Güv. Str. Derg. 2021, 17(38): 411-439
DOI: 10.17752/guvenlikstrtj.964066

Araştırma Makalesi
Research Article

A Comparison between the Concepts of Gray Zone and Hybrid War: What is New for International Security?

Gri Bölge ve Hibrit Savaş Konseptleri Arasında Bir Karşılaştırma: Uluslararası Güvenlik Açısından Ne Gibi Yenilikler Vardır?

Fatih AKGÜL*

Abstract

Albeit the Hybrid War has dominated security studies since 2006, it is also observed that the term 'Gray Zone' has increasingly taken part as well in connection with China and Russia after 2015. However, there is also a debate and confusion in the literature over gray zone activities, its relationship with hybrid war, and their implementations. This article aims to discuss and assess the theoretical relationship between these concepts and their implications for international security, by comparing recent Russian and Chinese practices. The article asserts that hybrid and gray zone activities are neither new nor the same, and the Gray Zone Concept emerged as a reflection of the shift in the US strategical attention from Russia to China, and aimed to harmonize US national interests with other Allies' security concerns. However, it also acknowledges that the concept is real, and should be differentiated and separated from hybrid war.

Keywords: *Gray Zone Concept, Hybrid War, Russia, China, the US.*

Öz

Güvenlik çalışmalarında; 2006'dan bu yana Hibrit Savaş kavramı baskın konumunu korusa da 2015 sonrasında Rusya ve Çin'le ilişkili olarak 'Gri Bölge' kavramına da artan biçimde yer verilmeye başlanılmıştır. Diğer taraftan akademik yazında, gri bölge aktiviteleri, hibrit savaş, bunların teorik ilişkisi ve uygulamaları konusunda ciddi bir tartışma ve görüş farklılığı olduğu gözlemlenmektedir. Bu makalenin amacı, söz konusu kavramların teorik ilişkisini ve uluslararası güvenliğe olan etkilerini Rusya ve Çin örnekleri

* Ph.D., Colonel at Supreme Headquarters of Allied Powers Europe (SHAPE) Mons/Belgium, ORCID: 0000-0001-9861-9378, e-mail: stratejist99@yahoo.com.tr.

Geliş Tarihi / Submitted: 30.10.2020
Kabul Tarihi / Accepted: 03.05.2021

üzerinden karşılaştırarak incelemektir. Makale; her iki kavramın da yeni olmadığını, fakat aynı da olmadığını, Gri Bölge Konseptinin ABD'nin stratejik dikkatini Rusya'dan Çin'e kaydırmasının bir yansıması olduğunu ve ABD'nin ulusal çıkarları ile müttefiklerinin güvenlik kaygılarını örtüştürmeyi amaçladığını iddia etmektedir. Ancak, yine de Gri Bölge Konsepti bir realiteye işaret etmektedir ve Hibrit Savaş Konseptinden ayrıştırılmalıdır.

Anahtar Kelimeler: *Gri Bölge Konsepti, Hibrit Savaş, Rusya, Çin, ABD.*

Introduction

Once, Clausewitz rightfully stated that "Every age had its own kind of war."[1] In our contemporary international security environment, the more technology and its applications facilitate powers to challenge the status quo, the less explicit use of force and exoneration are required. Thus, the world becomes less predictable and more complicated to deter newer threats or to make an alliance against them. Anyway, new concepts and strategies are also developed to define and cover new threats. In this context, since the Lebanon war in 2006, but especially after the Crimea Crisis in 2014, hybrid war and hybrid threats have become a significant part of security studies. However, it is also observed that the term 'Gray Zone' has increasingly taken part as well in connection with China's and Russia's extraordinary methods after 2015. For example, North Atlantic Treaty Organization (NATO), as the most enduring alliance, is advised to focus on "geopolitical shifts" particularly caused by China and Russia in their near abroad, and "the impact of the technological revolution" in terms of new generation 'Gray Zone threats' for its next 70 years.[2] Similarly, recent strategic documents of the United States (US) have highlighted that the 'Gray Zone' strategies have reached their greatest impact since the end of the Cold War[3], while they have started depicting China and Russia as

[1] Carl von Clausewitz, *On War*, Michael Howard and Peter Paret, (ed. and trans.), Princeton University Press, Princeton, NJ 1984, p. 593.
[2] For details and articles on the issues see: *New Perspectives on Shared Security: NATO's Next 70 Years*, Tomas Valasek (ed.), Carnegie Endowment for International Peace Publications, Brussels, 2019.
[3] Office of the Director of US National Intelligence, *Global Trends: Paradox of Progress*, National Intelligence Council, Washington, DC, 2017, p.220. Kathleen Hicks, Alice Hunt Friend, et all., *Campaigning in the Gray Zone by Other Means,* Center for Strategic and International Studies (CSIS), International Security Program Report, Rowman

the most dangerous actors who are using these kinds of strategies against the US and its allies.[4] These documents generally agree on the prediction that combined use of traditional and new ways of gray zone activities such as strong-arm diplomacy, economic coercion, conducting covert and political subversion, manipulating media, and abusing corruption are the main tools in competition among big powers, and their long term effects on the international security will be crucial.

At this point, one can also remember Robert Cox's critical approach to traditional international relations theories: "Theory is always for someone and for some purpose."[5] Although the Gray Zone Concept is not a theory,[6] but an evolving term to define some new methods, this evolution might clue us on a 'standpoint' of some special interests of big powers and a change in power relations. Hereby some questions come to mind: Is it really a new phenomenon? What is the theoretical relationship between the concepts of the Gray Zone and Hybrid War? Why has the Hybrid War Concept been extended to or replaced with it? Finally, how will they affect the future security environment?

On the other hand, although this new concept is catching on and developing, there is also a lively debate and confusion over gray zone activities, hybrid war, their contents, and their relationship. Therefore, this article will compare gray zone activities with hybrid threats and assess their implications for international security, especially by focusing on Russian and Chinese implementations. In this framework, firstly, 'gray zone activities' and 'hybrid threat' definitions as well as their similarities and differences will be visited. Successively, Russia and China will be

---

& Littlefield, July 2019, p. 6.

[4] The White House, *National Security Strategy of the United States of America*, Washington, D.C., December 2017; U.S. Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge*, Washington, D.C., January 2018.

[5] Robert W. Cox, "Social Forces, States and World Orders: Beyond International Relations Theory", *Millennium: Journal of International Studies*, 1981, Vol.:10, Issue: 2, 126-155, p. 128.

[6] For a study on theorization of the Concept see: Javier Jordan, "International Competition below the Threshold of War: Toward a Theory of Gray Zone Conflict", *Journal of Strategic Security*, 14, No.1, 2020.

examined with their gray zone activities in their recent foreign policies. The last part of the article will assess the theoretical relationship between these concepts and provide some recommendations and conclusions to clarify and contribute uniqueness and analytical value of the Gray Zone Concept as well as to settle the observed confusion in the literature.

1. Definitions and Relationship between Gray Zone Activities and Hybrid Threats

Based on the content of the academic work, both Hybrid and Gray Zone terms are often matched with different terms such as war, conflict, threat, approach, activity, tactic, or strategy in definitions. To provide cohesion, this article will prefer the Hybrid War Concept and the Gray Zone Concept terms and will follow a chronologic order.

The history of the Hybrid War has generally gone back as far as the Peloponnesian Wars, concerning the use of asymmetric, para-military, or civilian components in warfare. However, contemporary discussions on the issue were seen firstly after the Israel-Hezbollah War in 2006, then increased after Russia intervened in Georgia in 2008, and finally have become dominant in security studies after Russia's Crimea intervention in 2014.

Initially, hybrid war was defined as an overt use of armed forces against another country or a non-state actor, in combination with conventional and irregular tactics including political, cyber, and economic means such as covert operations, coercion, or supporting terrorist acts.[7] Later on, NATO has adopted it and depicted hybrid threat as "a wide range of overt and covert military, paramilitary, and civilian measures which are employed in a highly integrated design."[8] In this context; cyberwar, global terrorism, organized crime, piracy, asymmetric conflict scenarios, and retrenchment from globalization have been classified as the main hybrid threats to international peace and security.[9] Successively, the European

[7] Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*, Potomac Institute Publishing, Virginia, 2007. p. 8.
[8] North Atlantic Council, *NATO Wales Summit Declaration*, Para. 13, 05 September 2014, https://www.nato.int/cps/en/natohq /official_texts_112964.htm (Date of Access: 22 February 2020).
[9] Sascha Dominik Bachmann and Hakan Gunneriusson, "Hybrid Wars: The 21st-Century's New Threats to Global Peace and Security", *Scientia Militaria, South African*

Union (EU) has included exploitation of resource dependency, covert political operations, and maritime disputes as hybrid threats.[10] This addition was the first extension of the Hybrid War Concept.

