implementing community-based reconciliation programs to address historical grievances and thus building trust among marginalized social groups; (ix) creating economic opportunities for would-be rebels in conflict-affected areas through development programs and job creation in order to reduce their reliance on war economies; and, lastly, (x) fostering regional alliances through regional organizations to address cross-border issues collaboratively.

Bibliography

Akcinaroglu, S., & Radziszewski, E. (2005). Expectations, Rivalries, and Civil War Duration. *International Interactions*, *31*(4), 349–374.

Aliyev, H. (2020). Pro-regime Militias and Civil War Duration. *Terrorism and Political Violence*, *32*(3), 630–650.

Anderson, N. (2019). Competitive Intervention, Protracted Conflict, and the Global Prevalence of Civil War. *International Studies Quarterly*, *63*(3), 692–706.

Armstrong, A., & Rubin, B. R. (2002). *Conference Summary: Policy Approaches to Regional Conflict Formations*. New York. Center on International Cooperation.

Autesserre, Séverine. (2009). Hobbes and the Congo: Frames, Local Violence, and International Intervention. *International Organization*, *63*(2), 249–280.

Autesserre, Séverine. (2010). *Trouble With the Congo: Local Violence and the Failure of International Peacebuilding*. Cambridge University Press.

Bagozzi, B. E., Koren, O., & Mukherjee, B. (2017). Droughts, Land Appropriation, and Rebel Violence in the Developing World. *The Journal of Politics*, *79*(3), 1057–1072.

Balcells, L., & Kalyvas, S. N. (2012). Does Warfare Matter? Severity, Duration, and Outcomes of Civil Wars. *ICIP Working Papers*, *5*.

Balch-Lindsay, D., & Enterline, A. J. (2000). Killing Time: The World Politics of Civil War Duration, 1820-1992. *International Studies Quarterly*, *44*(4), 615–642.

Berdal, M. R. (2005). Beyond Greed and Grievance – and Not Too Soon …. *Review of International Studies*, *31*(4), 687–698.

Berdal, M. R., & Malone, D. (Eds.). (2000). *Greed and Grievance*. Lynne Rienner Publishers.

Biddle, S. (2023). Back in the Trenches: Why New Technology Hasn't Revolutionized Warfare in Ukraine. *Foreign Affairs*, *102*(5), 153+.

Brandt, P. T., Mason, T. D., Gurses, M., Petrovsky, N., & Radin, D. (2008). When and How the Fighting Stops: Explaining the Duration and Outcome of Civil Wars. *Defence and Peace Economics*, *19*(6), 415–434.

Buhaug, H., & Gates, S. (2002). The Geography of Civil War. *Journal of Peace Research*, *39*(4), 417–433.

Buhaug, H., Gates, S., & Lujala, P. (2009). Geography, Rebel Capability, and the Duration of Civil Conflict. *Journal of Conflict Resolution*, *53*(4), 544–569.

Cederman, L.-E., Gleditsch, K. S., & Buhaug, H. (2013). *Inequality, Grievances, and Civil War*. Cambridge University Press.

Cederman, L.-E., Weidman, N. B., & Gleditsch, K. S. (2011). Horizontal Inequalities and Ethnonationalist Civil War: A Global Comparison. *American Political Science Review*, *105*(3), 478–495.

Collier, P. (2000a). Doing Well Out of War: An Economic Perspective. In M. R. Berdal & D. Malone (Eds.), *Greed and Grievance: Economic Agendas in Civil Wars* (pp. 91–112). Lynne Rienner Publishers.

Collier, P. (2000b). Rebellion as a Quasi-Criminal Activity. *The Journal of Conflict Resolution*, *44*(6), 839–853.

Collier, P., Elliott, V. L., Hegre, H., Hoeffler, A., Reynal-Querol, M., & Sambanis, N. (2003). *Breaking the Conflict Trap*. Civil War and Development Policy. Washington, D.C.. The World Bank Group.

Collier, P., & Hoeffler, A. (1998). On Economic Causes of Civil War. *Oxford Economic Papers*, *50*(4), 563–573.

Collier, P., & Hoeffler, A. (2004). Greed and Grievance in Civil War. *Oxford Economic Papers*, *56*(4), 563–595.

Collier, P., Hoeffler, A., & Rohner, D. (2008). Beyond Greed and Grievance: Feasibility and Civil War. *Oxford Economic Papers*, *61*(1), 1–27.

Collier, P., Hoeffler, A., & Söderbom, M. (2004). On the Duration of Civil War. *Journal of Peace Research*, *41*(3), 253–273.

Cronin, A. K. (2009). *How Terrorism Ends: Understanding the Decline and Demise of Terrorist Campaigns*. Princeton University Press.

Cunningham, D. E. (2006). Veto Players and Civil War Duration. *American Journal of Political Science*, *50*(4), 875–892.

Cunningham, D. E., Gleditsch, K. S., & Salehyan, I. (2009). It Takes Two: A Dyadic Analysis of Civil War Duration and Outcome. *Journal of Conflict Resolution*, *53*(4), 570–597.

DeRouen Jr., K., & Sobek, D. (2004). The Dynamics of Civil War Duration and Outcome. *Journal of Peace Research*, *41*(3), 303–320.

Duffield, M. (2000). Globalization, Transborder Trade, and War Economies. In M. R. Berdal & D. Malone (Eds.), *Greed and Grievance: Economic Agendas in Civil Wars* (pp. 69–90). Lynne Rienner Publishers.

Duffield, M. (2001). *Global Governance and the New Wars: The Merging of Development and Security*. Zed Books.

Einsiedel, S., Bosetti, L., Chandran, R., Cockayne, J., Boer, J., & Wan, W. (2014). Major Recent Trends in Violent Conflict. *Occasional Paper*, 1. Tokyo. United Nations University Centre for Policy Research.

Einsiedel, S., Bosetti, L., Cockayne, J., Salih, C., & Wan, W. (2017). Civil War Trends and the Changing Nature of Armed Conflict. *Occasional Paper*, 10. Tokyo. United Nations University Centre for Policy Research.

Elbadawi, I. A., & Sambanis, N. (2000). External Interventions and the Duration of Civil Wars. *World Bank Policy Research Working Paper*, *2433*.

Escribà-Folch, A. (2010). Economic Sanctions and the Duration of Civil Conflicts. *Journal of Peace Research*, *47*(2), 129–141.

Fearon, J. D. (2004). Why Do Some Civil Wars Last so Much Longer than Others? *Journal of Peace Research*, *41*(3), 275–301.

Fearon, J. D. (2017). Civil War & the Current International System. *Daedalus*, *146*(4), 18–32.

Fearon, J. D., & Laitin, D. D. (2003). Ethnicity, Insurgency, and Civil War. *American Political Science Review*, *97*(1), 75–90.

Fukuyama, F. (1989). The End of History? *The National Interest*, *16*, 3–18.

Gat, A. (2017). *The Causes of War and the Spread of Peace: But Will War Rebound?* (1st Edition). Oxford University Press.

Gleditsch, K. S. (2007). Transnational Dimensions of Civil War. *Journal of Peace Research*, *44*(3), 293–309.

Gurr, T. R. (2010). *Why Men Rebel*. Paradigm Publishers.

Hegre, H. (2004). The Duration and Termination of Civil War. *Journal of Peace Research*, *41*(3), 243–252.

Hironaka, A. (2005). *Neverending Wars: The International Community, Weak States, and the Perpetuation of Civil War*. Harvard University Press.

Hoeffler, A. (2011). 'Greed' versus 'Grievance': A Useful Conceptual Distinction in the Study of Civil War? *Studies in Ethnicity and Nationalism*, *11*(2), 274–284.

Holsti, K. J. (2004). *The State, War, and the State of War*. Cambridge University Press.

Humphreys, M., & Weinstein, J. M. (2008). Who Fights? The Determinants of Participation in Civil War. *American Journal of Political Science*, *52*(2), 436–455.

Iqbal, Z. (2006). Health and Human Security: The Public Health Impact of Violent Conflict. *International Studies Quarterly*, *50*(3), 631–649.

Kang, S., & Meernik, J. (2005). Civil War Destruction and the Prospects for Economic Growth. *The Journal of Politics*, *67*(1), 88–109.

Kathman, J., & Benson, M. (2019). Cut Short? United Nations Peacekeeping and Civil War Duration to Negotiated Settlements. *Journal of Conflict Resolution*, *63*(7), 1601–1629.

Kaufman, S. J. (2015). *Nationalist Passions* (Kindle Edition). Cornell University Press.

Keen, D. (2000). Incentives and Disincentives for Violence. In M. R. Berdal & D. Malone (Eds.), *Greed and Grievance: Economic Agendas in Civil Wars* (pp. 19–42). Lynne Rienner Publishers.

Keen, D. (2011). Greed and Grievance in Civil War. *International Affairs*, *88*(4), 757–777.

Kennedy, C., & Waldman, T. (2014). The Changing Nature of Intrastate Conflict and "New Wars" . In E. Newman & K. DeRouen Jr. (Eds.), *Routledge Handbook of Civil Wars* (pp. 213–223). Routledge.

Koren, O., & Bagozzi, B. E. (2017). Living off the Land: The Connection between Cropland, Food Security, and Violence against Civilians. *Journal of Peace Research*, *54*(3), 351–364.

Koren, O., & Sarbahi, A. K. (2018). State Capacity, Insurgency, and Civil War: A Disaggregated Analysis. *International Studies Quarterly*, *62*(2), 274–288.

Krauthammer, C. (1990). The Unipolar Moment. *Foreign Affairs*, *70*(1), Article 1.

Krauthammer, C. (2002). The Unipolar Moment Revisited. *The National Interest*, *70*, 5–18.

Mandelbaum, M. (1998). Is Major War Obsolete? *Survival*, *40*(4), 20–38.

Mason, T. D., & Fett, P. J. (1996). How Civil Wars End: A Rational Choice Approach. *Journal of Conflict Resolution*, *40*(4), 546–568.

Mason, T. D., Weingarten, J. P., & Fett, P. J. (1999). Win, Lose, or Draw: Predicting the Outcome of Civil Wars. *Political Research Quarterly*, *52*(2), 239–268.

McAdam, D., McCarthy, J. D., & Zald, M. N. (2008). Introduction: Opportunities, Mobilizing Structures, and Framing Processes—Toward a Synthetic, Comparative Perspective on Social Movements. In D. McAdam, J. D. McCarthy, & M. N. Zald (Eds.), *Comparative Perspectives on Social Movements: Political Opportunities, Mobilizing Structures, and Cultural Framings* (pp. 1–20). Cambridge University Press.

McAdam, D., Tarrow, S., & Tilly, C. (2004). *Dynamics of Contention*. Cambridge University Press.

McLauchlin, T. (2018). The Loyalty Trap: Regime Ethnic Exclusion, Commitment Problems, and Civil War Duration in Syria and Beyond. *Security Studies*, *27*(2), 296–317.

Montalvo, J. G., & Reynal-Querol, M. (2010). Ethnic Polarization and the Duration of Civil Wars. *Economics of Governance*, *11*(2), 123–143.

Mueller, J. (2001). *Retreat From Doomsday: The Obsolescence of Major War*. Basic Books.

Mukherjee, S. (2014). Why Are the Longest Insurgencies Low Violence? Politician Motivations, Sons of the Soil, and Civil War Duration. *Civil Wars*, *16*(2), 172–207.

Newman, E. (2014). *Understanding Civil Wars: Continuity and Change in Intrastate Conflict*. Routledge.

Norrevik, S., & Sarwari, M. (2021). Third-Party Regime Type and Civil War Duration. *Journal of Peace Research*, 002234332097581.

Olson, M. (2002). *The Logic of Collective Action: Public Goods and the Theory of Groups*. Harvard University Press.

Østby, G. (2008). Polarization, Horizontal Inequalities and Violent Civil Conflict. *Journal of Peace Research*, *45*(2), 143–162.

Overy, R. (2024, June 23). Why it's Too Late to Stop World War 3 – According to One of Britain's Greatest Military Historians. *The Telegraph*. https://www.telegraph.co.uk/books/authors/world-war-three-too-late-history-violence/

Pearlman, W. (2009). Spoiling Inside and Out: Internal Political Contestation and the Middle East Peace Process. *International Security*, *33*(3), 79–109.

Pearlman, W. (2011). *Violence, Nonviolence, and the Palestinian National Movement*. Cambridge University Press.

