Committee: Disarmament & International Security (GA1)
Agenda Item: Mitigating the threats posed by the prolonged use of hybrid warfare methods
Student Officer: Sanem Naz Kafalı - President Chair

Introduction

The ever-changing world, developing technology, and globalization have revolutionized many aspects of our daily lives over the last century. This constant change and development have not only affected our daily lives but also created unknowns, new approaches to problems, and new perspectives on matters in many fields, from art and science to economics and politics. Not surprisingly, one of these areas is warfare.

Originally defined as a “range of different modes of warfare including conventional capabilities, irregular tactics, and formations, terrorist acts including indiscriminate violence and coercion and criminal disorder” by Hoffman in 2007, hybrid war is a type of war in which many different kinds of war are used at the same time for a collective purpose. (ÖZEL and İNALTEKİN). Due to differing availability and constant technological advancements, the meaning of "hybrid war" fluctuates and evolves throughout time and space. Hence, there is no fixed definition.

The concept of hybrid warfare emerged due to shifting international dynamics, growing political unpredictability, and the requirement that a successful conflict take many distinct forms tailored to the goals at hand. Although it may seem like a very new concept, it has its roots as far back as 3,000 years ago. Yet, it gained prominence in military discussions in the early 2000s. The term often gets confused with the grey zone conflict. Yet, they differ significantly regarding the scope of tactics, visibility, and objectives.

Several characteristics define hybrid war, such as its asymmetric nature, integration of technology, and psychological operations it involves. Asymmetric nature essentially means the asymmetric tactics used usually by the weaker side aiming to confront the more substantial side by resorting to unconventional means. This sometimes involves using proxy forces to achieve strategic aims while avoiding confrontation. Furthermore, modern hybrid warfare primarily uses advanced technology like drones and cyber capabilities, although having existed for millennia at various stages of technical development. This increases efficacy and permits flexibility and adaptation. A final crucial aspect of hybrid warfare is the psychological operations it entails, which often aim to influence public opinion, cause misunderstandings, etc., and incite distrust in opponents (Wither & Hoffman et al.)

As opposing sides attempt to accomplish their objectives on the modern battlefield, some hybrid warfare tactics become more apparent. Economic coercion, disinformation campaigns, cyber warfare, and urban guerrilla warfare are examples of many more. Hezbollah's successful employment of both guerrilla tactics and conventional military operations makes the 2006 battle between Israel and Hezbollah a notable example of hybrid warfare (“War by All Means: The Rise of Hybrid Warfare”). The focused overview's section on hybrid warfare tactics will further detail these strategies.

Traditional military doctrines need to be reevaluated in light of the emergence of hybrid warfare. Understanding a broad range of hybrid tactics is crucial for efficient defense and reaction plans, as countries use them more frequently for political gain.

This report entails the definition of important terms, major actors involved, a focused overview, a timeline of important events, related documents, past solution attempts, possible solutions, and useful links in that respected order.

Definition of Key Terms

Hybrid warfare: "the use of a range of different methods to attack an enemy, for example, the spreading of false information, or attacking important computer systems, as well as, or instead of, traditional military action" (Cambridge Dictionary)

Grey zone conflict: "activities by a state that are harmful to another state and are sometimes considered to be acts of war, but are not legally acts of war"(Cambridge Dictionary)

Kinetic Operations: military operations that employ conventional weaponry and physical force to accomplish particular goals (Data Science Association).

Cyber Warfare: "the use of computer technology to disrupt the activities of a state or organization, especially the deliberate attacking of information systems for strategic or military purposes." (Oxford Dictionary)

Disinformation: "False information deliberately and often covertly spread (as by the planting of rumors) to influence public opinion or obscure the truth" (Merriam-Webster Dictionary)

Lawfare: "the use of legal action to cause problems for an opponent" (Cambridge Dictionary)

Non-State Actors: "an individual or organization that has significant political influence but is not allied to any particular country or state." (Oxford Dictionary)

Urban Guerrilla Warfare: "type of warfare fought by irregulars in fast-moving, small-scale actions against orthodox military and police forces and, on occasion, against rival insurgent forces, either independently or in conjunction with a larger political-military strategy." (Britannica)

Psychological Operations (PSYOPS): "A military operation usually aimed at influencing the enemy's state of mind through non-combative means (such as distribution of leaflets)" (Merriam-Webster Dictionary)

Proxy Force: a variety of non-state armed groups, such as militias, insurgents, and private military corporations, that are used by a state to accomplish military goals secretively, frequently to avoid direct engagement in wars (Britannica).