On the other hand, in time, some Chinese activities raised doubt in the US in terms of effectiveness and accountability of the current national security concept as well as hybrid threat definition. For example, an American scholar assessed that events such as: "a private Chinese oil rig anchoring inside Vietnam's exclusive economic zone, a Chinese frigate chasing off a Philippines survey ship over Reed Bank, or a Chinese infantry platoon appearing on a pile of rocks near the Spratly Islands" were "thin slices" of a fundamental change in the region. However, they were also too minor things individually, and declaring casus belli would be ridiculous.[11] In other words, recent Chinese activities can hardly be categorized as hybrid threats. Likewise, the inventors of the Hybrid War Concept also observed that the current version was not able to cover some new threats. For example; Hoffmann confessed that the hybrid threats definition had failed to capture some of the other non-violent actions such as "economic and financial acts, subversive political acts like creating or covertly exploiting trade unions and Non-Governmental Organizations (NGOs) as fronts, or information operations using false websites and planted newspaper articles" as a part of a bigger, non-military and stealthy project by directly citing from the Chinese Unrestricted Warfare Concept.[12] Simultaneously, several US military resources and officials have started using the term 'gray zone threats' for similar cases.[13] Thus, the concept of the Gray Zone

---

Journal of Military Studies, 2015, Vol.43, No.1, 77-98, pp. 78-79.

[10] Patryk Pawlak, "At a glance: Understanding Hybrid Threats", *European Parliamentary Research Service Fact Sheet*, PE 564.355, June 2015, http://www.europarl.europa.eu/RegData/etudes/ATAG/2015/564355/EPRS_ATA(2015)564355_EN.pdf (Date of Access 29 January 2020).

[11] Robert Haddick, "Salami Slicing in the South China Sea," *Foreign Policy*, 3 August 2012, https://foreignpolicy.com/2012/08/03/salami-slicing-in-the-south-china-sea/ (Date of Access: 20 May 2020).

[12] Frank Hoffman, "On Not-So-New Warfare: Political Warfare vs. Hybrid Threats," *War on the Rocks*, 28 July 2014, warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/ (Date of Access: 15 March 2020).

[13] For these examples see: Michael J. Mazarr, *Mastering the Gray Zone: Understanding a Changing Era of Conflict*, The Strategic Studies Institute and U.S. Army War College

has been welcomed in the US as a new approach to the pursuit of different kinds of aggressive aims.

Just like the Hybrid Warfare Concept, the Gray Zone Concept is not brand new. The doctrinal roots of gray zone threats are generally traced back to George Kennan's definition of political warfare in 1948. Kennan described political warfare as a logical application of Clausewitz's doctrine in peacetime, which employs all possible short-of-war-means to achieve national objectives. These means "could range from overt actions such as political alliances, economic measures and white propaganda to such covert operations as clandestine support of friendly foreign elements, black psychological warfare and encouragement of underground resistance in hostile states."[14] As can be seen here, political warfare comprised not only a significant part of US Foreign Policy during the Cold War but was also a good base for the Gray Zone Concept.

Since there is a lack of consensus around terminology, three broad definitions will be chosen as a starting point to examine it. Firstly, in his detailed work, Mazarr defines gray zone activities as "the employment of nontraditional tools of statecraft to achieve gradual but decisive results in the no-man's-land between peace and war" in a pattern of state rivalry.[15] Secondly, as offered by Hoffmann, gray zone activities are:

> "covert or illegal activities of non-traditional statecraft that are below the threshold of armed organized violence; including disruption of order, political subversion of government or non-governmental organizations, psychological operations, abuse of legal processes, and financial corruption as part of an integrated design to achieve strategic advantage."[16]

> Thirdly, gray zone is defined as "a conceptual space between peace and war, occurring when actors purposefully use multiple

---

Press, Ashburn Drive, Carlisle, PA, December 2015, p. 4.

[14] George F. Kennan, "Policy Planning Staff Memorandum", *National Archives*, RG 273, Records of the National Security Council, NSC 10/2, 4 May 1948, http://academic.brooklyn.cuny.edu/history/johnson/65ciafounding3.htm (Date of Access: 21 January 2020).

[15] Mazarr, ibid, p. 55.

[16] Frank G. Hoffman, "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges", *Prism*, November 2018, Vol. 7, No. 4, 30-47, p. 36.

> elements of power to achieve political security objectives with activities that are ambiguous or cloud attribution, and threaten the US and allied interests by challenging, undermining, or violating international customs, norms, or laws."[17]

In these definitions, we can observe three additions to hybrid threats: use of statecraft, use of a gradualist approach to achieve a strategical advantage, and deliberate blurring of the perpetrator, aim, and status of activities. Regarding content, political and economic tools are prioritized over military methods, while the last one also directly includes 'US interests' in the definition.

In this regard, the most crucial aspects and similarities between gray zone and hybrid activities can be summarized with the following. Firstly, they are operated in a blurring line between war and peace, the perpetrator cannot be identified, and all offenses are deniable. Secondly, both use asymmetric tools, so the effects cannot be measured and it is not easy to counter or deter with classical methods. Thirdly, both use technology effectively as well as other facilities of globalization. Particularly, information war and cyberwar are common and widely used in both. Lastly, these activities are more influential when they are combined and used together clandestinely.

As to differences, Mazarr highlights three specifications of his approach: measured revisionism, strategical gradualism, and using unconventional tools. In this context, China and Russia are given as measured revisionist states, since they are not adventurist and want to remain as responsible members of the international community. However, they also take calculated risk to change some aspects of the current system gradually in a patient way, instead of overturning it suddenly or completely. He includes most hybrid and unconventional war tools into gray zone activities, except for their less intensive use for a strategical purpose.[18] Actually, his criteria point to China and Russia as the main actors of the 'Gray Zone', but exclude terrorist and crime organizations to some extent.

---

[17] Lyle J. Morris, Michale J. Mazarr, et. all., *Gaining Competitive Advantage in the Gray Zone*, RAND Corporation, Santa Monica, Calif., 2019, p. 8.
[18] Mazarr, ibid, p. 9-74.

Another study highlights the main difference that gray zone activities generally refer to long-term strategic dimension, while hybrid warfare presents a tactical subset of gray zone cycle to reach short term victory or advantage. Likewise, whereas gray zone activities are mostly involved in political, informational, and economic tools, hybrid warfare is often characterized by military weighted paramilitary and civilian activities in a highly integrated design.[19] In another study, gray zone activities are depicted as 'indirect and less violent' actions, while hybrid tactics contain more violent, aggressive, and military methods.[20] So, again, it can be inferred that, unlike hybrid war, gray zone activities have a strategic perspective and prefer soft power tools.

On the other hand, these activities are also accused of aiming not only to achieve short-term tactical victories against the US and NATO but also to challenge the regional and global order.[21] Therefore, not long after, the US strategical documents incorporated these threats into assessments, albeit not naming them as 'Gray Zone threats'. For example, recent US National Defense Strategy mentions almost all of these activities by exemplifying them from China and Russia as the main threats to the US.[22] Likewise, the latest US Council on Foreign Relations survey forecasts the possibility of a cyber-attack from Russia on NATO members as the most probable and significant threat to international security while a deliberate military confrontation between these parties is highly unlikely.[23]

NATO hasn't accepted the 'Gray Zone' yet as a separate concept. However, we can see a tendency towards wider recognition. For example,

---

[19] David Carment and Dani Belo, "War's Future: The Risks and Rewards of Gray-Zone Conflict and Hybrid Warfare", *Canadian Global Affairs Institute Policy Paper*, October 2018, https://www.cgai.ca/wars_future_the_risks_and_rewards_of_grey_zone_conflict_and_hybrid_warfare, (Date of Access: 11 January 2020), p. 4-11.
[20] Hofmann, ibid, p. 39.
[21] David Carment and Dani Belo, "Gray-zone Conflict Management: Theory, Evidence, and Challenges", *European, Middle Eastern, & African Affairs*, Summer 2020, 21-41, p.38. Hicks and Friend, "Campaigning in the Gray Zone", p.9; Morris and Mazarr, "Gaining Competitive Advantage", p. 1-5.
[22] Supra note 4.
[23] Paul B. Stares, *Preventive Priorities Survey 2020*, Council on Foreign Relations\Center for Preventive Actions, https://cdn.cfr.org/sites/default/files/report_pdf/PPS_2020_12162019_CM_single_0.pdf (Date of Access: 27 May 2020).

for the first time, NATO Secretary-General Jens Stoltenberg warned the Allies regarding some of Chinese and Russian policies, as well as their partnership in military technology and their accusation to NATO Allies for the existence of the Covid-19 Pandemic, by not mentioning 'Gray Zone'.[24] Likewise, NATO's new strategic perspective has been advised to be directed towards Russian and Chinese activities such as cyber-attacks to economies and armed forces, blackmails by using artificial intelligence, and scary development in military and information technology, which were undreamed only a decade ago.[25] Thus, there can be seen a direct link between these concepts and their perpetrators, namely Russia and China.