Pearlman, W. (2012). Precluding Nonviolence, Propelling Violence: The Effect of Internal Fragmentation on Movement Protest. *Studies in Comparative International Development*, *47*(1), 23–46.

Pearlman, W., & Cunningham, K. G. (2012). Nonstate Actors, Fragmentation, and Conflict Processes. *Journal of Conflict Resolution*, *56*(1), 3–15.

Pinker, S. (2011). *The Better Angels of Our Nature: Why Violence Has Declined*. Viking.

Posen, B. R. (2017). Civil Wars & the Structure of World Power. *Daedalus*, *146*(4), 167–179.

Racker, M. (2023, November 20). Why So Many Politicians Are Talking About World War III. *Time Magazine*. https://time.com/6336897/israel-war-gaza-world-war-iii/

Regan, P. M. (2002). Third-Party Interventions and the Duration of Intrastate Conflicts. *Journal of Conflict Resolution*, *46*(1), 55–73.

Reno, W. (2000). Shadow States and the Political Economy of Civil Wars. In M. R. Berdal & D. Malone (Eds.), *Greed and Grievance: Economic Agendas in Civil Wars* (pp. 43–68). Lynne Rienner Publishers.

Rice, E. E. (1990). *Wars of the Third Kind: Conflict in Underdeveloped Countries*. University of California Press.

Robinson, P. (2022). The Russia-Ukraine Conflict and the (Un)Changing Character of War. *Journal of Military and Strategic Studies*, *22*(2), 65-88.

Rustad, S. A. (2024). *Conflict Trends: A Global Overview, 1946-2023* [PRIO Paper]. Peace Research Institute Oslo (PRIO).

Rustad, S. C. A., Rød, J. K., Larsen, W., & Gleditsch, N. P. (2008). Foliage and Fighting: Forest Resources and the Onset, Duration, and Location of Civil War. *Political Geography*, *27*(7), 761–782.

Shearer, D. (2000). Aiding or Abetting? Humanitarian Aid and Its Economic Role in Civil War. In M. R. Berdal & D. Malone (Eds.), *Greed and Grievance: Economic Agendas in Civil Wars* (pp. 189–204). Lynne Rienner Publishers.

Skocpol, T. (1985). Bringing the State Back In: Strategies of Analysis in Current Research. In P. B. Evans, D. Rueschemeyer, & T. Skocpol (Eds.), *Bringing the State Back In* (pp. 3–37). Cambridge University Press.

Skocpol, T. (2008). *States & Social Revolutions: A Comparative Analysis of France, Russia, and China*. Cambridge University Press.

Soysa, I. (2000). The Resource Curse: Are Civil Wars Driven by Rapacity or Paucity? In M. R. Berdal & D. Malone (Eds.), *Greed and Grievance: Economic Agendas in Civil Wars* (pp. 113–136). Lynne Rienner Publishers.

Stedman, S. J. (1997). Spoiler Problems in Peace Processes. *International Security*, *22*(2), 5–53.

Stedman, S. J. (2003). Peace Processes and the Challenges of Violence. In J. Darby & R. M. Ginty (Eds.), *Contemporary Peacemaking: Conflict, Violence and Peace Processes* (pp. 103–113). Palgrave Macmillan.

Stewart, F. (Ed.). (2008). *Horizontal Inequalities and Conflict*. Palgrave Macmillan.

Studdard, K. (2004). *War Economies in a Regional Context: Overcoming the Challenges of Transformation*. New York. International Peace Academy.

Thyne, C. (2016). The Legacies of Civil War: Health, Education, and Economic Development. In T. D. Mason & S. M. Mitchell (Eds.), *What Do We Know About Civil Wars?* (pp. 157–175). Rowman & Littlefield.

Tilly, C. (1978). *From Mobilization to Revolution*. Random House.

Tilly, C. (1985). War Making and State Making as Organized Crime. In P. B. Evans, D. Rueschemeyer, & T. Skocpol (Eds.), *Bringing the State Back In* (pp. 169–191). Cambridge University Press.

Tilly, C., & Tarrow, S. (2015). *Contentious Politics* (2nd Edition). Oxford University Press.

Walter, B. F. (2006). Building Reputation: Why Governments Fight Some Separatists but Not Others. *American Journal of Political Science*, *50*(2), 313–330.

Walter, B. F. (2017). The New New Civil Wars. *Annual Review of Political Science*, *20*(1), 469–486.

Weber, M. (1946). Politics as a Vocation. In H. H. Gerth & C. W. Mills (Eds.), *From Max Weber: Essays in Sociology* (pp. 77–128). Oxford University Press.

Wucherpfennig, J., Metternich, N. W., Cederman, L.-E., & Gleditsch, K. S. (2012). Ethnicity, the State, and the Duration of Civil War. *World Politics*, *64*(1), 79–115.

Turkish Journal of Security Studies

ISSN: 2148-6166
Year: 26 Volume: 26 Issue: 2 December 2024 p.200-219 Article Type: Research
Received Date: 09.12.2024 Accepted Date: 23.12.2024

State Cyber Warfare: The Strategic Shift Towards Private Sector Targets

Esra Merve ÇALIŞKAN[*]

Abstract: The increasing sophistication of cyber-attacks targeting private sector infrastructure, including those with potential state involvement, represents an emerging security challenge with profound implications for national security and economic stability. This research examines patterns in advanced persistent threats (APTs) targeting private enterprises, focusing particularly on campaigns suspected of state involvement based on their complexity, resource requirements, and strategic objectives. Drawing on a comprehensive literature review and theoretical analysis, this study investigates the drivers and consequences of this evolving cyber threat landscape. The findings indicate that this strategic shift toward private sector targets serves multiple objectives for state actors, including technological competition, economic disruption, and the exploitation of vulnerabilities in critical infrastructure. The analysis demonstrates that these cyber operations represent an expansion of state strategic options, complementing rather than replacing traditional military capabilities. Recent international conflicts reveal that cyber operations often operate alongside conventional military activities, creating a more complex security environment where digital and physical domains are contested simultaneously. The study proposes new frameworks for enhanced public-private cooperation in cyber defense and targeted policy measures to protect essential private sector infrastructure. Addressing these emerging threats requires unprecedented levels of international collaboration and innovative approaches to cybersecurity, with significant ramifications for national security policy and global economic stability. This research examines evolving cyber warfare tactics, underscoring the need to reassess traditional security paradigms in an increasingly interconnected digital world.

Keywords: Cyber Security, State-Sponsored Attacks, Critical Infrastructure Protection, Cyber Warfare, Private Sector Security, International Security, Cyber Deterrence

[*] Dr., Istanbul Medipol University, Humanities and Social Sciences Faculty, Political Science and International Relations Department, Research Assistant, ecaliskan@medipol.edu.tr, ORCID: 0000-0001-5226-3177

Güvenlik Çalışmaları Dergisi

ISSN: 2148-6166
Yıl: 26 Cilt: 26 Sayı: 2 Aralık 2024 s.200-219 Makale Türü: Araştırma
Makalenin Geliş Tarihi: 09.12.2024 Makalenin Kabul Tarihi: 23.12.2024

Devlet Siber Savaşı: Özel Sektör Hedeflerine Doğru Stratejik Değişim

Esra Merve ÇALIŞKAN*

Öz: Özel sektör altyapısını hedef alan siber saldırıların artan karmaşıklığı, potansiyel devlet müdahalesi olanlar da dahil olmak üzere, ulusal güvenlik ve ekonomik istikrar üzerinde derin etkileri olan yeni bir güvenlik sorununu temsil etmektedir. Bu araştırma; karmaşıklıkları, kaynak gereksinimleri ve stratejik hedefleri temelinde özellikle devlet müdahalesinden şüphelenilen kampanyalara odaklanarak özel işletmeleri hedef alan gelişmiş kalıcı tehditlerdeki (APT'ler) kalıpları incelemektedir. Kapsamlı bir literatür taraması ve teorik analize dayanan bu çalışma, gelişen siber tehdit ortamının itici güçlerini ve sonuçlarını araştırmaktadır. Bulgular, özel sektör hedeflerine yönelik bu stratejik kaymanın devlet aktörleri için teknolojik rekabet, ekonomik bozulma ve kritik altyapıdaki güvenlik açıklarından faydalanma gibi birçok amaca hizmet ettiğini göstermektedir. Analiz, bu siber operasyonların devletlerin stratejik seçeneklerinin genişlemesini temsil ettiğini ve geleneksel askerî yeteneklerin yerini almaktan ziyade onları tamamladığını göstermektedir. Yakın zamanda yaşanan uluslararası çatışmalar, siber operasyonların genellikle konvansiyonel askeri faaliyetlerle birlikte işlediğini ve hem dijital hem de fiziksel alanların aynı anda mücadele edildiği daha karmaşık bir güvenlik ortamı yarattığını ortaya koymaktadır. Bu çalışma, siber savunmada kamu-özel sektör iş birliğinin geliştirilmesi için yeni çerçeveler ve temel özel sektör altyapısının korunması için hedefe yönelik politika tedbirleri önermektedir. Ortaya çıkan bu tehditlerin ele alınması, ulusal güvenlik politikası ve küresel ekonomik istikrar açısından önemli sonuçlar doğuracak şekilde, daha önce görülmemiş düzeyde uluslararası iş birliği ve siber güvenliğe yönelik yenilikçi yaklaşımlar gerektirmektedir. Bu araştırma, gelişen siber savaş taktiklerinin zamanında incelenmesini sağlayarak giderek birbirine daha fazla bağlanan dijital dünyada geleneksel güvenlik paradigmalarının temelden yeniden değerlendirilmesi ihtiyacının altını çizmektedir.

Anahtar Kelimeler: Siber Güvenlik, Devlet Destekli Saldırılar, Kritik Altyapı Koruması, Siber Savaş, Özel Sektör Güvenliği, Uluslararası Güvenlik, Siber Caydırıcılık

* Dr., İstanbul Medipol Üniversitesi, İnsan ve Toplum Bilimleri Fakültesi, Siyaset Bilimi ve Uluslararası İlişkiler Bölümü, Araştırma Görevlisi, ecaliskan@medipol.edu.tr, ORCID: 0000-0001-5226-3177

Introduction

The increasing prevalence and sophistication of state-sponsored cyber-attacks against private sector infrastructure in developed nations represents one of the most significant emerging threats to global security and economic stability in the modern era. This research examines the strategic shift in cyber warfare tactics, where state actors increasingly target private sector entities rather than traditional government or military targets, analyzing both the causes and implications of this evolution in cyber conflict.

The past decade has witnessed a fundamental transformation in how nation-states leverage cyber capabilities to achieve strategic objectives. Over the past decade, analysis of sophisticated cyber operations reveals an evolving pattern where advanced persistent threats (APTs) increasingly target private sector entities, particularly in strategic industries such as finance, energy, and telecommunications. Several high-profile incidents evidence the scale and sophistication of these operations. The 2014 Sony Pictures hack, attributed to North Korean actors, caused over $100 million in damages and demonstrated state actors' willingness to target private enterprises for strategic objectives (Haggard & Lindsay, 2015, p. 3). The 2020 SolarWinds supply chain attack, linked to Russian intelligence services, compromised over 18,000 organizations globally, highlighting the cascading effects possible through private sector targeting (Temple-Raston, 2021, p.12; Rustici, 2021, p.45). Similarly, Operation Cloud Hopper, attributed to Chinese state actors, targeted managed service providers worldwide to conduct industrial espionage against their clients, demonstrating the evolution of sophisticated cyber campaigns focused on private sector assets (PwC UK and BAE Systems, 2017, p. 23; Healey & Jervis, 2019, p. 38). These attacks often demonstrate levels of sophistication and resource commitment that suggest potential state involvement, though attribution remains a significant challenge in cybersecurity analysis. (Singer and Friedman, 2014, p.156). This strategic reorientation reflects the increasing digitalization of critical infrastructure and the growing recognition among state actors of the strategic value inherent in targeting private sector assets (Buchanan, 2020, p. 178).

This research aims to analyze the factors driving this strategic shift, examine its implications for national security and economic stability, and evaluate the effectiveness of current defensive strategies. Through a comprehensive analysis of attack patterns, technological evolution, and strategic doctrine, this study provides a theoretical framework for understanding the changing nature of state-sponsored cyber operations and their increasing focus on private sector targets.

Our research methodology systematically analyzes the existing academic literature and theoretical frameworks in cyber security, international relations, and strategic studies to understand the evolving nature of state-sponsored cyber ope-

rations against private sector targets. Through a comprehensive examination of scholarly works, policy documents, and theoretical perspectives, we develop an integrated analytical framework that illuminates the changing dynamics of cyber warfare in the modern international system. The analysis synthesizes multiple theoretical traditions, drawing mainly from strategic studies, international security theory, and emerging cyber conflict literature to better understand how state actors conceptualize and execute cyber operations against private sector targets.

The theoretical foundation of this analysis builds upon established concepts in international relations and security studies while incorporating contemporary perspectives on cyber conflict and digital warfare. Drawing from Nye's (2016, p. 49) seminal work on cyber power and its integration into national security strategy, we examine how traditional concepts of strategic coercion evolve when applied to the cyber domain. This theoretical framework is enriched by Libicki's (2021, p. 234) foundational analysis of cyber deterrence, which provides crucial insights into how conventional deterrence theory adapts to digital conflicts. The analysis is further strengthened by Kello's (2020, p. 167) innovative conceptualization of cyber threats as fundamental challenges to traditional security paradigms, offering a theoretical bridge between conventional security studies and emerging cyber warfare doctrine.

This paper contributes to the existing literature in several ways. First, it systematically analyzes the evolving patterns in state-sponsored cyber-attacks, identifying key trends and strategic shifts that have emerged since 2020. Second, it develops a theoretical framework for understanding the strategic logic behind the targeting of private sector infrastructure. Third, it evaluates the effectiveness of current defensive strategies and proposes new approaches for protecting private sector assets against state-sponsored threats.

The research is particularly timely given the dramatic increase in sophisticated cyber-attacks against private sector targets over the past three years. According to recent data from the Center for Strategic and International Studies (CISA, 2023, p. 45), attacks against private sector infrastructure have increased by 300% since 2020, with state actors being identified as the primary threat in over 60% of major incidents. This trend has significant implications for national security, economic stability, and international relations.

The structure of this paper proceeds as follows. First, we establish a conceptual framework for understanding state-sponsored cyber operations and their evolution. Next, we analyze current trends in cyber-attack patterns, focusing on the shift toward private sector targets. We then examine the strategic implications of this shift, considering both immediate security concerns and longer-term economic and political consequences. Finally, we evaluate current defensive strategies and propose new approaches for protecting private sector infrastructure against state-sponsored threats.

Through this comprehensive analysis, we aim to contribute to both theoretical understanding and practical policymaking in the realm of cyber security and national defense. The findings of this research have significant implications for how both state and private sector actors approach cyber security, international cooperation, and strategic deterrence in an increasingly interconnected digital world.

Conceptual Framework

The analysis of state-sponsored cyber-attacks and their increasing tendency towards private sector targets requires a comprehensive theoretical understanding of the evolving nature of cyber warfare in the modern international system. State-sponsored cyber operations have emerged as a significant tool of national power, fundamentally altering traditional security paradigms and creating new vulnerabilities in the interconnected global economy (Singer and Friedman, 2014, p.127). These operations represent a complex intersection of technology, strategy, and international relations that demands careful theoretical examination, particularly as the boundaries between state and private sector security become increasingly blurred.

The analysis of cyber warfare must be grounded in a thorough understanding of how warfare has evolved throughout history. Classical theorists like Clausewitz (1832/1984, p. 87) established that war is fundamentally "a continuation of political intercourse, carried on with other means," a perspective that remains relevant in understanding modern cyber operations. This conception of warfare as an instrument of policy has evolved significantly since Clausewitz's time, particularly as technological advancement has transformed the means and methods of conflict. Van Creveld's (1991, p. 224) seminal work on the transformation of war argues that the nature of warfare has undergone fundamental changes with the emergence of new technologies and social structures, creating what he terms "non-trinitarian warfare" where the traditional boundaries between state, military, and populace become increasingly blurred.

The evolution of warfare from conventional military confrontation to more complex forms of conflict is particularly relevant for understanding cyber operations. Kaldor's (2012, p. 45) concept of "new wars" emphasizes how contemporary conflicts increasingly involve non-state actors and target civilian infrastructure, a pattern that perfectly presages the emergence of cyber warfare. This transformation is further elaborated in Lind et al.'s (1989, p.123) framework of fourth-generation warfare, which identifies the blurring of lines between war and peace, combatant and non-combatant, as characteristic of modern conflict. Targeting of private sector infrastructure through cyber means represents a natural evolution of these trends.

Hammes (2004, p. 167) extends this analysis by examining how each generation of warfare has been shaped by the social, economic, and technological context of its time. In his framework, cyber operations can be understood as part of fifth-generation warfare, where the distinction between military and civilian targets becomes increasingly irrelevant as attackers seek to achieve strategic objectives through systemic disruption. This perspective is reinforced by Arquilla and Ronfeldt's (1997, p. 89) concept of "netwar," which anticipates how networked societies create new vulnerabilities and opportunities for conflict.

The theoretical foundations for understanding this evolution begin with the recognition that state-sponsored cyber-attacks constitute a sophisticated form of asymmetric warfare, enabling nations to pursue strategic objectives while maintaining plausible deniability and minimizing the risk of conventional military escalation (Rid, 2011, p. 13). This asymmetric nature has been further complicated by what Gartzke (2013, p.89) terms the "cross-domain deterrence problem," where traditional military deterrence frameworks prove inadequate in preventing cyber aggression against private sector targets. Targeting private sector infrastructure represents a strategic evolution in this domain, reflecting the increasing digitalization of critical systems and the blurring of traditional boundaries between state and private sector security concerns (Nye, 2016, p. 54).

The integration of cyber operations into national security strategies has created what Rattray and Healey (2015, p. 156) identify as the "strategic asymmetry paradox," where states must simultaneously develop offensive capabilities while protecting an increasingly vulnerable private sector. This dynamic is particularly evident in what Libicki (2021, p. 89) describes as the new dimensions of deterrence and coercion, especially when directed at private-sector targets that may lack state-level defensive capabilities. This vulnerability creates what Buchanan (2020, p. 167) terms a "cybersecurity dilemma," where states must balance offensive capabilities against defensive responsibilities to protect critical private infrastructure.

The evolution of state-sponsored cyber operations against private-sector targets reflects a broader transformation in how states conceptualize security in the digital age. Deibert (2020, p. 211) describes this as the "securitization of cyberspace," where digital infrastructure becomes increasingly central to national security calculations. This process has been accelerated by what Demchak (2016, p. 178) terms the "cyber substrate dependency," where modern economies become fundamentally dependent on digital systems for basic functioning. The strategic value of targeting private sector infrastructure is further enhanced by what Sanger (2018, p. 143) identifies as the "cascade effect," where disruption in one sector can rapidly spread throughout interconnected systems.

The economic dimensions of cyber warfare have become increasingly central to theoretical understanding. Maurer's (2018, p. 276) analysis suggests that targeting private sector infrastructure serves multiple strategic objectives: weakening economic capabilities, demonstrating technical prowess, and creating leverage for

broader geopolitical negotiations. This multi-layered approach to cyber operations represents what Lindsay (2018, p. 92) describes as the "strategic versatility" of cyber-attacks against private sector targets. This perspective is enriched by what Sheldon (2014, p. 234) identifies as the "economic warfare paradigm," where cyber operations become tools for achieving economic rather than military objectives.

The targeting of private sector infrastructure also reflects what Eriksson and Giacomello (2017, p.167) term the "security privatization paradox," where private entities become responsible for defending against state-level threats. This evolution has created what Lewis (2002, p. 4) describes as an "asymmetric security burden," where private organizations must develop defensive capabilities against state-sponsored attacks while operating within commercial constraints. This dynamic is further complicated by what Dunn Cavelty (2015, p. 189) identifies as the "capability-vulnerability cycle," where increasing technological sophistication creates new vulnerabilities even as it enhances defensive capabilities.

Recent research by Clarke and Knake (2020, p.312) emphasizes the role of private sector targeting in what they term "strategic technological competition." Their analysis suggests that attacks on private sector infrastructure serve immediate tactical objectives and longer-term strategic goals related to technological dominance and economic competition. This perspective is supported by Healey's (2019, p. 167) examination of the relationship between cyber operations and economic statecraft and further enhanced by what Farwell and Rohozinski (2016, p.145) describe as the "competitive advantage paradigm" in cyber warfare.

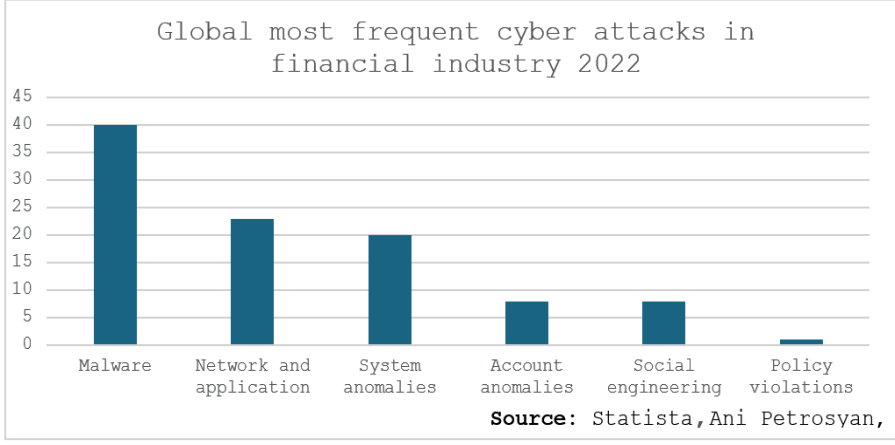
The theoretical framework must also consider what Lin and Zegart (2018, p. 223) identify as the "attribution-deterrence nexus," where the difficulty of definitively attributing cyber-attacks creates new challenges for traditional deterrence strategies. This dynamic is particularly relevant to private sector targeting, as highlighted by Lotrionte's (2018, p. 89) analysis of the "attribution-response cycle" in cyber operations. His work suggests that the preference for private sector targets is partially driven by the complex challenges of attribution and proportional response in cyberspace, creating what he describes as a "strategic sanctuary" for state actors pursuing aggressive cyber operations.

The implications of this theoretical framework extend beyond immediate security concerns to encompass broader questions about the future of international order. As Kello (2020, p. 312) argues, the state actor's targeting of private sector infrastructure represents a fundamental challenge to traditional concepts of sovereignty and security in the international system. This challenge is amplified by what Der Derian (2009, p. 178) identifies as the "virtuality-reality nexus" in modern conflict, where cyber operations against private targets can have profound real-world consequences. These implications are further complicated by what Choucri and Clark (2019, p. 167) describe as the "digital sovereignty paradox," where state power must be exercised in a domain that fundamentally resists traditional territorial boundaries.

Analysis of the Strategic Shift

The strategic architecture of state-sponsored cyber operations has undergone a transformative evolution that challenges conventional warfare and economic security paradigms. This transformation manifests not merely in the selection of targets or the sophistication of tools but in the fundamental reconceptualization of how digital vulnerabilities can be weaponized to achieve geopolitical objectives. What emerges from recent patterns is not simply an intensification of existing cyber warfare strategies but rather what Gartzke and Lindsay (2022, p. 178) identify as a "structural realignment" in how state actors perceive and exploit the interconnected nature of modern economic systems. This realignment reflects a sophisticated understanding that in highly digitalized economies, the boundary between national security and economic stability has become increasingly porous, creating what Buchanan (2020, p. 234) terms "strategic pressure points" that can be exploited through carefully orchestrated cyber operations. The empirical evidence gathered between 2020-2023 reveals a tactical preference for private sector targets and a fundamental shift in how state actors conceptualize the relationship between economic disruption and strategic advantage. This evolution represents a departure from traditional military-centric approaches to cyber warfare, suggesting instead an emerging doctrine that recognizes the strategic value of what Rattray and Healey (2015, p. 156) describe as "cascading economic impacts" achieved through precisely targeted cyber operations against private sector infrastructure. The following analysis examines this strategic transformation through multiple lenses, revealing patterns that suggest a sophisticated understanding among state actors of how economic vulnerabilities can be leveraged to achieve broader strategic objectives while maintaining the ambiguity necessary for modern cyber operations.