Apart from the referred studies above, which try to separate these concepts by focusing on their differences, there are also different approaches and critics.[26] For example, some studies assert that it is impossible and even counterproductive to separate them,[27] while some others assert that both the Hybrid War and the Gray Zone Concepts are not new, thus making definitions are useless and even dangerous since they can create a false perception which might cause a 'real' war.[28] Likewise, the debate between realists and institutionalists over the role of international organizations and norms in 'Gray Zone' conflicts also seems to contribute to the contradiction.[29] On the other hand, it is also observed that they are often used interchangeably, or all kinds of modern and non-conventional

[24] Jens Stoltenberg, "Remarks", *NATO 2030-Strengthening the Alliance in an increasingly competitive world, Online Conference*, 8 June 2020, https://www.nato.int/cps/en/natohq/opinions_176197.htm (Date of Access: 12 July 2020).
[25] For details and articles on the issue see: Valasek, "New Perspectives".
[26] For different perspectives and criticism see: Adam Elkus, "50 Shades of Gray: Why the Gray Wars Concept Lacks Strategic Sense, *War on the Rocks*, 15 December 2015, https://warontherocks.com/2015/12/50-shades-of-gray-why-the-gray-wars-concept-lacks-strategic-sense/ (Date of Access: 7 February 2020). Hal Brands, "Paradoxes of the Gray Zone", *Foreign Policy Research Institute E-Notes*, 5 February 2016, https://www.fpri.org/article/2016/02/paradoxes-gray-zone/ (Date of Access: 9 July 2020).
[27] For an example see: Anthony H. Cordesman and Grace Hwang, "Chronology of Russian Gray Zone and Hybrid Operations", *Center for Strategic and International Studies*, 02 July 2020, https://www.csis.org/analysis/chronology-possible-russian-gray-area-and-hybrid-warfare-operations (Date of Access: 12 July 2020).
[28] For an example see: Donald Stoker and Craig Whiteside, "Blurred Lines: Gray-Zone Conflict and Hybrid War-Two Failures of American Strategic Thinking," *Naval War College Review*, 2020, Vol. 73, No. 1, 13-48.
[29] Carment and Belo, ibid, p. 23.

conflicts are categorized as gray zone activities with or without hybrid threats. For example, some studies start the date of 'Gray Zone struggles' from the Cold War, because of their intensive use in political, economic, informational, and military competition by two superpowers, while they include special warfare campaigns, counterterrorism, and counterinsurgency to the Gray Zone Concept by matching their characteristics such as small-footprint, low-visibility, and their covert nature.[30]

In this context, there seems an inclination to depict the Gray Zone Concept too widely by including all kinds of innovative technologies and activities of terrorist organizations such as DAES and Boko Haram. Likewise, almost all of the referred studies make a comparison between Russia and China, particularly between China's reef dredging activities in the South China Sea and Russia's military intervention in Crimea, and finally accept them as the most dangerous 'Gray Zone' actors. However, we believe that creating a catch-all concept could do little to define modern threats. Similarly, Russian and Chinese activities should be exemplified and analyzed in a proper context. For this reason, before approaching an assessment, we need to examine gray zone activities of Russia and China in their recent policies shortly, to understand better the similarities and differences between the Hybrid War and Gray Zone Concepts, as well as to match the theoretical perspectives and their practices in the theatre.

2. Russia's Gray Zone Activities

Though hybrid tactics or gray zone activities are relatively new terms in security studies, Russia is asserted to have been using that kind of mixture of political, economic, and subversive activities since the Soviet Union times.[31] However, it has become more visible when General Valery Gerasimov has put forward some thoughts in 2013, which is later referred to 'Non-linear War' or Gerasimov Doctrine, and implemented them one year later in Crimea. In his article, Gerasimov emphasizes the changing

[30] Joseph L. Votel, Charles T. Cleveland, et all., "Unconventional Warfare in the Gray Zone," *Joint Forces Quarterly*, 1st Quarter 2016, No:80, 101-109. Jahara W. Matisek," Shades of Gray Deterrence: Issues of Fighting in the Gray Zone", *Journal of Strategic Security*, 2017, Vol.10, No.3, 1-26.
[31] Hofmann, ibid, p. 32.

nature of contemporary wars towards which nonmilitary means have exceeded the power of military force and armies have been used only for sudden and fierce attacks against strategic targets, without declaration of war.[32] Here, it was easy to see the similarity between Russian tactics and the Hybrid War. Thus, there appears a consensus among the academicians that particularly in Putin's terms, Russia has preferred hybrid tactics as a combination of military and nonmilitary instruments to surprise, confuse, and to wear down multinational bodies such as the NATO and the EU, against their vulnerabilities on a long decision and response processes.

As the most referenced example, following the toppling of Ukrainian pro-Russian Ex-President Viktor Yanukovych, Russia executed a special operation by using its Naval Infantry and, Special Forces together with pro-Russian Crimean militias as well as all capacity of electronic and cyber warfare. With this swift operation, Russian troops seized control of the peninsula quickly as of March 2014. One month later, the so-called Crimea Parliament decided to join the Russian Federation and then the conflict has spread to Luhansk and Donbas which brought further Russian domination over the region.[33] Here, we must underline that while Russia used some non-military tools, the army played a decisive role with conventional force such as artillery, rocket systems, drones, and electronic warfare, which caused thousands of death at Debaltsevo and Donbas.[34]

Ultimately, these two maneuvers provided a great geostrategic advantage to Russia, but also they are perceived as the most severe security crises in Europe since the end of the Cold War. Because, for the first time, a country had annexed territory from another by using not-well defined or recognized methods and tools.[35] It is also predicted by many NATO and

---

[32] Valery Gerasimov, "The Value of Science in in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying Out Combat Operations," *Military Review*, January-February 2016, Vol.96, 23-29.
[33] Michael Kofman, *Lessons from Russia's Operations in Crimea and Eastern Ukraine*, Library of Congress Cataloging-in-Publication, RAND Corporation, Santa Monica, California, 2017, p. 73.
[34] Oktay Bingöl, "Hybrid War and Its Strategic Implications to Turkey", *Gazi Akademik Bakış*, 2017, Vol: 11, No: 21, 107-132, p. 118-119.
[35] Jeffrey Mankoff. "Russia's Latest Land Grab: How Putin Won Crimea and Lost Ukraine", *Foreign Affairs*, May/Jun 2014, Vol. 93, Issue 3, 60-68, p. 60.

EU members that Russia could attempt to destabilize not only Ukraine but also could undermine Alliance guarantees and jeopardize overall international security by adopting these hybrid methods. [36]

On the other hand, Russia is also claimed to have expertise in using a combination of gray zone and hybrid warfare tools complementarily such as political coercion, information operations and cyber operations in certain military space operations.[37] Therefore, it is hard to understand where the hybrid tactics start and gray zone tactic finish, which is required for a more detail examination. In this context, when going through a deeper dive into Russia's toolkit, firstly, it is asserted that Russia applies gray zone activities by using its networks of economic and political patronage to influence and direct political decision-making processes as well as strategic sectors of a country's economy. Thus, exerting political and economic influence via corrupt regimes and officials, regime-affiliated individuals, state-owned enterprises, and transnational organized crime are used together in an interconnected way as a part of their political warfare.[38]

In this context, meddling in the electoral campaigns, elections, and democratic decision processes is seen as a permanent tool in Russia's gray zone activities. For example, Russia is accused of intervening in at least 18 elections in Europe and the US since 2014 and achieved a substantial impact on results.[39] Likewise, Russia is claimed to have intervened in the 2016 presidential election of the US, French presidential elections by spreading fake news and using bribery in 2017, Bulgaria general elections as well as the Brexit vote and general elections in the United Kingdom

---

[36] Rainer L. Glatz and Martin Zapfe, "NATO Defense Planning between Wales and Warsaw: Politico-military Challenges of a Credible Assurance against Russia", *German Institute for International and Security Affairs*, SWP Comments No: 5, January 2016, https://www.swp-berlin.org/fileadmin/contents/products/comments/2016C05_glt_Zapfe.pdf (Date of Access: 10 May 2020), p. 1-2.

[37] Carment and Belo, ibid, p.7. Hicks and Friend, ibid, p. 9.