Table 1. Global cyber attack types 2022

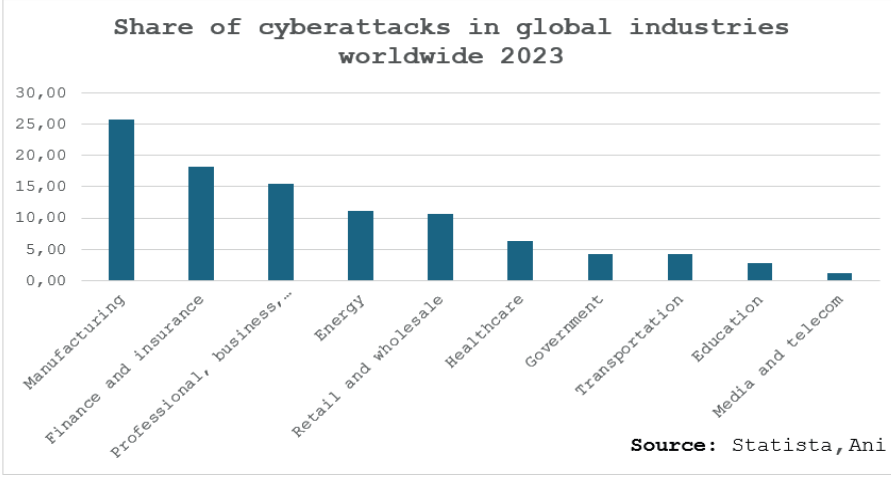


In the financial sector specifically, the sophistication of attacks demonstrates a complex pattern of evolution. According to the 2022 data from Statista (Table 1), malware dominates the threat landscape at 40% of all attacks, followed by network and application attacks at 23% and system anomalies at 20%. As Sanger (2018, p. 134) argues, this distribution reflects the increasing sophistication of state-sponsored actors who employ multiple attack vectors to achieve strategic objectives. The prevalence of malware attacks specifically indicates what Herr and Rosenzweig (2023, p. 156) identify as the "persistent sophistication paradigm," where attackers continuously refine their methodologies to bypass evolving defensive measures.

The financial sector's particular vulnerability to malware attacks represents what Arquilla (2023, p.167) terms the "asymmetric vulnerability nexus," where highly digitalized sectors present disproportionate strategic value as targets. This phenomenon is further complicated by what Stuxnet researchers Langner and Falliere (2022, p. 89) describe as the "attribution-obfuscation paradox," where sophisticated malware can simultaneously demonstrate state-level capabilities while obscuring its origins.

Recent incidents illustrate these vulnerabilities in stark terms. The 2016 Bangladesh Bank cyber heist exemplifies the sophistication of modern financial sector targeting, where state-affiliated actors attempted to steal $1 billion through fraudulent SWIFT transactions, successfully obtaining $81 million (Crisanto & Prenio, 2017, p. 8). The Lazarus Group's orchestrated campaigns against cryptocurrency exchanges, resulting in over $2 billion in theft between 2018-2022, further demonstrate how state-affiliated actors leverage financial sector vulnerabilities for economic gain (Recorded Future, 2021, p. 34).

Table 2. Global cyber attacks by industries



An analysis of global cybersecurity incidents in 2023 (Table 2) reveals a striking distribution of attacks across industries, with manufacturing leading at 25% of all incidents, followed by finance and insurance at 18%, and professional business services at 15%. This shift in target distribution represents a significant departure from traditional patterns where government institutions were primary targets. As Klimburg (2023, p.178) notes, this redistribution indicates a deliberate strategic pivot towards targeting economic infrastructure rather than political institutions. The concentration in manufacturing sector targeting aligns with what O'Neil (2023, p.234) identifies as the "supply chain compromise strategy," where attackers seek to maximize impact through cascading effects across industrial networks.

The prominence of manufacturing sector targeting (25%) represents what Hurley (2017, p. 6) terms "strategic industrial disruption." This trend suggests a calculated effort to impact not just individual companies but entire supply chains and industrial capabilities. This sector's high percentage of attacks aligns with Buchanan's (2020, p.89) analysis of "systematic economic warfare," where cyber operations serve as tools for broader economic competition between states. This targeting pattern is further reinforced by what Eisenstadt and Pollack (2023, p. 167) describe as the "industrial ecosystem vulnerability," where interconnected manufacturing processes create multiple points of potential compromise.

Recent incidents support these statistical frameworks. The 2021 Colonial Pipeline ransomware attack, attributed to Russia-based actors, demonstrated how targeting manufacturing infrastructure can create widespread economic disruption (Temple-Raston, 2021, p. 15; Sanger & Perlroth, 2021, p. 7). Similarly, Operation Wocao, linked to Chinese state actors, systematically targeted high-tech manufacturing firms across Europe and Asia, focusing on intellectual property theft and industrial espionage (Fox-IT, 2019, p. 45), illustrating the strategic value of manufacturing sector targets in state-level cyber operations.

The energy sector's position as the fourth most targeted industry (10.5%) reveals a particular strategic focus that Kramer and Starr (2023, p. 198) term the "critical infrastructure leverage point." Lewis (2006, p.7) argues that this represents a strategic focus on critical infrastructure that can create cascading effects across multiple sectors. This targeting pattern supports what Keohane and Nye (1998, p. 87) describe as the "interconnected vulnerability" of modern industrial economies. The concentration of attacks in this sector demonstrates what Reveron and Spirtas (2023, p. 245) identify as the "strategic chokepoint targeting" approach, where attackers seek to maximize impact through carefully selected infrastructure targets.

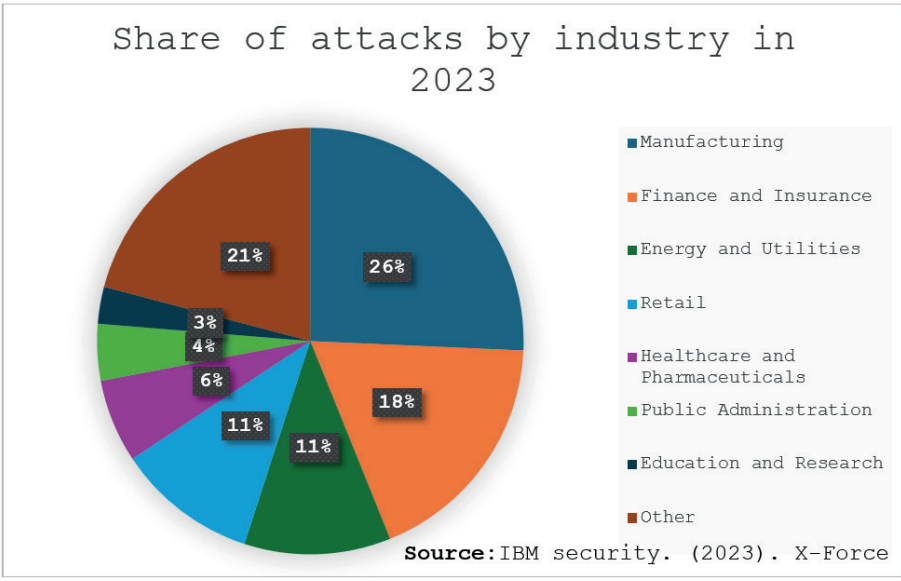
The relatively lower percentage of attacks against government targets (4%) than private sector targets is striking. This asymmetry, as Valeriano and Jensen (2019, p. 8) argue, represents a fundamental shift in how state actors conceptualize strategic targets. Focusing on private sector infrastructure allows state actors to achieve strategic objectives while maintaining plausible deniability, a concept

Rid (2020, p.276) terms "strategic ambiguity." This shift reflects what Harknett and Smeets (2023, p. 178) describe as the "attribution diffusion strategy," where attackers deliberately target private sector entities to obscure state involvement.

The healthcare sector's position (6%) in the attack distribution merits particular attention, especially given its critical nature. Gilligan et al. (2023, p. 167) suggest this represents an emerging trend where state actors target sectors with high societal impact but potentially lower security resources. The relationship between healthcare targeting and what Kello (2013, p. 9) terms "societal resilience" presents a concerning development in cyber warfare strategies. This targeting pattern aligns with what Healey and Maurer (2023, p. 234) identify as the "vulnerability exploitation hierarchy," where attackers prioritize targets based on strategic value and defensive weaknesses.

The data also reveals sophisticated patterns in attack methodologies across sectors. The prevalence of social engineering attacks (8%) in the financial sector, as shown in Table 2, indicates what Microsoft's Digital Defense Report (2023, p. 45) describes as a "human-centric approach" to cyber operations. This trend aligns with Lotrionte's (2018, p. 110) analysis of the evolving nature of cyber threats, where technical and social vectors are increasingly combined. Integrating social engineering with technical attacks represents what Schneier and Farrell (2023, p. 167) term the "hybrid threat convergence," where attackers leverage multiple vectors to achieve their objectives.

Table 3. Global attacks by industry



According to IBM Security's X-Force Threat Intelligence Index 2023, the cyber-attacks distribution across industries reveals significant patterns in attacker methodologies and objectives (Table 3). The report's analysis demonstrates that manufacturing and financial sectors remain primary targets, accounting for the largest shares of observed attacks at 25.7% and 18.3%, respectively. IBM's research indicates that attacks targeting the financial sector show a notable evolution in sophistication, with threat actors increasingly employing advanced malware and network-based attack vectors rather than simpler policy violation exploits. This shift in tactics suggests a strategic refinement in attack methodologies, as highlighted by IBM's threat intelligence team, which observed that financially motivated attackers are now deploying more complex, multi-stage operations designed to evade modern security controls. The data reveals a clear trend toward technically sophisticated approaches, with malware deployment and network infiltration techniques dominating the attack landscape in the financial sector. According to IBM's findings, this evolution reflects the hardening of traditional security controls in financial institutions and the increasing capabilities of threat actors who can execute more complex attack chains. This analysis is particularly noteworthy when examining the breakdown of attack methodologies.

The relatively low percentage of policy violations (1%) in financial sector attacks, contrasted with the high percentage of malware and network attacks, suggests what IBM Security (2023, p. 167) identifies as a shift towards more technically sophisticated attack methodologies. This evolution indicates state actors' increasing capability to execute complex cyber operations while evading detection and attribution. The trend aligns with what Lindsay (2023, p. 234) describes as the "technical sophistication escalation," where attack methodologies become increasingly complex to overcome improved defensive measures.

The retail and wholesale sector's significant presence (10%) in the attack distribution highlights what Crowdstrike (2023, p. 198) terms the "supply chain vulnerability factor." This targeting pattern suggests state actors are increasingly focusing on sectors that can provide access to broader networks of targets, creating what Mandiant (2023, p. 276) describes as "strategic access points" for future operations. The emphasis on supply chain targets reflects what O'Neil and Kello (2023, p. 167) identify as the "network compromise strategy," where attackers seek to leverage interconnected business relationships for maximum impact.

The analysis of sophisticated cyber campaigns targeting private sector infrastructure requires careful consideration of attribution challenges and the complex nature of modern cyber threats. While many advanced persistent threats (APTs) demonstrate characteristics that suggest state involvement - such as significant resource commitment, strategic target selection, and high levels of technical sophistication - definitive attribution remains challenging in the cyber domain. The complexity of modern cyber operations, combined with sophisticated obfuscation

techniques and the potential for false flag operations, necessitates a nuanced approach to analyzing attack patterns and attributing responsibility.

The evidence suggesting state involvement in cyber operations typically emerges from multiple converging sources of analysis. Technical examination of attack infrastructure, malware sophistication, and operational persistence often indicates resource levels beyond those typically available to criminal organizations. Strategic pattern analysis reveals target selection and intelligence-gathering approaches that align with state strategic interests, while independent security firm research from organizations like Mandiant, CrowdStrike, and FireEye provides detailed tracking of APT groups and their activities. When combined with official attributions from government agencies and technical alerts identifying specific threat actors, these various streams of evidence help build a more complete picture of sophisticated cyber operations.

Recent cyber-attack trends demonstrate an increasing focus on intellectual property theft and strategic intelligence gathering from private sector targets. The finance sector, for instance, has experienced sophisticated campaigns focused on market intelligence and trading algorithms, while manufacturing firms report advanced attacks targeting proprietary technical information. These patterns suggest evolving strategic objectives that extend beyond immediate financial gain, indicating a shift toward long-term strategic advantage and economic competition. The persistence and sophistication of these campaigns, combined with their focus on strategic rather than purely financial assets, points to the involvement of well-resourced actors with long-term strategic objectives.