[38] For details and examples see: Heather Conley, James Mina et all., *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe*, CSIS, Lanham: Rowman & Littlefield, Washington, DC, 2016.

[39] Heine Sorensen and Dorthe Bach Nyemann, "Going Beyond Resilience. A revitalized approach to countering hybrid threats", *Hybrid CoE Strategic Analysis*, No: 13, 8 January 2019, https://www.hybridcoe.fi/wp-content/uploads/2020/06/Strategic-analysis-Sorensen-Nyeman-11-2018.pdf. (Date of Access: 04 January 2020).

(UK) between 2016 and 2019, by using direct cyber-attacks, shadowy media activities and financial aids. It is also claimed that Russia illicitly acquired and revealed some sensitive documents about a secret trade agreement between the US and the UK, which was not the first case.[40]

A similar accusation was observed in 2017 when Catalonia voted for independence. A NATO specialist in cyber warfare reported that Russia spent approximately one billion USD to establish a 'troll farm' company for the operation in Spain. Then, this so-called research company hired dozens of hackers, bloggers, and writers to disseminate fake news and articles favorable to the Kremlin. Thus, it is claimed that Russia achieved to destabilize Spain, a strong NATO and EU member.[41]

In the same context, Russia is claimed to exert power by using "shadowy financial flows, corrupt relationships, bribes, kickbacks, and blackmail" as well as its cyber mischief activities and demagogic populism via media and private false front organizations in all of Europe. These tactics are claimed to be used by Russia to create destabilization and friction among EU countries and within NATO.[42] As a specific example, it is claimed that Hungary had a secret contract with the Russian Rosatom Corporation on constructing two new nuclear reactors for 12.2 billion Euro in 2014. After then, Hungary has been seen to change its policies towards Russia and expressed strong opposition against the EU sanctions regarding Crimea intervention, while it also began questioning NATO presence in the country. In the same manner, it is also asserted that the

---

[40] Guy Faulconbridge, "UK says Russia tried to meddle in election by leaking U.S. trade documents", *National Post*, 16 July 2020, https://nationalpost.com/pmn/news-pmn/crime-pmn/uk-says-russia-tried-to-meddle-in-election-by-leaking-u-s-trade-documents-3 (Date of Access: 20 July 2020). Gordon Corera, "Russia 'interference' report to be published", *BBC*, 16 July 2020. https://www.bbc.com/news/uk-politics-53428246 (Date of Access: 20 July 2020).

[41] Martin Arostegui, "Spain Warns Russia's Catalonia Hacking Efforts Could Intensify", *VOA News*, 23 January, 2018. https://www.voanews.com/europe/spain-warns-russias-catalonia-hacking-efforts-could-intensify (Date of Access: 20 July 2020).

[42] More details and some examples are available in Celeste A. Wallander, "NATO's Enemies Within", *Foreign Affairs*, Jul/Aug 2018, Vol.97, Issue 4, 70-81. Sheera Frenkel, Kate Conger, et. all., "Russia's Playbook for Social Media Disinformation Has Gone Global," *New York Times*, 31 January 2019, https://www.nytimes.com/2019/01/31/technology/ twitter-disinformation-united-states-russia.html (11 March 2020).

more Russian footprint in the economy and energy sector have appeared the more corruption and non-transparency cases have been recorded. Therefore, it is concluded that these changes are interconnected, and not only the Hungary case but also almost all corruption cases from Latvia to Bulgaria, and scandals from the International Olympic Committee to the Fédération Internationale de Football Association (FIFA) have Russian involvement or instigation.[43]

As the world's largest exporter of natural gas and the second-largest exporter of crude oil and refined products, Russia also plays in energy diplomacy. In fact, it is believed that Russia has been using this card to create not only more dependency and monopoly but also to support its strategical goals at least for two decades.[44] More recently, it has been seen that Russia still uses energy as a tool of coercion by manipulating the prices, controlling all related assets, implementing politically motivated energy cuts and contractual restrictions. Despite this, Russia never admits and finds commercial excuses instead, it is believed that Gazprom and Rosneft have influence over decision-making in key EU countries.[45] As a consequence, indeed, today it is possible to see different approaches towards Russia between more or less energy-dependent and between geographically nearer or remote EU countries.

Lastly, as seen above, several analysts believe that Russia has been using these tools to achieve a more ambitious and strategical project: 're-establishment of Russia as a key international player' and some call it 'Hybrid Conflict 2.0'.[46] Shortly, all these efforts are accepted as parts of a bigger project. However, it should be admitted that Russia does not hesitate to

[43] Conley and Mina, ibid, p. 36-53.
[44] For examples see: Fatih Akgül, "Effects of Eurasian Energy Policies of Putin's Russia on Turkish-Russian Relations" (in Turkish), *Güvenlik Stratejileri Dergisi*, 2007, Vol: 3, No: 5, 129-157.
[45] Rem Korteweg, "Energy as a tool of foreign policy of authoritarian states, in particular Russia", *EU Policy Department for External Relations*, PE 603.868- April 2018, https://www.europarl.europa.eu/RegData/etudes/STUD/2018/603868/EXPO_STU(2018)603868_EN.pdf (Date of Access: 22 April 2020), 13-21.
[46] Graeme P. Herd, "Hybrid Conflict 2.0 Targeting the West", *Concordiam*, 20 May 2016, George Marshall Center, https://perconcordiam.com/hybrid-conflict-2-0-targeting-the-west/ (Date of Access: 22 April 2020).

use military power and hybrid methods in its near abroad, while it uses different tools for the rest of Europe to achieve its long-run political purpose, which might be classified in the Gray Zone Concept.

3. China's Gray Zone Activities

Interestingly, China has precedence as well on this issue albeit in different terms from Russia. China is believed to assume that it could never encounter the US militarily, thus, it has started focusing on unconventional tactics since the 1990s, and finally developed the 'Unrestricted Warfare' concept which is seen as an antecedent of gray zone activities.[47] Today, China is not only the second-largest country in economic terms, it also has the second-largest defense budget after the US, and the most massive armed forces in the world with more than two million personnel. However, it is still seen as an outstanding 'gray zone' player, with a softer version of gray zone activities, especially in economy and technology domains.[48]

In this context, the most referred gray zone effort is China's dredging the ocean floor and creating artificial islands, which was resulted in creating 3,200 acres of new land for military bases over the South China Sea. However, China is claimed to carry out this project by employing a wide range of instruments of power which are also called gray zone tools. Within this scope, it is observed that China generally use civilian fishing fleets and drilling stations to occupy critical locations. Simultaneously, civilian construction companies create new lands. Then, it establishes bases and tries to convince its neighbors for their permanent presence. While approaching the states of the region, China sometimes uses 'carrots' in terms of trade and exchange opportunities together with economic assistance, while sometimes uses 'sticks' such as cyber-harassment and political coercion. If something goes wrong, then China steps back and waits for months for better conditions.[49] So, this is depicted as a patient but a safe strategy.

On the other hand, China is also asserted to have a more varied toolkit that contains diplomatic pressure, false narratives, propaganda, and more

[47] Carment and Belo, ibid, p. 5.
[48] Hicks and Friend, ibid, p. 7-9.
[49] Mazarr, ibid, p. 43-44.

widely but less known economy and innovation projects.[50] When we look at these less-known activities closer, firstly, it can be seen that at least for a decade, China has been trying 'all ways' including 'practical moralism' approach to be a 'Technology Super Power'. Both reverse engineering and imitating technology have been utilized by China in research and development. For example, in high-speed train production, China seemed to rely on Japanese technology for many years during a learning period, but finally it has become a major exporter of the high-speed rail systems to Eastern European, Asian, and Latin American countries.[51]

Military modernization is another area of concern in terms of less-known gray zone activities. For example, China's growing influence and recent policies were mentioned as a challenge for the first time at the NATO London Summit on 3-4 December 2019. Likewise, Stoltenberg warned the Allies that the recent rise of China and its efforts to shift the global balance of power by heating the race for economic and technological supremacy would have consequences for global security and military supremacy of NATO. In the same vein, he stressed that China had been investing heavily in modern military capabilities and had been cooperating with Russia in military technology.[52]

In this context, China is claimed to acquire foreign military and dual-use technologies from advanced industrial economies both by legitimate and illicit means. As an example, in the US, artificial intelligence company Neurala, as well as information and military sensor technology companies Quanergy and Lattice Semiconductor were taken over by Chinese state-owned companies because of their financial problems. Concordantly, China is claimed to engage in cyber-enabled economic espionage, cyber intrusions, and other covert activities to strengthen its economic competitiveness unfairly. For example, China is alleged to be responsible for more than fifty percent of cross-border intellectual property theft worldwide, most of which is targeting the US directly and causes 300 billion

[50] Hofmann, ibid, p. 33-34.
[51] Philip Huang, "How Has the Chinese Economy Developed So Rapidly? The Concurrence of Five Paradoxical Coincidences", *Modern China*, 2015, Vol. 41, No. 3, 239-277, pp. 255-257.
[52] Stoltenberg, "Remarks".