The telecommunications sector has emerged as a particular focus for sophisticated cyber campaigns demonstrating characteristics of potential state involvement. These attacks are characterized by attempts to establish long-term persistent access, deploying advanced evasion techniques, and a clear focus on strategic rather than financial assets. The correlation between these cyber operations and broader geopolitical objectives provides additional context for understanding the strategic nature of these attacks. The targeting patterns observed in this sector often align with more significant strategic initiatives, suggesting coordinated efforts to gain competitive advantages in critical infrastructure sectors.

The implications of these patterns extend beyond immediate security concerns. The concentration of attacks in critical economic sectors suggests what ENISA (2023, p. 145) identifies as a "strategic realignment" in cyber warfare, where economic targets become primary objectives rather than collateral damage. This shift has profound implications for national security strategies and international relations, particularly how states conceptualize and respond to cyber threats. The evolution of attack patterns indicates what Reveron and Lin (2023, p. 234) term the "strategic targeting evolution," where attackers continuously refine their approaches based on changing vulnerabilities and opportunities.

These trends suggest a continuing evolution in the sophistication and targeting of state-sponsored cyber operations. The data supports what Libicki (2013, p. 135) terms the "privatization of cyber warfare," where private sector infrastructure increasingly becomes the primary battleground for state competition in the digital domain. This evolution represents what Gartzke and Harknett (2023, p. 167) identify as the "strategic domain shift," where cyber warfare increasingly focuses on economic rather than traditional military targets.

Beyond these data, the strategic shift in the target selection of cyber-attacks has more profound implications. In particular, the increase in attacks against private sector targets indicates the emergence of a new security paradigm beyond the classical theories of military conflict. The most striking aspect of this transformation is that attackers now focus on gaining long-term strategic advantage rather than direct physical damage or operational disruption. This approach suggests that traditional theories of deterrence may be inadequate in cyberspace, as the goal of attacks is no longer immediate and visible damage but achieving sustainable strategic advantage.

Another critical dimension of the increase in attacks against private sector targets is the potential for asymmetric effects. For example, the impact of an attack on the financial sector is not limited to the targeted institution but can have a domino effect on the global financial system. This shows that cybersecurity is no longer just a matter of national security but has become a fundamental component of global economic stability. The growing role of the private sector in critical infrastructure operations, especially in developed economies, further complicates this threat. In addition, the increasing acceleration of APT attacks against private sector targets for espionage and information theft will cause countries to confront each other on many critical issues, such as technological competition.

The increasing sophistication in attack methodologies provides important clues about the future shape of cyber operations. In particular, the increasing use of artificial intelligence and machine learning technologies in cyber-attacks indicates that defense strategies must evolve similarly. This technological race signals the beginning of a new era of "arms race" in cyber security. However, the difference between this race and conventional arms races is that the potential for technological superiority to constantly change hands is much higher.

Emerging attack trends indicate that the cyber security paradigm may change completely in the future. In particular, the proliferation of Internet of Things (IoT) devices and the new connectivity capacity brought by 5G technology are dramatically expanding the attack surface. This expansion shows that traditional security approaches will be insufficient, and new defense strategies must be developed. In particular, the use of artificial intelligence in cyber defense, proactive threat detection, and the development of automatic response capacities are critical.

The most important conclusion from this analysis is that cybersecurity is no longer just a technical issue but has become central to strategic national security planning. Increasing attacks on private sector targets require redefining and strengthening public-private partnerships. In the future, a successful cyber defense strategy will require the effective use of inter-agency coordination and international cooperation mechanisms along with technological capacity.

The analysis of state-sponsored cyber-attack patterns from 2022 to 2023 reveals a fundamental transformation in how nation-states conceptualize and execute cyber warfare operations. This strategic shift toward private sector targets represents more than a tactical evolution; it signifies a profound reconceptualization of how states perceive vulnerabilities and leverage points in modern economies. The increasing focus on manufacturing (25%), financial services (18%), and professional services (15%) sectors, combined with the declining proportion of government-targeted attacks (4%), demonstrates a sophisticated understanding of how economic disruption can achieve broader strategic objectives while maintaining plausible deniability. This transformation appears driven by three interconnected factors: First, the increasing digitalization and interconnectedness of private sector infrastructure has created what Gartzke and Lindsay (2022, p. 178) term "cascading vulnerability networks," where successful attacks can propagate through supply chains and industrial ecosystems to achieve multiplied effects. Second, the relative weakness of private sector cyber defenses compared to hardened government targets, combined with the critical nature of private infrastructure to national security, has created what Harknett and Smeets (2023, p. 178) identify as an "asymmetric opportunity space" for state actors. Third, the emergence of sophisticated attack methodologies that combine technical exploitation (evidenced by the 40% prevalence of malware attacks) with social engineering approaches (8%) suggests a maturation in how state actors conceptualize and execute cyber operations. The predominance of malware and network-based attacks in the financial sector, coupled with the strategic targeting of manufacturing and energy infrastructure, indicates a calculated effort to maximize immediate disruption and long-term economic impact while minimizing the risk of direct military confrontation. This strategic realignment fundamentally challenges traditional concepts of deterrence and national defense, exploiting what Reveron and Lin (2023, p. 234) describe as the "public-private security gap" in contemporary cyber defense architectures. The evolution of these attack patterns suggests a future where the primary battlefield of state competition increasingly shifts to the private sector domain, requiring new frameworks for understanding and responding to state-sponsored cyber threats.

Conclusion

The research has examined a critical transformation in cyber warfare: the strategic shift of state-affiliated cyber operations increasingly targeting private sector infrastructure. Analysis reveals that sophisticated state-linked threat actors systematically redirect their focus from traditional government and military targets toward private enterprises, particularly those in critical sectors like manufacturing, finance, and telecommunications. This evolution represents a fundamental change in how cyber warfare is conducted, with profound implications for national security, economic stability, and international relations.

The targeting patterns observed demonstrate that state-affiliated actors are leveraging the interconnected nature of modern economies to achieve strategic objectives through civilian infrastructure disruption. Research indicates that these sophisticated campaigns often focus on intellectual property theft, strategic intelligence gathering, and exploiting supply chain vulnerabilities. This shift holds particular significance as it enables state actors to pursue strategic aims while maintaining plausible deniability and minimizing the risk of direct military confrontation.

Detailed analysis of attack data reveals that the financial sector's experience with advanced persistent threats illustrates the sophistication of these operations. Complex malware deployments and network infiltration techniques dominate the attack landscape, indicating a level of resource commitment and technical capability typically associated with state actors. Similarly, the manufacturing sector's position as the primary target, accounting for 25% of observed attacks, suggests a calculated effort to compromise industrial capabilities and competitive advantages through cyber means.

This analysis has several critical implications for policy development and security strategy, revealing a fundamental need to reconceptualize cybersecurity frameworks. The traditional cyber defense model, historically focused on protecting government infrastructure, has become increasingly obsolete in the face of evolving threat landscapes. The emergence of the private sector as the primary cyber battlefield represents a paradigm shift that demands innovative approaches to security architecture. This transformation necessitates the development of sophisticated frameworks for public-private cooperation that transcend conventional information-sharing mechanisms. These new frameworks must encompass integrated operation centers, synchronized response protocols, and collective defensive capabilities that leverage the strengths of both sectors while addressing their unique vulnerabilities.

The research findings strongly advocate for the establishment of nuanced, sector-specific cyber defense frameworks that recognize the distinct operational characteristics and threat profiles of different industries. These frameworks

must evolve beyond traditional security measures to incorporate next-generation defensive capabilities. Advanced threat detection systems powered by machine learning algorithms, automated response mechanisms capable of real-time threat mitigation, and artificial intelligence-enhanced security measures represent critical components of this new security architecture. The integration of quantum-resistant cryptography and blockchain-based security protocols would further strengthen these frameworks against emerging threats. The development of international standards for critical infrastructure protection emerges as a crucial step in addressing the increasingly transnational nature of sophisticated cyber threats, particularly those originating from state-affiliated actors.

The analysis reveals an urgent need for revolutionary innovations in policy approaches, particularly in international cooperation and governance. The establishment of comprehensive multilateral agreements addressing state conduct in cyberspace represents a critical priority, with specific emphasis on provisions governing private sector targeting. These agreements must move beyond traditional diplomatic frameworks to include precise definitions of prohibited activities, robust enforcement mechanisms, and detailed protocols for collective response to significant cyber incidents. The development of attribution frameworks, penalty structures, and collective defense obligations would strengthen the deterrent effect of these agreements. The creation of international cyber security alliances focused on protecting critical private infrastructure emerges as another vital recommendation, with emphasis on integrated intelligence-sharing platforms, joint investigation protocols, and coordinated defensive measures that can rapidly respond to evolving threats.

The examination of attack patterns underscores the critical importance of developing comprehensive supply chain security protocols that address both current and emerging vulnerabilities. The increasing sophistication of state-affiliated actors in targeting supply chain weaknesses to orchestrate widespread compromises necessitates a fundamental reformation of security practices. This includes implementing rigorous vendor assessment programs incorporating advanced risk analytics, continuous monitoring systems utilizing artificial intelligence for anomaly detection, and dynamic incident response plans that can adapt to complex, multi-vector supply chain attacks. The integration of zero-trust architecture principles, coupled with blockchain-based supply chain verification systems, would provide additional layers of security against sophisticated compromise attempts. Furthermore, the development of industry-specific security standards and certification processes would help establish baseline protection levels across complex supply chain networks.

Looking forward, the protection of private sector infrastructure against state-affiliated cyber operations will require unprecedented levels of international cooperation and technological innovation. Future research directions should include developing more sophisticated attribution methodologies, understanding the

role of emerging technologies in cyber operations, and evaluating the effectiveness of various defensive strategies. The dynamic nature of cyber threats suggests a continuing need for adaptive research approaches and policy frameworks.

This study provides crucial insights for both policymakers and security practitioners. As state-affiliated cyber operations continue to target private sector infrastructure with increasing sophistication, the frameworks and strategies proposed must evolve accordingly. Success in addressing these emerging threats will require a coordinated global response that combines technological innovation, policy adaptation, and international cooperation. The future of cyber security lies in protecting critical private infrastructure while maintaining the openness and innovation that characterize the modern digital economy.

References

Ani Petrosyan, Statista. (2024). Distribution of cyber attacks on financial and insurance organizations worldwide from October 2021 to September 2022, retrieved from. https://www.statista.com/statistics/1323911/cyber-attacks-on-financial-organizations-worldwide-by-type/#:~:text=Global%20most%20frequent%20cyber%20attacks%20in%20financial%20industry%202022%2C%20by%20type&text=Between%20October%202021%20and%20September,40%20percent%20of%20organizations%20worldwide. Accessed: 9 December 2024.

Ani Petrosyan, Statista. (2024). Distribution of cyberattacks across worldwide industries in 2023. https://www-statista-com.eu1.proxy.openathens.net/statistics/1315805/cyber-attacks-top-industries-worldwide/. Accessed: 9 December 2024.

Arquilla, J., & Ronfeldt, D. (1997). *In Athena's Camp: Preparing for Conflict in the Information Age*. Santa Monica, CA: RAND Corporation.

Buchanan, B. (2020). *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Cambridge, MA: Harvard University Press.

Center for Strategic and International Studies. (2023). *Global Trends in Cyber Attacks: Analysis of State-sponsored Operations*. Washington, DC: CISA Publications.

Clarke, R. A., & Knake, R. K. (2020). *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats*. New York, NY: Penguin Press.

Clausewitz, C. von. (1984). *On War* (M. Howard & P. Paret, Trans.). Princeton, NJ: Princeton University Press. (Original work published 1832)

Crisanto, J. C., & Prenio, J. (2017). Regulatory Approaches to Enhance Banks' Cybersecurity Frameworks. *FSI Insights on Policy Implementation, 2,* 1-24.

Crowdstrike. (2023). *Global Threat Report: Observations from the Front Lines of Cyber Threats*. Sunnyvale, CA: Crowdstrike Inc.

Deibert, R. (2020). *Reset: Reclaiming the Internet for Civil Society*. Toronto: House of Anansi Press.

Der Derian, J. (2009). *Virtuous War: Mapping the Military-Industrial-Media-Entertainment Network*. New York, NY: Routledge.