USD annual costs to the US economy.[53] Similarly, China is also accused of targeting US government entities, personnel, allies, and defense contracting companies in several cyber-attack cases.[54] Therefore, it is claimed that technologies such as artificial intelligence, robotics, autonomous vehicles, augmented and virtual reality, and gene editing are targeted areas of China both for military and civilian purposes to gain an economic and geopolitical advantage over its Western competitors,[55] and this diversion of acquired military technology is underlined as a new security risk.[56]

In the same context, major Chinese projects under the Belt and Road Initiative (BRI) are seen as tools for Chinese expansion of influence as well as a military presence. Chinese BRI has been establishing new ports, new roads, railways, and pipelines by investing in key industries, sensitive technologies, and infrastructure. For example, BRI has been reported to achieve already 200 projects covering more than 70 countries and 90 billion USD investment in BRI countries until 2020.[57] In addition, the Digital Silk Road Initiative has been bringing technological advances and digital infrastructure to developing countries. However, the US has seen these projects as 'debt-trap diplomacy', since they will bring economic dominance, and create vulnerably and dependency.[58] Therefore, the US has already started encountering China-led BRI initiatives and Huawei Company-led fifth-generation (5G) network developments for security reasons.[59]

---

[53] Zack Cooper, "Understanding the Chinese Communist Party's Approach to Cyber-Enabled Economic Warfare", *Foundation for Defense of Democracies*, September 2018, https://s3.us-east-2.amazonaws.com/defenddemocracy/uploads/documents/REPORT_China_CEEW.pdf, (Date of Access: 04 January 2020), pp. 5-6.
[54] For examples see: Hicks and Friend, ibid, p. 8.
[55] Cooper, ibid, p. 10.
[56] Anthony H. Cordesman and Arleigh A. Burke, "China and the US: Cooperation, Competition and/or Conflict", *CSIS Report*, 1 October 2019, https://www.csis.org/analysis/china-and-united-states-cooperation-competition-andor-conflict (Date of Access: 7 January 2020), p. 60.
[57] Ibid, pp. 166-171.
[58] U.S. Department of Defense, "Summary of the", p.38-47. Hicks and Friend, "Campaigning in the Gray Zone", p. 8.
[59] Edward Wong, "The US versus China: A New Era of Great Power Competition, but Without Boundaries", *The New York Times*, 26 June 2019. https://www.nytimes.com/2019/06/26/world/asia/united-states-china-conflict.html (Date of Access: 7 January 2020).

Of course, BRI is not the only project labeled as Chinese Gray Zone activities. For example, under the umbrella of the Polar Silk Road project, China has been building five new scientific research stations, new icebreakers, and sending more and more 'patriotic tourists' to Antarctica and Greenland. This project is also assessed as a grand strategy in the Gray Zone, which aims to approach fish, mineral, and hydrocarbons sources as well as to provide new bases for its Navy in future years.[60]

In closing, it should be highlighted that most of the resources are from the US, and some of the claims can be seen as 'prejudgments' or 'pre-emptive' allegations. However, there are also similarities between some Chinese and Russian activities in terms of political and economic coercion via cyber operations, false narratives, and propaganda which are defined in the Gray Zone Concept.

4. Analysis and Assessments

By considering the theoretical framework and its practices together, firstly, we can assess that although the terms and using high technology are new aspects, it is hard to accept that both hybrid and gray zone activities are new threats to international security, as are their concepts. The new things in their concepts are their tools, their contents, and their executions in a highly sophisticated way. These components have been more clearly recognized and defined recently, thanks to the technology which has increased detection ability and situational awareness.

With regard to tools, we can see that electronic war, cyberwar, psychological war, and their applications have become a significant component of hybrid war. Concordantly, their use in peacetime and low intensity has been defined as hybrid conflicts or hybrid threats. Thus, we can deduce that hybrid war is true "war" in a Clausewitzian sense of the continuation of policy by other means, while hybrid threats refer to a less violent and looser form of conflict in a lower intensity. Yet, both still inherently retain the use of military/para-military force and conventional

[60] Rebecca Pincus, "China's Polar Strategy: An Emerging Gray Zone?", *The Diplomat*, 06 July 2018, https://thediplomat.com/2018/07/chinas-polar-strategy-an-emerging-gray-zone/ (Date of Access: 7 January 2020).

tools. On the contrary, it is hard to accept that the Gray Zone Concept contains using direct military force or overt coercion. From this point of view, Gray Zone activities can be ranked much closer to Kennan's Political war concept than the Hybrid War concept in the warfare spectrum, except that Gray Zone tools are used in peacetime in a stealthy and gradualist form and as a part of one specific project. As seen in both Chinese and Russian cases, their projects are indeed long-term, but not constant and not just a part of information warfare.

With regard to content and execution, we can assess that these concepts are similar, but not the same. At least two determinative differences can be found. The first difference in the gray zone activities lies in their gradualist revision of international order or status quo by acting under the threshold of a conventional response. In this context, Russian destabilization activities in Eastern Europe and Euro-Atlantic relations in a broader term, and Chinese expansionism in the South China Sea and to all Eurasia can be classified as gray zone activities. Because both states use a variety of synchronized tools for the long-term-purpose. However, unlike China, which projects long-term, insidious, and gradualist gray zone activities, Russia's Crimea intervention sought a 'fait accompli' advantage in the short term, and it was implemented overtly at the cost of condemnations and sanctions. Likewise, terrorist organizations generally prefer sudden impacts instead of gradual and long-term strategies. Therefore, some of the examined Russian activities, piracy, and terrorist activities should be accepted as hybrid war or threats, but not as gray zone threats.

The other main difference between gray zone activities and hybrid war threats is that the former is naturally state-centric while the latter is literally hybrid. This should be also a key element in the determination and classification of these activities, despite it is overlooked in earlier studies. In this context, firstly, we must question the proxy actors such as Russian and Chinese backing NGOs, cyber-attackers, or the Huawei Company whether they are really non-state and independent actors or not. We see that all of them have been either created or used by states and they are only small parts of a bigger project. Likewise, as mentioned before, gray zone strategies derive their power from their combined, coordinated, and simultaneous use for a specific end. However, using a lot of tools together in a 'salami-slicing strategy' can be achieved only by states, even

big and revisionist states. Hence, it might be seen as a realist perspective, but we cannot ignore states just because they keep their ambiguity. Unlike some hybrid threats, states are still main actors in gray zone activities.

At this point, it can be assessed that hybrid war has already been ill-defined and naturally controversial, and this causes the expansion in the Gray Zone Concept resembling it to hybrid war. Therefore, this article suggests differentiating the Gray Zone Concept by including some recommendations below to increase its uniqueness and analytical value and to contribute to settle the confusion in the literature.

The first reason for the confusion comes from the fact that both concepts refer to 'a gray area' and 'hybridity' in tools, actors, and activities. Indeed, hybrid warfare is operated in a gray area between tactical and operational levels. However, whether conducted by a state or not, since hybrid tactics are generally contained military tools and accompanied by para-military elements, they can easily be located in an illegal-crime spectrum. Namely, they are black and contain certain crimes. On the other hand, even if the gray zone activities imply hybridity in conventional and modern tools in an integrated and offensive way, they use a 'gray area' as a legal gap between crime and misdemeanor, thus cannot be declared as a 'violation of international law' singlehandedly. In other words, it is easy to define that hybrid war tactics are a kind of war or act of aggression, whereas gray zone activities cannot be defined in the same way only with one case. As examined, meddling elections, abuse of corruption or bribery, technology thefts, and cyber-attacks are executed by 'quasi' civilian individuals, independent NGOs, or private companies, thus, their offenses come under private-commercial law at first sight. Therefore, it is recommended to use their concepts in academic works instead of their dictionary meaning, and to focus on international law to deter them in the legal framework. Additionally, we must highlight that this insidious and trickery appearance of gray zone activities makes it more eligible to break international law, especially non-interventionism rule.

The other reason for this confusion might be the fact that almost all literature has American origin, and, if the US has a national interest in involvement, scholars tend to categorize all conflicts or threats as 'gray zone' or 'gray war' to receive more attention. However; mixing, complicating, or demonizing gray zone activities can do little to provide wider recognition

as well as to deter them altogether. At this point, it is recommended to let the Gray Zone Concept jettison its hybrid war burden, by separating it from counterinsurgency or fight against terrorism. Similarly, all countermeasures of NATO members should not be labeled as gray zone activities. If you recognize them you legitimize them. NATO efforts are not covert or gradual strategies nor are they controversial in law. In short, gray zone activities should not be mixed with hybrid war and should not be seen as a kind of war.