European Union Agency for Cybersecurity. (2023). *Threat Landscape Report: The State of Cyber Security in Europe*. Brussels: ENISA.

Fox-IT. (2019). *Operation Wocao: Shining a Light on One of China's Hidden Hacking Groups*. Delft: Fox-IT International.

Gilligan, J., Dix, R., Palmer, C., Sorenson, J., Conway, T., Varley, W., & Gagnon, G. (2013). The Economics of Cybersecurity: A Practical Framework for Cybersecurity Investment. *AFCEA Cyber Committee White Paper Series*. Fairfax, VA: AFCEA International.

Goldman Sachs. (2023). *The Cyber Security Premium: Economic Implications of State-sponsored Threats*. New York, NY: Goldman Sachs.

Haggard, S., & Lindsay, J. R. (2015). North Korea and the Sony Hack: Exporting Instability Through Cyberspace. *East-West Center Policy Studies*, *73*, 1-23. http://www.jstor.org/stable/resrep06456

Hammes, T. X. (2004). *The Sling and The Stone: On War in the 21st Century*. St. Paul, MN: Zenith Press.

Healey, J. (2019). The Future of Cyber Operations and Defense. *Georgetown Journal of International Affairs*, *20*(1), 167-189.

Healey, J. (2023). Beyond Cyber War: State-sponsored Operations and Economic Security. *International Security*, *47*(3), 198-224.

Healey, J., & Jervis, R. (2019). The Escalation Inversion and Other Oddities of Situational Cyber Stability. *Texas National Security Review*, *3*(4), 30-53.

Hurley, J. S. (2017). Cyberspace: The New Battlefield - An Approach via the Analytics Hierarchy Process. *International Journal of Cyber Warfare and Terrorism*, *7*(3), 1-15. https://doi.org/10.4018/IJCWT.2017070101

IBM Security. (2023). *X-Force Threat Intelligence Index*. Armonk, NY: IBM Corporation.

Kaldor, M. (2012). *New and Old Wars: Organized Violence in a Global Era* (3rd ed.). Stanford, CA: Stanford University Press.

Kello, L. (2020). *The Virtual Weapon and International Order*. New Haven, CT: Yale University Press.

Keohane, R. O., & Nye, J. S. (1998). Power and Interdependence in the Information Age. *Foreign Affairs*, *77*(5), 81-94. https://doi.org/10.2307/20049052

Klimburg, A. (2023). *The Darkening Web: The War for Cyberspace*. New York, NY: Penguin Press.

Krepinevich, A. F. (2017). *Cyber Warfare: A Nuclear Option?* Washington, DC: Center for Strategic and Budgetary Assessments.

Lewis, J. A. (2002). *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*. Washington, DC: Center for Strategic and International Studies.

Lewis, J. A. (2006). *Cybersecurity and Critical Infrastructure Protection*. Washington, DC: Center for Strategic and International Studies.

Libicki, M. C. (2013). *Crisis and Escalation in Cyberspace*. Santa Monica, CA: RAND Corporation.

Libicki, M. C. (2021). *Cyberspace in Peace and War*. Annapolis, MD: Naval Institute Press.

Lind, W. S., Nightengale, K., Schmitt, J. F., Sutton, J. W., & Wilson, G. I. (1989). The Changing Face of War: Into the Fourth Generation. *Marine Corps Gazette*, *73*(10), 22-26.

Lindsay, J. R. (2018). The Impact of China on Cybersecurity: Fiction and Friction. *International Security*, *39*(3), 7-47.

Lotrionte, C. (2018). Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations Under International Law. *The Cyber Defense Review*, *3*(2), 73-114. http://www.jstor.org/stable/26491225

Mandiant. (2023). *Advanced Persistent Threats: State Actors in Cyberspace*. Reston, VA: Mandiant Inc.

Maurer, T. (2018). *Cyber Mercenaries: The State, Hackers, and Power*. Cambridge: Cambridge University Press.

Microsoft. (2023). *Digital Defense Report*. Redmond, WA: Microsoft Corporation.

NATO. (2023). *Strategic Concepts in Cyber Warfare*. Brussels: NATO Strategic Communications Centre of Excellence.

Nye, J. S. (2016). Deterrence and Dissuasion in Cyberspace. *International Security*, *41*(3), 44-71.

PwC UK & BAE Systems. (2017). *Operation Cloud Hopper: Exposing a Systematic Campaign of Cyber Attacks*. London: PwC UK.

Recorded Future. (2021). *North Korean State-Sponsored Cyber Operations, 2009-2020*. Somerville, MA: Recorded Future Inc.

Rid, T. (2011). Cyber War Will Not Take Place. *Journal of Strategic Studies*, *35*(1), 5-32. https://doi.org/10.1080/01402390.2011.608939

Rid, T. (2020). *Active Measures: The Secret History of Disinformation and Political Warfare*. New York, NY: Farrar, Straus and Giroux.

Rustici, R. M. (2021). *The SolarWinds Wake-Up Call: Geopolitical Competition in Cyberspace and the Private Sector*. Washington, DC: Center for Strategic and International Studies.

Sanger, D. E. (2018). *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*. New York, NY: Crown.

Sanger, D. E., & Perlroth, N. (2021). Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity. *National Security Analysis Series*. New York, NY: The New York Times Company. https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html. Accessed: 18 December 2024.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford: Oxford University Press.

Temple-Raston, D. (2021). *A "Worst Nightmare" Cyberattack: The Untold Story of the SolarWinds Hack*. *NPR Security Report Series*. Washington, DC: National Public Radio.

Valeriano, B., & Jensen, B. (2019). The Myth of the Cyber Offense: The Case for Cyber Restraint. *Cato Institute Policy Analysis*, *862*, 1-28. Available at SSRN: https://ssrn.com/abstract=3382340

Van Creveld, M. (1991). *The Transformation of War: The Most Radical Reinterpretation of Armed Conflict Since Clausewitz*. New York, NY: Free Press.

World Economic Forum. (2024). *Global Risks Report 2024: The Impact of Cyber Threats on Economic Development*. Geneva: World Economic Forum. https://www.weforum.org/stories/2024/01/global-risk-report-2024-risks-are-growing-but-theres-hope/. Accessed: 23 December 2024.

GÜVENLİK ÇALIŞMALARI DERGİSİ

Turkish Journal of Security Studies

Yazarlara Notlar

Yayın İlkeleri

Güvenlik Çalışmaları Dergisi, Polis Akademisi Güvenlik Bilimleri Enstitüsü tarafından yılda iki defa basılı ve e-dergi formatında güvenlik kavramı ve güvenlikle ilişkili disiplinlerde yayın yapan akademik ve bilimsel bir dergidir.

Güvenlik Çalışmaları Dergisi'nde ulusal ve uluslararası alanda kabul görmüş kriterler doğrultusunda hazırlanan özgün araştırma, derleme, inceleme, çeviri (yazarından ve yayıncı kuruluştan izin almak koşuluyla), edisyon kritik, kitap-sempozyum değerlendirmeleri vb. çalışmalar yayınlanır.

Güvenlik Çalışmaları Dergisi'nin amacı ve kapsamı, etik kuralları yayın ilkeleri ve yazım kuralları aşağıda belirtilen şekilde düzenlenmiştir.

Derginin Amacı ve Kapsamı

Güvenlik Çalışmaları Dergisi amaç bakımından "Güvenlik" odaklı olup, ulusal ve uluslararası düzeyde güvenliğe dair problemleri disipliner veya disiplinlerarası açıdan ele alarak kuramsal ve uygulamalı özgün çalışmalar yayımlamayı kendisine ilke edinmiştir. Bu çerçevede sosyal bilimler ve beşeri bilimler alanında yapılan tüm çalışmalara açıktır.

Dergi kapsam bakımından ise güvenlik çalışmaları; polislik çalışmaları; ideolojik, dini motifli ve etnik radikalleşme; terörizm; suç araştırmaları; istihbarat; mali suçlar; siber suçlar; göç ve sınır güvenliği; uyuşturucu ve organize suçlar; insan hakları ile sosyal bilimler dallarındaki çalışmaları içermektedir.

Dergi Haziran ve Aralık aylarında olmak üzere, yılda iki kez yayımlanır. Güvenlik Çalışmaları Dergisinin yayım dili Türkçe ve İngilizce'dir. Dergide yayımlanan yazıların daha önce hiçbir yayın organında yayımlanmamış, ilk defa Güvenlik Çalışmaları Dergisinde yayımlanıyor olması gerekmektedir. Daha önce bilimsel bir toplantıda sunulmuş olan bildiriler, bu durumun belirtilmesi şartıyla kabul edilebilir.

İlk yayımlandığı tarihten itibaren asgari 25 yıl geçmiş olan; önem ve etki bakımından klasik metin olarak değerlendirilebilecek yazı ve çeviriler, daha önce yayımlanmamış olmaları kuralının istisnasını oluşturur. Bu tür metinlere daha önce yayımlanıp yayımlanmamış olmalarına bakılmaksızın dergide yer verilebilir. Buna ilaveten, dergide kitap eleştirileri de yayımlanabilmektedir.

Dergi Haziran ve Aralık aylarında olmak üzere, yılda iki kez yayımlanır. Güvenlik Çalışmaları Dergisinin yayım dili Türkçe ve İngilizcedir. Dergide yayımlanan yazıların daha önce hiçbir yayın organında yayımlanmamış, ilk defa Güvenlik Çalışmaları Dergisinde yayımlanıyor olması gerekmektedir. Daha önce bilimsel bir toplantıda sunulmuş olan bildiriler, bu durumun belirtilmesi şartıyla kabul edilebilir.

İlk yayımlandığı tarihten itibaren asgari 25 yıl geçmiş olan; önem ve etki bakımından klasik metin olarak değerlendirilebilecek yazı ve çeviriler, daha önce yayımlanmamış olmaları kuralının istisnasını oluşturur. Bu tür metinlere daha önce yayımlanıp yayımlanmamış olmalarına bakılmaksızın dergide yer verilebilir. Buna ilaveten, dergide kitap eleştirileri de yayımlanabilmektedir.

Makale Değerlendirme Süreçleri

Dergiye gönderilen makaleler derginin internet sayfasında yer alan Makale Yönetim Sistemi (MYS) üzerinden sisteme yüklenecektir. Yazılar, bilgisayar ortamında ve dizgi programlarında kullanılabilecek şekilde Word formatında gönderilmelidir.

Dergiye gönderilen makaleler şekil incelemesinden geçerek hakem değerlendirme sürecine alınmaktadır. Şekil şartlarını sağlamayan çalışmalar hakem değerlendirilmesine alınmamakta, yazar(lar)dan şekil şartlarını sağlamaları istenmektedir. Şekil şartlarına ilişkin doküman internet sitesinden indirilebilir. Şekil şartları açısından eksiksiz olan makaleler ilgili alan editörleri tarafından incelenerek uygun bulunduğu takdirde hakem değerlendirme sürecine alınır. Dergiye yayımlanmak üzere yollanan makaleler, "kör hakem" yöntemiyle değerlendirilmektedir. Editör, editör yardımcısı veya alan editörleri tarafından makaleler, alanında uzman en az iki hakeme gönderilmektedir. İki hakemin görüş ayrılığı durumunda, üçüncü bir hakemin görüşüne başvurulmaktadır. Editörler hakemlerden gelen eleştiri ve önerileri kendi değerlendirmeleri ile birlikte yazar/lara iletmektedir. Değerlendirme sonuçları en fazla 90 gün içinde yazara bildirilir. Üçüncü bir hakeme gönderilen eserlerde bu süre 120 güne çıkabilmektedir. Düzeltme talep edilen eserler, editör tarafından yazara gönderilir ve düzeltme için gerekli ek süre yazara verilir. Hakemlerden gelen raporlar doğrultusunda, makalenin yayımlanmasına, yazardan hakem raporuna göre düzeltme istenmesine ya da yazının reddedilmesine karar verilmekte ve karar yazara iletilmektedir. Basımı uygun bulunan yazıların, yayımlanıp yayımlanmayacağına ya da derginin hangi sayısında yayımlanacağına editörler ve/veya yayın kurulu karar verir. Yazar, süreç konusunda Makale Yönetim Sistemi veya E-posta yoluyla bilgilendirilmektedir.

Makale derginin yazım kurallarına uygun olarak hazırlanmalıdır (Kelime aralıklarından atıf ve kaynakça yazımına kadar bütün detaylar yazım kurallarına uygun olmalıdır).