Another reason for the confusion can come from the fact that the subject is highly interdisciplinary and studied by varied branches with different motivations. Experts on security, economy, politics, and technology are looking at the same activities, but interpreting different things. In this context, it is again recommended that, like this article's efforts, these concepts should be differentiated and separated with the criteria mentioned above or more, to specify it and to decrease relevant parties.

Before closing the assessment part, we must also highlight that the gray zone discussion is neither limited to three big powers nor limited to the methods described above. Just as an example, to attract Turkish scholars' attention, even Turkey is sometimes mentioned either as a victim[61] or a perpetrator of 'gray zone' activities. For example, Turkey is assessed as one of the six "revisionist or dissatisfied powers" who has the potential to apply gray zone tactics.[62] Similarly, Turkey is claimed to have been applying gray zone activities in Syria by using proxies to manipulate and control the conflict[63] or by asserting 'gray zones' in the Aegean Sea to expand its sovereignty.[64] In another example, Turkey's medical aid during the Coronavirus pandemic in 2020 is assessed as opportunism for a more assertive foreign policy and willingness to present itself as an alternative to China. Moreover, the article continues with a comparison between China and Turkey in terms of using the adaptive industry within the defense sector,

[61] For example, Turkey is asserted to have been in a multi-front hybrid war with its neighbors. See: Bingöl, "Hybrid War", p. 8.
[62] Mazarr, ibid, p.11.
[63] Rebecca K.C. Hersman, *Meeting Security Challenges in a Disordered World*, Rowman & Littlefield, June 2017, p. 99.
[64] Alexis Heraclides, *The Greek-Turkish Conflict in the Aegean*, New Perspectives on South-East Europe Series, Palgrave Macmillan, London, 2010, pp. 209-213.

and the development of armed drones as military might.[65] These examples indicate that the Gray Zone Concept is quite a new concept and has a potential to include all subjects of power struggle and information war, and all new methods such as innovations in different sectors, from drone technology to vaccine development in the same context. Examples also show that Turkey is not exempt from this discussion.

Concluding Remarks

As a consequence of the analysis and assessment; firstly it can be asserted that comparing China with Russia might not provide a perfect analogy, but it might serve a certain purpose. From this perspective, Russian efforts such as cyber-attacks, propaganda, political campaign, and abusing media against NATO and the EU can be likened to Chinese efforts in Asia. Besides, trying to create monopolies and dependencies, using secret and coercive political and information war tactics are common in both cases. However, Russia's Crimea annexation and following violence in Eastern Ukraine presents a typical hybrid warfare case, since it contains military tools which resulted in thousands of deaths. Contrarily, it is hard to find a hybrid warfare example in which China has triggered, involved, or supported even though it is the most cited actor of the Gray Zone. Likewise, while technology theft, reverse engineering, and imitation tools are widely seen in China's case, Russia is known as already at a good level in innovative and military technology. Therefore, we can assert that the Hybrid War Concept matches very well to Russian politics and interventions, while the Gray Zone Concept fits perfectly for China with its economy based strategies.

In the same context, we can draw another conclusion that creation, re-creation, and evolution of the Gray Zone Concept have a direct correlation with the shift in the US strategical security concerns. In fact, it was known that China would replace the US in terms of economy, but later on, there also seemed a new perception in the US that China was giving signals to change its policies towards a more assertive and aggressive manner against

[65] Marc Pierini, "Emerging from the Pandemic, Turkey Rolls out a More Assertive Foreign Policy", *Carnegie Europe*, 03 June 2020, https://carnegieeurope.eu/2020/06/03/emerging-from-pandemic-turkey-rolls-out-more-assertive-foreign-policy-pub-81963 (Date of Access: 22 Jun 2020).

the US. Therefore, the US has changed its strategic attention from Russia to China since 2015, and revised its strategical security documents accordingly. However, most of the NATO members have seen Russia as a bigger threat than China, and only Russia and its hybrid tactics were on their agenda. Accordingly, American scholars and think-tanks conceptualized an extended version of hybrid threats by including Chinese activities but not excluding Russia. Consequently, the Gray Zone Concept emerged as a reflection of this shift and as an effort to harmonize US strategical interests with other allies' security concerns. Thus, we can conclude that the Gray Zone Concept targets China substantially, while it provides some flexibility to keep Russia and other threats at stake. Therefore, by borrowing from Cox, we can also conclude that even if it is not an international relations theory yet, the Gray Zone Concept has a specific target and a purpose.

Albeit this article asserts that the Gray Zone concept is a reflection of this shift and its adaptation to security assessments, it also acknowledges that it is a phenomenon and deserves to be dealt with seriously by limiting it, not expanding it. Because deterring gradualist gray zone strategies is generally more difficult than conventional threats since the short term interests are less significant than escalation risk. However, if we let them pass over, long-term consequences and cumulative after-wit effects might be inevitable to all stakeholders of the international community. Similarly, China can be seen as the only main threat to the US for this decade. Nevertheless, when considering its development acceleration, one might predict that China changes its peaceful stance to a monopolist and coercive superpower in the next decades. There have precedents in world history.

Consequentially, 'what should be done to encounter gray zone threats?' is a valid question, but subject for another article. However, we can suggest at least one answer, based on the findings. Due to the United Nations (UN) Charter and other overarching documents defining the act of aggression very strictly to avoid military intervention or arbitrary inference, new and revisionist powers often tend to apply gray zone and hybrid activities. Namely, strong international norms against intervention conduced to create alternative methods. Thus, the solution might lie in the same approach. Since this paper asserts that gray zone activities are state-centric and should be seen in the milieu of interventionism, if NATO and other allies are fully convinced of the concept, these activities

can be recognized as an intervention and thus can be codified in international law in the context of non-intervention principle. Likewise, including cyber-attacks in NATO's Article 5 principle might be a good start to update international law codes to cover the loopholes which are increasingly abused. Considering the fact that Russia and China give a special emphasis on violation of the principle of sovereignty, the benefit of this approach can be understood better.

Finally, although the term and concept are not new, it is predictable that the Gray Zone Concept will have wider recognition, will be conceptualized more, and will keep its importance in the near future, while Turkey will continue to be a part of discussions. Therefore, we believe that the Gray Zone Concept deserves more attention in Turkish security studies, since it offers a wide range of research interests for Turkish scholars, albeit they are beyond the scope of this article. For example; impacts of the neighboring hybrid and gray zone threats to Turkey, effectiveness of the recent measures in cyber defense, social media, international trade, and technology development, as well as the relationship between the border security-counterterrorism and hostile hybrid-gray zone activities are different and crucial subjects for future studies in Turkish security literature.

Özet

Güvenlik çalışmalarında; 2006'dan bu yana hibrit savaş kavramı baskın konumunu korusa da 2015 sonrası Rusya ve Çin'le ilişkili olarak 'Gri Bölge' kavramına da artan biçimde yer verilmeye başlandığı görülmektedir. Örneğin, ABD Stratejik Dokümanları, adını doğrudan zikretmese de 'Gri Bölge' tehditlerine değinmekte ve bu aktivitelerin stratejik etkilerinin Soğuk Savaş sonrasından bu yana en üst seviyeye ulaştığını iddia etmektedir. Benzer şekilde, NATO ilk kez Çin'i bir tehdit olarak değerlendirmiş, Rusya ve Çin'in bazı 'gri bölge' stratejilerinin geleceğin güvenlik ortamı için geri döndürülemez sonuçlar doğurabileceğini tartışmaya başlamıştır. Söz konusu tartışmalarda; bir bölgenin fiziki yapısını veya hukuki statüsünü gizlice değiştirme çabaları, siber saldırılarla bilgi çalma veya bir seçimi veya kararı etkilemeye çalışma, sahte medya kuruluş ve faaliyetleriyle politik konuları maniple etme, belli kaynak ve teknolojilerde bağımlılık veya tekelleşme yaratmak maksadıyla ekonomik baskı, zorlama, hırsızlık, ispiyonculuk,

rüşvet, yolsuzluk ve şantaj gibi yasa dışı yollara başvurma yöntemleri yeni nesil 'gri bölge tehditleri' olarak kabul edilmektedir. Bu yöntemlerin ise ağırlıklı olarak Rusya ve Çin tarafından küresel güç mücadelesinin bir parçası olarak kullanıldığı iddia edilmektedir.

Diğer taraftan akademik yazında, gri bölge aktiviteleri, hibrit tehditler, bunların teorik ilişkisi ve uygulamaları konusunda ciddi bir tartışma ve görüş farklılığı olduğu gözlemlenmektedir. Bazı çalışmalar, Hibrit Savaş Konsepti ve Gri Bölge Konseptini birbirinin yerine kullanmakta, bazı çalışmalar ise bunları ayırmakta veya tamamen yok saymaktadır. Bununla birlikte, Türkiye için konu çok yeni olmasına rağmen Türkiye'yi de söz konusu gri bölge aktivitelerinin ve hibrit taktiklerin mağduru veya uygulayıcısı olarak gösteren çalışmalar bulunmaktadır. Bu kapsamda bu makalede; Gri Bölge Konsepti ile Hibrit Savaş Konseptinin teorik ilişkisi nedir?, neden Hibrit Savaş Konsepti Gri Bölge Konseptini kapsayacak şekilde genişletilmiş veya değiştirilmiştir? ve bu değişik geleceğin güvenlik ortamını nasıl etkileyecektir? sorularına cevap aranmıştır. Bu maksatla; öncelikle hibrit savaş ve gri bölge kavramlarının tanımları, özellikleri, benzerlikleri ve farklılıkları incelenmiş, daha sonra Rusya ve Çin örnekleri üzerinden söz konusu konseptlerin uygulamaları karşılaştırarak belli çıkarım ve değerlendirmelerde bulunulmuştur.

Makale; öncelikle her iki kavramın da yeni olmadığı, fakat incelenen tanımlar ve sahadaki uygulamaları ile birbirlerinden farklı özellikler barındırdığı sonucuna ulaşmıştır. Bu noktada, en büyük benzerlikleri başta elektronik harp ve siber savaş alanında olmak üzere teknolojinin sağladığı tüm imkânların sonuna kadar kullanılmasıdır. Bu durum, söz konusu yöntemleri bir yandan daha etkin diğer yandan daha görünür hale getirmiştir. Gri Bölge aktivitelerinin hibrit tehditlerden en büyük farklarının ise devlet merkezli olması ve stratejik bir amaca yönelik kademeli politikaların ilk bakışta devletler hukukunda suç sayılmayacak biçimde uygulanması olduğu görülmektedir. Aynı paralelde, Gri Bölge Konseptinin hibrit savaş içeriğinden tamamen ayrıştırılmasının ve özgünleştirilmesinin yazındaki kavram kargaşasını giderebileceği, konseptin analiz ve açıklama gücünü artırabileceği değerlendirilmektedir.

Diğer taraftan, yazındaki birçok çalışmanın aksine, Rusya ve Çin'in benzerlikleri kadar farklı yöntem ve özelliklerinin olduğu da gözlemlenmektedir. Örneğin Rusya, Kırım örneğinde görüldüğü üzere, yakın çevresinde askerî güç kullanmaktan çekinmemekte, ulusal güvenliğini tehdit

altında hissettiğinde sert ve çabuk sonuç alan 'hibrit' tedbirlere başvurmaktadır. Ancak Çin'in büyük çaplı ölümlerle sonuçlanan bir askerî müdahalesi veya benzer bir 'gri bölge' aktivitesi bulunmamaktadır. Diğer taraftan Çin; tersine mühendislik, teknoloji hırsızlığı, ispiyonculuk ve ekonomik zorlama tedbirlerini uzun süreli ve gizli yöntemlerle uygularken, Rusya özellikle askerî teknolojide zaten belli bir seviyededir ve mecbur kaldığında geri adım atmak yerine mevcut teknolojisini ve kendisine müzahir unsurları kullanarak doğrudan müdahale yoluna gitmektedir. Genel bir değerlendirmeyle, Hibrit Savaş konseptinin daha çok Rusya'yı tanımladığı, fakat Gri Bölge Konseptinin Rusya'yı da dışarıda bırakmaksızın asıl olarak Çin'i hedef aldığı söylenebilir.

Netice itibariyle; bu makalede her iki ülkenin aynı konsept ve çalışmalarda bir araya getirilmesinin özel bir amaç taşıdığı değerlendirilmiş ve Gri Bölge Konseptinin, ABD'nin stratejik dikkatini Rusya'dan Çin'e kaydırmasının bir yansıması olduğu ve ABD'nin kendi çıkarları ile diğer müttefiklerinin güvenlik kaygılarını örtüştürmeyi amaçladığı sonucuna varılmıştır. Çünkü Çin, artık ABD için daha büyük bir tehlikedir ve mevcut Hibrit Savaş Konsepti Çin'in yöntemlerini yeterince kapsayamamaktadır. Fakat NATO ve Avrupa Birliği için hala en belirgin tehdit Rusya'dır. Bu yönüyle Gri Bölge Konsepti; her ne kadar bir teori olmasa da müttefiklere ortak bir çalışma zemini vaat etmesi ve Rusya ile Çin'i aynı tanımda birleştirmesi boyutlarıyla belli bir amaca hizmet etmektedir ve Robert Cox'un geleneksel uluslararası ilişkiler teorileri için ortaya attığı "teorilerin her zaman özel bir hedefi ve bir amacı vardır" tezini hatırlatmaktadır. Son olarak Gri Bölge Konseptinin, zamanla daha çok kuramlaştırılabileceği, gelecek dönem güvenlik çalışmalarında daha çok yer bulabileceği ve Türk akademik yazını için yeni araştırma alanları sunabileceği öngörülmektedir.

Declaration of Conflict of Interest:

As the sole author of this article, I warrent that there is no conflict of interest to declare, nor is there any financial or academic support taken.

Thanks:

The Author thanks to Mrs. Amelia C. Gracia, Dr. Öner Akgül and Dr. Cüneyt Özşahin for their contributions to draft versions of this article.

References

Books

CLAUSEWITZ, Carl von. *On War*, Michael Howard and Peter Paret, (ed. and trans.), Princeton University Press, Princeton, NJ, 1984.

CONLEY, Heather, MINA James et all., *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe*, CSIS, Lanham: Rowman & Littlefield, Washington, DC, 2016.

HERACLIDES, Alexis. *The Greek-Turkish Conflict in the Aegean*, New Perspectives on South-East Europe Series, Palgrave Macmillan, London, 2010.

HERSMAN, Rebecca K.C. *Meeting Security Challenges in a Disordered World*, Rowman & Littlefield, June 2017.

HICKS, Kathleen, FRIEND, Alice Hunt et all., *Campaigning in the Gray Zone by Other Means*, CSIS International Security Program Report, Rowman & Littlefield, July 2019.

HOFFMAN, Frank G. *Conflict in the 21st Century: The Rise of Hybrid Wars*, Potomac Institute Publishing, Virginia, 2007.

KOFMAN, Michael. *Lessons from Russia's Operations in Crimea and Eastern Ukraine*, Library of Congress Cataloging-in-Publication, RAND Corporation, Santa Monica, California, 2017.

MAZARR, Michael J. *Mastering the Gray Zone: Understanding a Changing Era of Conflict*, The Strategic Studies Institute and U.S. Army War College Press, Ashburn Drive, Carlisle, PA, December 2015.

MORRIS, Lyle J., Mazarr, Michale J. et. all., *Gaining Competitive Advantage in the Gray Zone*, RAND Corporation, Santa Monica, California, 2019.

VALASEK, Tomas (ed.) *New Perspectives on Shared Security: NATO's Next 70 Years*, Carnegie Endowment for International Peace Publications, Brussels, 2019.

Articles

AKGÜL, Fatih. "Effects of Eurasian Energy Policies of Putin's Russia on Turkish-Russian Relations" (in Turkish), *Güvenlik Stratejileri Dergisi*, 2007, Vol: 3, No: 5, 129-157.

BACHMANN, Sascha Dominik and GUNNERIUSSON, Hakan. "Hybrid Wars: The 21st-Century's New Threats To Global Peace And Security", *Scientia Militaria, South African Journal of Military Studies*, Vol 43, No. 1, 2015, 77-98.

BINGÖL, Oktay. "Hybrid War and Its Strategic Implications to Turkey", *Gazi Akademik Bakış*, 2017, Vol: 11, No: 21, 107-132.

CARMENT, David and BELO, Dani. "Gray-zone Conflict Management: Theory, Evidence, and Challenges", *European, Middle Eastern, & African Affairs*, Summer 2020, 21-41.

COOPER, Zack. "Understanding the Chinese Communist Party's Approach to Cyber-Enabled Economic Warfare", *Foundation for Defense of Democracies*, September 2018, https://s3.us-east-2.amazonaws.com/defenddemocracy/uploads/documents/REPORT_ China_CEEW.pdf, (Date of Access: 04 January 2020).

COX, Robert W. "Social Forces, States and World Orders: Beyond International Relations Theory", *Millennium: Journal of International Studies*, 1981, Volume: 10, Issue: 2, 126-155.