Makale süreç akışı şu şekildedir:

- Yazar tarafından makalenin Makale Yönetim Sistemine yüklenmesi
- Makalenin şekil açısından incelenmesi
- Şekil incelemesinden geçen makalelerin hakem değerlendirme sürecine alınması
- Editör incelemesi ve gerektiğinde yazardan ek talepler
- Çalışma konusunda uzman 2 hakeme makalenin gönderilmesi (gerekli görülmesi durumunda 3. hakem değerlendirmesine gönderilmesi)
- Hakem görüşleri doğrultusunda makalenin kabulü veya reddine karar verilmesi
- Yayınlanmasına karar verilen makalenin dizgi ve tasarımının yapılması
- Dizgisi ve tasarımı yapılmış makalenin yazara son kontrol için gönderilmesi
- Makalenin yayınlanması

Etik Kurallar

Yayınlanmak üzere dergiye gönderilen çalışmalarda bilimsel atıf kurallarına azami özen gösterilmesi gerekmektedir.

Güvenlik Çalışmaları Dergisinde yayımlanan yazıların fikri sorumluluğu yazarlara aittir. Dergiye gönderilen çalışmalarda, etik kurul kararı gerektiren klinik ve deneysel insan ve hayvanlar üzerindeki çalışmalar için ayrı ayrı etik kurul onayı alınmış olmalı, bu onay makalede belirtilmeli ve belgelendirilmelidir.

Gönderilen makalenin bir kısmı ya da tamamı başka bir yerde yayınlanmamış, yayınlanmak üzere başka bir yere yollanmamış olmalıdır.

Tüm yazarlar ilgili makaleyi okumuş, onaylamış ve dergiye yayınlanmak üzere gönderildiğinden haberdar olmalıdır.

Makale yazar/lar tarafından yazılmış, özgün bir çalışma olması gerekmektedir.

Dergiye gönderilen çeviri makale çalışmalarında orijinal makalenin yazarından ve yayıncı kuruluşundan izin alındığını gösteren belgenin sunulması gerekmektedir.

Yazar/lar makalenin telif hakkını, makalenin Güvenlik Çalışmaları Dergisinde yayınlanmasına karar verildiğinden itibaren dergiye devretmiş sayılır. Yazar/yazarlar derginin yazı işlerinden izin almadan makaleyi başka bir platformda (dergi, editoryal kitap, internet sitesi, blog vb.) yayınlayamaz.

Yazar/lar bilimsel etiğin bütün unsurlarını yerine getirmek üzere makale ile birlikte "**İntihal Denetim Raporu**"nu ve "**Etik ve Telif Hakkı Devir Formu**"nu mutlaka doldurarak sistem üzerinden dergiye ulaştırmalıdır.

Yazım Kuralları

Yazım dili Türkçe ve İngilizcedir. Türkçe makalelerin yazım ve noktalamasında ve kısaltmalarda Türk Dil Kurumu internet sitesindeki Güncel Sözlük ve Yazım Kuralları esas alınır. Gönderilen yazılar dil ve anlatım açısından bilimsel ölçülere uygun, açık ve anlaşılır olmalıdır.

Makalelerde Türkçe ve İngilizce başlık, öz ve abstract, anahtar kelimeler ve keywords; metin içinde giriş, bölüm başlıkları ve sonuç kısımları ile kaynakçanın yer alması gerekmektedir. Makale yukarıda sayılan tüm unsurları ile birlikte 4000 ile 8000 kelime arasında olmalıdır. Makalelerde yer alan Türkçe ve İngilizce öz ve abstract'ın her birinin 150-250 kelime, anahtar kelime ve keywords'ün 3-7 kelime aralığında olması gerekmektedir.

Yazar adı makale başlığının alt satırının sağ köşesine italik koyu, 11 punto olarak yazılmalı; yazarın unvanı, görev yeri ve elektronik posta adresi dipnotta (*) işareti ile 9 punto yazılarak belirtilmelidir. Diğer açıklamalar için yapılan dipnotlar metin içinde veya sayfa altında numaralandırılarak verilmelidir.

Yazı karakteri Times New Roman, 11 punto, satırlar bir buçuk aralıklı, açıklamalara ilişkin dipnotlar 9 punto ve tek aralıklı yazılmalıdır.

Dergide yayımlanan makalelere ve makale değerlendirmesi yapan hakemlere 23.01.2007 tarih ve 26412 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren "Kamu Kurum ve Kuruluşlarınca Ödenecek Telif ve İşlenme Ücretleri Hakkında Yönetmelik" hükümleri uyarınca telif ücreti ödenir.

Kitap incelemelerinde aşağıdaki hususlara ayrıca dikkat edilmelidir;

Kitap inceleme metinleri 1000 ile 1500 kelime arasında olmalıdır.

Başlık bilgilerinde tanıtım veya incelemesi yapılan eserin adı, yazarı, yayımlandığı şehir ve yayınevi, yayım yılı ve ISBN numarası yazılmalıdır.

Kitap inceleme veya tanıtımı yapan yazarın adı makale başlığının alt satırının sağ köşesine italik koyu, 11 punto olarak yazılmalı; unvanı, görev yeri ve elektronik posta adresi dipnotta (*) işareti ile 9 punto yazılarak belirtilmelidir.

Kitap tanıtımı bir eserin sırf özeti değil, eleştirel olarak değerlendirmesi olmalıdır. Kitap tanıtımı yapan yazar kitapla aynı fikirde olabilir veya kitabın fikirlerine karşı çıkabilir

veya kitabın sunduğu bilgilerde, yargılarda veya yapıda örnek teşkil eden veya eksik kalan yönleri belirtebilir. Kitap tanıtımı yapan yazar ayrıca kitapla ilgili düşüncelerini de açık bir şekilde ifade etmelidir.

Kitap incelemesi, bir kitaptan ortaya konulan en önemli noktalara ışık tutularak bunların eleştirel olarak tartışılmasıdır. Kitap incelemesi giriş, kitabın özeti, eleştirel tartışma ve sonuç gibi genel bir yapıyı takip etmelidir.

Sayfa Düzeni

Metin içinde yazı tipi 11 punto Times New Roman yazı karakteri kullanılmalıdır. Sayfa Yapısı A4 boyutlarındaki kâğıdın üst, alt, sağ ve sol boşlukları 2,5 cm (0.98 inç) bırakılarak, iki yana dayalı, satır sonu tirelemesiz şekilde olmalıdır. Paragraf arası, ilk satır 1.25, paragraflar arası önceki 3 nk, sonra 3 nk, iki yana dayalı, satır aralığı bir buçuk olmalıdır. Sayfa numaraları alt sağda verilmelidir.

Temel Başlıklar (Birinci Düzey) ortalı ve bold yazılmalıdır. Kendisinden önce ve sonra bir satır boşluk bırakılmalıdır.

İkinci Düzey Başlıklar, sola dayalı ve bold yazılmalıdır. Kendisinden önce ve sonra bir satır boşluk bırakılmalıdır.

Üçüncü Düzey Başlıklar, Sola dayalı bold yazılmalıdır. Kendisinden önce bir satır boşluk bırakılmalıdır.

Dördüncü Düzey Başlıklar, Sola dayalı, bold ve italik yazılmalıdır. Kendisinden önce bir satır boşluk bırakılmalıdır.

Beşinci Düzey Başlıklar, Sola dayalı ve italik yazılmalıdır. Kendisinden önce bir satır boşluk bırakılmalıdır.

Beş düzeyden daha fazla başlık oluşturulması önerilmemektedir.

Atıf ve Kaynakça Yazımı

Atıf

Metin içi yöntemde parantez içinde kaynak gösterimi yapılır. Atıflar makalede kullanılan punto ile yazılır. Bu yöntemde, metin içinde alıntı sonrasında (Yazarın Soyadı, Basım Yılı: Sayfa Numarası) parantez içinde verilir. Bir eserden veya mülakattan doğrudan alıntı yapılması durumunda alıntı 3 satırdan az ise cümle içerisinde kullanılır; 3 satır ve daha fazla ise ayrı bir paragrafta belirtilir. Bu paragraf tek aralıklı, 9 punto ve her iki taraftan 1.25 cm içeriden hizalı yazılır.

Atıf Örnekleri

Tek yazar	(Aras, 2011, s. 236)
İki yazarlı	(Kazgan ve Ulçekno, 2003, s. 32)
Üç ile beş yazar arası	İlk sefer atıf yaparken tüm yazarların adı listelenir; (Kernis, Cornell, Sun, Berry, ve Harlow, 1993). Sonraki atıflarda ise sadece ilk yazarın adı belirtilip "vd." ifadesi kullanılır. (Kernis vd., 1993, s. 42)
Altı ve daha fazla yazarlı metinler	Altı ve daha fazla yazarlı metinlerde, sadece ilk yazarın adı kullanılıp sonrasında "vd." ifadesi kullanılır: (Harris vd., 2001, s. 112)
Yazar olarak bir kurum	İlk atıfta kurumun tam adı açık bir şekilde belirtilerek yazılır: (Avrupa Komisyonu Türkiye Temsilciliği, 2000, s. 3), sonraki atıflarda ise kısaltması (AKTT, 2000, s.) yazılır. Kurum literatürde kısaltılmış ismiyle biliyorsa ilk atıfta da kısaltma ile kullanılabilir. (EGM, 2000, s. 12)
Editörlü kitaptan bölüm (Bölüm yazarı dikkate alınır)	(Karaışık, 2008, s. 40)
Yazarsız çalışma	(Bilimsel Makaleler Hazırlama, 2000, s. 45)
Standartlar	(TS-40561, 1985, s. 6)
Resmi Gazete	(Başlık, Yıl)
Yazarı olmayan internet dokümanı	(www.hurriyet.com.tr, 2012)
Aynı yazarın farklı yıl birden çok çalışması	(Tekin, 2011, s. 220; 2013, s. 30)
Aynı yazarın aynı yıla ait birden fazla eseri	(Heper, 1999a, s. 165) ve (Heper, 1999b, s. 140)
Aynı soyadlı iki yazar	(Ö. Aslan, 2000, s. 6; M. Aslan, 2010, s. 71)
Birden fazla kaynaktan yararlanma	(Aytekin, 2004, s. 71; Küçük, 2008, s. 87)
Orijinal kaynağa ulaşılamaması durumunda	(Metin içinde bahsedilirse) İnalcık'a göre (akt. Hanioğlu,2012, s. 40) (Metin içinde bahsedilmezse) (İnalcık'tan akt. Hanoğlu, 2006, s. 40)
Kişisel iletişim vasıtasıyla ulaşılan mülakatlar, mektuplar, e-mailler	Kişisel iletişim vasıtasıyla ulaşılan mülakatlar, mektuplar, e-maillerde, kişisel iletişim kurulan kişinin adı ve görüşmenin tarihi belirtilmelidir. Ancak, kişisel iletişim yoluyla elde edilmiş veriler kaynakçaya eklenmemelidir:(N. AlSayyad, kişisel iletişim, 25 Mart 2018)
Dipnotlar ve sonnotlar	APA yazım stilinde, dipnot ve sonnot kullanımı pek tercih edilmemektedir. Bundan dolayı mümkün olduğu kadar az dipnot kullanılmalıdır. Yalnızca çok elzem bir açıklayıcı not gerektiğinde dipnot kullanılmalıdır.

Önemli not: APA atıf ve kaynakçada "and" yerine "&" kullanılmasını önermektedir. Ancak Türkçede "&" sembolü "ve" yerine kullanılmadığından, Türkçe olarak yazılan metinlerde atıf yaparken ve kaynakça yazarken "&" sembolü kullanılmamalıdır.

Ayrıca, üç kişiden çok yazarlı metinlere atıf yaparken APA "et al." (Kernis et al., 1993, s.65) kullanılmasını önermektedir. Ancak Türkçe'de "et al." yerine "vd." (Kernis vd., 1993, s. 65) kullanılmalıdır.

Bununla birlikte, eğer değerlendirilmek üzere Güvenlik Çalışmaları Dergisi'ne gönderilen çalışma İngilizce hazırlanmışsa, bu metinlerde atıf ve kaynakçada APA standartlarına uygun olarak "and" yerine "&" sembolü ve "et al." kullanılmalıdır.