ELKUS, Adam. "50 Shades of Gray: Why the Gray Wars Concept Lacks Strategic Sense", *War on the Rocks*, 15 December 2015, https://warontherocks.com/2015/12/50-shades-of-gray-why-the-gray-wars-concept-lacks-strategic-sense/ (Date of Access: 7 February 2020).

GERASIMOV, Valery. "The Value of Science in in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying Out Combat Operations," *Military Review*, Vol. 96, January-February 2016, 23-29.

GLATZ Rainer L. and Zapfe, Martin. "NATO Defense Planning between Wales and Warsaw: Politico-military Challenges of a Credible Assurance against Russia", *German Institute for International and Security Affairs*, SWP Comments No: 5, January 2016, https://www.swp-berlin.org/fileadmin/contents/products/comments/2016C05_glt_ Zapfe.pdf (Date of Access: 10 May 2020).

HOFFMAN, Frank G. "On Not-So-New Warfare: Political Warfare vs. Hybrid Threats," *War on the Rocks*, 28 July 2014, warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/ (Date of Access: 15 March 2020).
HOFFMAN, Frank G. "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges", *Prism*, Vol.7, No.4, November 2018, 30-47.
HUANG, Philip. "How Has the Chinese Economy Developed So Rapidly? The Concurrence of Five Paradoxical Coincidences", *Modern China*, 2015, Vol.41, No.3, 239-277.
JORDAN, Javier. "International Competition Below the Threshold of War: Toward a Theory of Gray Zone Conflict", *Journal of Strategic Security*, 14, No. 1, 2020, 1-24.
KORTEWEG, Rem. "Energy as a tool of foreign policy of authoritarian states, in particular Russia", *EU Policy Department for External Relations*, PE 603.868, April 2018, https://www.europarl.europa.eu/RegData/etudes/STUD/2018/603868/EXPO_STU(2018)603868_EN.pdf (Date of Access: 22 April 2020).
MANKOFF, Jeffrey. "Russia's Latest Land Grab: How Putin Won Crimea and Lost Ukraine", *Foreign Affairs*, May/Jun 2014, Vol.93, Issue 3, 60-68.
MATISEK, Jahara W. "Shades of Gray Deterrence: Issues of Fighting in the Gray Zone", *Journal of Strategic Security*, 2017, Vol.10, No.3, 1-26.
PINCUS, Rebecca. "China's Polar Strategy: An Emerging Gray Zone?", *The Diplomat*, 06 July 2018, https://thediplomat.com/2018/07/chinas-polar-strategy-an-emerging-gray-zone/ (Date of Access: 7 January 2020).
SORENSEN, Heine and NYEMANN, Dorthe Bach. "Going Beyond Resilience. A revitalised approach to countering hybrid threats", *Hybrid CoE Strategic Analysis*, No: 13, 8 January 2019, https://www.hybridcoe.fi/wp-content/uploads/2020/06/Strategic-analysis-Sorensen-Nyeman-11-2018.pdf. (Date of Access: 04 January 2020).
STOKER, Donald and WHITESIDE, Craig. "Blurred Lines: Gray-Zone Conflict and Hybrid War-Two Failures of American Strategic Thinking," *Naval War College Review*, 2020, Vol.73, No.1, 13-48.
VOTEL, Joseph L., CLEVELAND, Charles T. et all. "Unconventional Warfare in the Gray Zone," *Joint Forces Quarterly*, 1st Quarter 2016, No: 80, 101-109.
WALLANDER, Celeste A. "NATO's Enemies Within", *Foreign Affairs*, Jul/Aug 2018, Vol. 97, Issue 4, 70-81.

Reports

CORDESMAN, Anthony H. and BURKE, Arleigh A "China and the US: Cooperation, Competition and/or Conflict", *CSIS Report*, 1 October 2019, https://www.csis.org/analysis/china-and-united-states-cooperation-competition-andor-conflict (Date of Access: 7 January 2020).
North Atlantic Council, *NATO Wales Summit Declaration*, 05 September 2014, https://www.nato.int/cps/en/natohq /official_texts_112964.htm (Date of Access: 22 February 2020).
The White House, *National Security Strategy of the United States of America*, Washington, D.C., December 2017.
Office of the Director of US National Intelligence, *Global Trends: Paradox of Progress*, National Intelligence Council, Washington, DC, 2017.
U.S. Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge*, Washington, D.C., January 2018.

Internet Resources

AROSTEGUI, Martin. "Spain Warns Russia's Catalonia Hacking Efforts Could Intensify", *VOA News*, 23 January, 2018. https://www.voanews.com/europe/spain-warns-russias-catalonia-hacking-efforts-could-intensify (Date of Access: 20 July 2020).
BRANDS, Hal. "Paradoxes of the Gray Zone", *Foreign Policy Research Institute E-Notes*,

5 February 2016, https://www.fpri.org/article/2016/02/paradoxes-gray-zone/ (Date of Access: 9 July 2020).
CARMENT David and BELO, Dani. "War's Future: The Risks and Rewards of Gray-Zone Conflict and Hybrid Warfare", *Canadian Global Affairs Institute Policy Paper*, October 2018, https://www.cgai.ca/wars_future_the_risks_and_rewards_of_grey_zone_conflict_and_hybrid_warfare, (Date of Access: 11 January 2020).
CORDESMAN, Anthony H. and HWANG, Grace. "Chronology of Russian Gray Zone and Hybrid Operations", *Center for Strategic and International Studies*, 02 July 2020, https://www.csis.org/analysis/chronology-possible-russian-gray-area-and-hybrid-warfare-operations (Date of Access 12 July 2020).
CORERA, Gordon. "Russia 'interference' report to be published", *BBC*, 16 July 2020, https://www.bbc.com/news/uk-politics-53428246 (Date of Access: 20 July 2020).
FAULCONBRIDGE, Guy. "UK says Russia tried to meddle in election by leaking U.S. trade documents", *National Post*, 16 July 2020, https://nationalpost.com/pmn/news-pmn/crime-pmn/uk-says-russia-tried-to-meddle-in-election-by-leaking-u-s-trade-documents-3 (Date of Access: 20 July 2020).
FRENKEL, Sheera, CONGER, Kate et. all. "Russia's Playbook for Social Media Disinformation Has Gone Global," *New York Times*, 31 January 2019, https://www.nytimes.com/2019/01/31/technology/ twitter-disinformation-united-states-russia.html (Date of Access: 11 March 2020).
HADDICK, Robert. "Salami Slicing in the South China Sea," *Foreign Policy*, 3 August 2012, https://foreignpolicy.com/2012/08/03/salami-slicing-in-the-south-china-sea/ (Date of Access: 20 May 2020).
HERD, Graeme P. "Hybrid Conflict 2.0 Targeting the West", *Concordiam*, 20 May 2016, George Marshall Center, https://perconcordiam.com/hybrid-conflict-2-0-targeting-the-west/ (Date of Access: 22 April 2020).
KENNAN, George F. "Policy Planning Staff Memorandum", *National Archives*, RG 273, Records of the National Security Council, NSC 10/2, 4 May 1948, http://academic.brooklyn.cuny.edu/history/ johnson/65ciafounding3.htm (Date of Access: 21 January 2020).
PAWLAK, Patryk. "At a glance: Understanding Hybrid Threats", *European Parliamentary Research Service Fact Sheet*, PE 564.355, June 2015, http://www.europarl.europa.eu/RegData/etudes/ATAG/2015/564355/EPRS_ATA(2015)564355_EN.pdf (Date of Access: 29 January 2020).
PIERINI, Marc. "Emerging from the Pandemic, Turkey Rolls Out a More Assertive Foreign Policy", *Carnegie Europe*, 03 June 2020, https://carnegieeurope.eu/2020/06/03/emerging-from-pandemic-turkey-rolls-out-more-assertive-foreign-policy-pub-81963 (Date of Access: 22 Jun 2020).
STARES, Paul B. *Preventive Priorities Survey 2020*, Council on Foreign Relations\Center for Preventive Actions, https://cdn.cfr.org/sites/default/files/report_pdf/PPS_2020_12162019_CM_ single_0.pdf (Date of Access: 27 May 2020).
STOLTENBERG, Jens. "Remarks", *NATO 2030- Strengthening the Alliance in an increasingly competitive world Online Conference*, 8 June 2020, https://www.nato.int/cps/en/natohq/opinions_ 176197.htm (Date of Access: 12 July 2020).
WONG, Edward. "The US versus China: A New Era of Great Power Competition, but Without Boundaries", *The New York Times*, 26 June 2019. https://www.nytimes.com/2019/06/26/world/asia/united-states-china-conflict.html (Date of Access: 7 January 2020).