Kaynakça

Kaynak bilgileri verilirken yazar(lar)ın önce soyadı sonra adı yer alır. İki yazarlı bir kaynakta yazarlar arasına "ve" bağlacı konur. İkiden fazla yazarlı eserlerde ise yazarların arasına noktalı virgül (;) konulup son yazardan önce "ve" bağlacı konulur.

Yazarlar soy ismine göre alfabetik olarak sıralanır. Yazarların soyadları ve adlarının ilk harfi büyük yazılır. Kullanılan kaynağın künye bilgileri açık olmalıdır. Çok basımlı kitaplarda baskı sayısı yazılır. Yabancı kaynaklarda, künye bilgilerinin tamamı kaynağın yazım dili ile yazılır, Türkçeleştirme yapılmaz.

Kaynakça Örnekleri

Kitap, temel biçim	Yazar, A. A. (Yayın yılı). Çalışma adı. Yer: Yayıncı.
Tek yazarlı kitap	Özbudun, E. (2008). *Anayasalcılık ve demokrasi*. İstanbul: Bilgi Üniversitesi Yayınları.
İki yazarlı kitap	Alkın, S. ve Özer, K. (2011). *Muhafazakarlığın farklı boyutları*. Ankara: Kadim Yayınları.
Üç ile yedi yazar arası kitap	Yazar1, A.A., Yazar2, A.A., Yazar3, A.A., Yazar4, A.A., Yazar5, A.A. ve Yazar7, A.A. (Yayın yılı). *Kitabın adı*. Yer: Yayıncı
Süreli yayında makale, temel biçim	Yazar, A. A., Yazar, B. B., ve Yazar, C. C. (Yıl). Makale adı. *Dergi adı, cilt. No* (sayı no), sayfa/lar. doi:http://dx.doi.org/xx.xxx/yyyyy
Tek Yazarlı Makale	Ayhan, U. (2016). Yeni güvenlik konsepti ve güvenliği sınır ötesinde karşılama. *Güvenlik Çalışmaları Dergisi. 18*, (3-4), s.26-41.
İki yazarlı süreli yayın	Wegener, D. T. ve Petty, R. E. (1994). Mood management across affective states: The hedonic contingency hypothesis. *Journal of Personality and Social Psychology, 66*, 1034-1048.
Üç ile yedi yazar arası süreli yayın	Kernis, M. H., Cornell, D. P., Sun, C. R., Berry, A., Harlow, T. ve Bach, J. S. (1993). There's more to self-esteem than whether it is high or low: The importance of stability of self-esteem. *Journal of Personality and Social Psychology, 65*, 1190-1204.
Yazar adı olarak kurum	Emniyet Genel Müdürlüğü. (2000). *Polis 1999 Emniyet Genel Müdürlüğü çalışmaları*. Ankara: EGM APK Dairesi Başkanlığı, Yayın No.138.

Yazar Adı bilinmiyorsa ya da yoksa	International Tourism Report. (1997). *Travel and tourism intelligence.* No. 2.
Çeviri	Serra, N. (2011). *Demokratikleşme sürecinde ordu: Silahlı kuvvetlerin demokratik reformu üzerine düşünceler*. (Şahika Tokel, Çev.). İstanbul: İletişim Yayınları.
Hazırlayan	Pamir, N. (Haz.). (1993). *Terörizm, kont-terör ve güvenlik.* İstanbul: Kastaş Yayınları.
Editörlü Kitap	Yazar, A. A. (Ed.). (Yayın yılı). *Kitap adı*. Yer: Yayıncı.
	Özbek, M. (Ed.). (2005). *Kamusal alan*. İstanbul: Hil Yayınevi. Diamond, L. ve Plattner, M. (Ed.). (1996). *Civil-military relations and democracy*. Baltimore ve London: Johns Hopkins University Press. Özkol, A. O., Delici, M. ve Özhan, S. (Ed.). (2009). *ABD dış politikası.* İstanbul: Küre Yayınları.
Editörlü Kitapta Bölüm	Yazar, A. A. (Yayın yılı). Bölüm/makale adı. A. Editör ve B. Editör (Ed.), *Kitap adı* içinde (sayfa numaraları). Yer: Yayıncı.
	Çınar, M. (2011). 2000'li yıllarda Türkiye'de siyaset. A. Demirhan (Ed.), *2000'li yıllarda siyaset ve siyasi partiler* içinde (s.136-152). İstanbul: Meydan Yayıncılık.
Yazarsız Süreli	*The Economist.* (2011). Trade and wages. s. 341, Londra s.74-75.
Sempozyum ve Kongrede Sunulan Yayınlar	Taşagıl, A. (2017). Gök Türk döneminde iç güvenlik meselesine bir bakış. *Türk polis tarihinin kökenleri. 1. Uluslararası kolluk tarihi sempozyumu*, 15-17 Nisan 2016, Ankara: Polis Akademisi Yayınları, ss. 15 - 32.
Raporlar	Burke, W. F., Uğurtaş, G. (2002). Seismic interpretation of thrace basin. *TPAO internal report.* Ankara.
Yazarsız Raporlar	Uluslararası Terörizm ve Güvenlik Araştırmaları Merkezi. (2016). Türkiye'de güvenlik sektörünün dönüşümü: Polisliğin yeniden yapılandırılması. Ankara: Polis Akademisi Yayınları
Seminerler	Lawrence, E. (1983). Gelişmiş ülkelerde sermaye piyasası ve bankaların fonksiyonu. *Uluslararası sermaye piyasası ve bankalar semineri*. 24-25 Ekim 1983. Çeşme, ss.33-37.
Standartlar	TS-40561. (1985). *Çelik yapıların plastik teoriye göre hesap kuralları*. Ankara: Türk Standartları Enstitüsü.
Broşür	Türkiye Cumhuriyet Merkez Bankası. (2006). *Enflasyon hedeflemesi*. [Broşür].
Gazete	Bardakçı, M. (2016, 16 Aralık). Halep dramı Osmanlı'nın hala devam eden tasfiye mücadelesidir. *Haber Türk*, s.6.
Online gazete makalesi	Yazar, A. A. (Yıl, Gün Ay). Makale adı. *Gazete Adı*. http://www.aaaaaaaaaaa.com/full/url/ adresinden erişildi.
Resmi Gazete	Başlık. (Yıl, Gün Ay). Resmi Gazete (Sayı: xxx). Erişim adresi: http://xxxx

Sözlük	Madde başlığı. (Yıl). Sözlük ismi. Yer: Yayıncı
Ansiklopedi	Yiğit, İ. (2009). Bahri Memluk sultanları. *İslam tarihi ansiklopedisi* içinde (Cilt. 7, ss. xx-xx). İstanbul: Kayhan Yayınları.
Devlet Dokümanları	Genelkurmay Ateşe Başkanlığı. (2000). *57. piyade alayının tarihçesi*. Ankara: Milli Savunma Bakanlığı Arşiv Müdürlüğü. Yayın No: 19175.
Kutsal Kitaplar	*Kur'an.* Bakara süresi. Ayet 25 (Mealde Basımevi ve meal yazarı belirtilir).
Yayınlanmamış Tezler	Haklı, S. Z. (2014). *Liberalizm ve komüniteryanizmde birey fikri: Kar- şılaştırmalı bir inceleme*. (Yayınlanmamış Doktora Tezi). Gazi Üniversitesi Sosyal Bilimler Fakültesi, Ankara
Mahkeme Kararları	Yargıtay H.G.K. 19 Mayıs 1963. E. 4-39, K.59 (*Adalet Dergisi*, Mart-Nisan 1964). 3-4.
Kişisel Görüşme (Mülakat)	Taşkın, M. Atatürk Mahallesi Muhtarı. (15.01.2017). *Mahallenin güvenlik sorunlarının çözümüne ilişkin görüşme.* Ankara.
İnternet-Yazar Adı Olarak Bir Kurum	TCMB. (2012). *Finansal istikrar raporu*. http://www.tcmb.gov.tr/ (E.T.04 Temmuz 2012).
İnternette Yayımlanan Gazete Makalesi	Henninger, D. (2012). The president that time forgot. *Wall Street Journal*. 28 Haziran 2012. 04 Temmuz 2012 http://online.wsj.com/article/wonder_land.html?mo- d=WSJ_topnav_europe_opinion#articleTabs=article adresinden erişilmiştir.
Elektronik Posta	Beck, A. (2011). (bna@le.ac.uk). *Crime prevention report*. Ahmet Güney'e kişisel e-posta. 12 Haziran 2011 [aguney53@gmail.com].
Film ya da Video	Valdes, D. (Yapımcı). (1999). F. Darabont (Yönetmen). Green Mile [Film]. ABD: Warner Bros Pictures
Televizyon Programı	Özdemir, C. (Yapımcı). (2012). *5N1K* [Televizyon Programı]. 27 Haziran 2012. İstanbul: CNN TÜRK tv. Sopel, J. & Donovan, T. (Producer). (2012). Political shows [Television Broadcast]. 04 July 2012. London: BBC One.
Ses Kaydı	Selçuk, M. (1999). Aziz İstanbul [CD]. İstanbul: YKY Müzik.
Video Kayıtları	Son Darbe: 28 Şubat. (2012). 2. Bölüm. 65 dak. Türkiye: CNN TÜRK. 2012.

Tablolar

Tablo numarası ve başlığı, tablonun bir aralık üstünde yer alır. Başlıkla tablo arasında ayrıca boşluk olmaz. Tablo numaraları (**Tablo 1**., **Tablo 2.** vd.) şeklinde verilir. Tablo kelimesi, numarası ve nokta koyu (bold) yazılır. Tablolarda kullanılan verilerin kaynağı, tablonun sol alt köşesinde belirtilir ve koyu olarak "**Kaynak:**" şeklinde yazılır. Tablonun başlığı ve kaynağı yazılırken sadece ilk kelimenin ilk harfi büyük yazılır, diğer kelimeler küçük harfle yazılır ve koyu (bold) olmadan yazılır.

Örnek Tablo:

Tablo 1. Kara para aklamada kullanılan sektörler

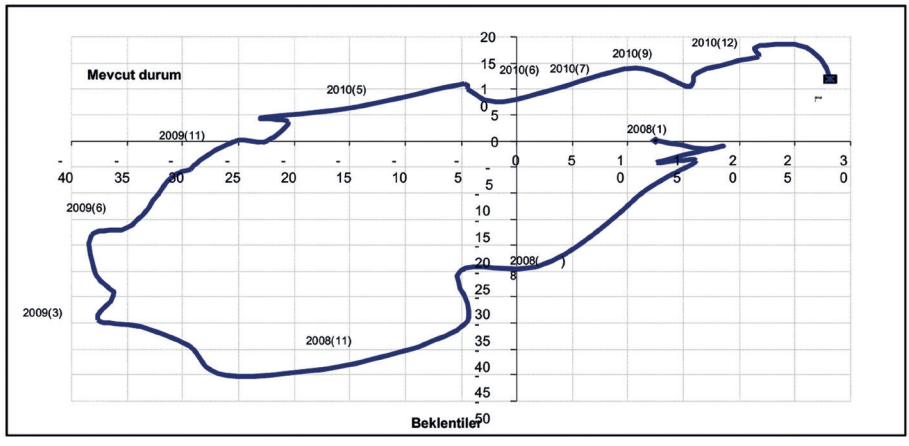
	Yerleştirme	**Ayrıştırma**	**Bütünleştirme**
Bankacılık	x	x	x
Döviz Büroları	x		
Para Transferleri	x		
Menkul Kıymet	x	x	x
Sigortacılık	x	x	x

Kaynak: Aydın, (2010, s.42).

Şekiller

Şekil numarası ve başlığı, şeklin altında yer alır. Şeklin kaynağı şekilden sonra parantez içinde verilebilir.

Örnek şekil:



Şekil 1. Almanya, reel kesimde mevcut durum ve beklentiler, (Kaynak: Gürsel ve Balcı, 2011, s.5)

Yazışma Adresi / For Correspondence:
Güvenlik Çalışmaları Dergisi
Polis Akademisi Başkanlığı, Güvenlik Bilimleri Enstitüsü Müdürlüğü
Necatibey Cad: No:108 06580 Anıttepe/Çankaya-Ankara / Türkiye
Tel: +90 (312) 462 90 43 • E-mail: guvenlikcalismalari@pa.edu.tr
www.**guvenlikcalismalari**.pa.edu.tr