Major Actors Involved

Russia

As a central figure in warfare, Russia, adopting "active defense" as a means of self-preservation, blends conventional military force with non-military tactics to establish dominance in the region after realizing the limitations of traditional military confrontations against NATO. Russia's warfare uses various areas of modern warfare, primarily information warfare, cyber operations, and proxy forces. In the past, following this strategy, they captured land without prompting a robust NATO military reaction in the annexation of Crimea. Moreover, Russia, through its use of hybrid warfare, aims to destabilize its neighbors and keep them from joining NATO and other Western alliances. The wars between Georgia and Ukraine are clear examples of this. (Chivvis & Clark & Erol and Oğuz & SWJ Staff)

China

China uses misinformation operations and propaganda to manipulate the public both at its borders and overseas by using social media and narratives that are controlled by the state. China has also used its cyber capabilities to attack companies worldwide, disrupt vital infrastructure, and carry out espionage since the early 2000s (Newton & "Institute for the Study of War").

Moreover, initiatives such as "Made in China 2025" seek to promote technological developments supporting military goals, further demonstrating China's growing more profound dependence on hybrid warfare (Gasier).

A good example of its use of hybrid warfare is in the South China Sea. Through the employment of the "salami-slicing" strategy in the South China Sea, China progressively established authority over disputed territories by combining coast guard activities with private fishing boats. China's hybrid warfare activities are mostly directed at Taiwan. In the past, Beijing used a variety of strategies to weaken the Taiwanese government, including cyberattacks and psychological operations (Solmaz).

United States of America (USA)

The US military is aware of the urgent need to develop a unified approach to counter hybrid threats, particularly those posed by Russia, as Russia's undeniable success in the areas is demonstrated by its deployment of hybrid tactics in Georgia and Ukraine. The USA's first encounter with hybrid war tactics goes as far back as the Vietnam War. More recently, ISIS and other state actors deploying cyber capabilities and proxy troops to subvert conventional military advantages posed hybrid threats for the USA (SWJ Staff & Wikipedia)

Belarus

Belarus' weaponization of migration in reaction to sanctions imposed by the EU and other Western countries after the contentious 2020 presidential elections is an example of its engagement in hybrid warfare. Migration from the Middle East to EU nations, including Poland, Lithuania, and Latvia, was made easier by Belarusian authorities, causing a humanitarian crisis and putting political pressure on these countries (Bendern).

The Islamic State of Iraq and Syria (ISIS)

ISIS emerged as a small Al Qaeda affiliate in Iraq that focused on suicide bombings and agitating the Sunni Muslim minority there against the Shiite majority (Thiele).

ISIS uses asymmetric warfare, guerilla warfare, and conventional military capabilities. The organization is well known for its bombings, artillery and mortar shelling, suicide attacks, aerial surveillance, and even chemical attacks. It uses terrorist strategies to create fear and disturb social order. Following the Hezbollah paradigm, the group now occupies a highly hybrid position in warfare since its advance throughout western Iraq (Thiele).

Hezbollah

Hezbollah employs advanced weaponry and unconventional tactics in a combination of traditional military operations and guerilla warfare. This keeps them unexpected and flexible while enabling them to take advantage of primarily Israel's military weaknesses. Iran's assistance and expertise in wars such as the Syrian Civil War further enhance their skills. Hezbollah's weaponry has been greatly enhanced both during and after the Syrian conflict (Murat Yeşiltaş).

NATO

NATO recognizes that its member states are in danger from hybrid threats, especially those from China and Russia; hence, it enhances national resilience, raises situational awareness, and creates collective defensive mechanisms. NATO has been using operational drills since 2015 to get ready to combat hybrid warfare in given circumstances. Moreover, Article 5 of the North Atlantic Treaty, which states that an attack on one member is an attack on all, is invoked to prevent hybrid actions from potentially triggering this clause (NATO)

General Overview of the Issue

General Characteristics of Hybrid Warfare

Combining traditional and unconventional tactics to accomplish strategic goals, hybrid warfare is defined by the adaptive and simultaneous use of several forms of warfare. It is often multifaceted, synchronizes several methods, is asymmetric and nonlinear, allows denial because of ambiguity, and utilizes technology.

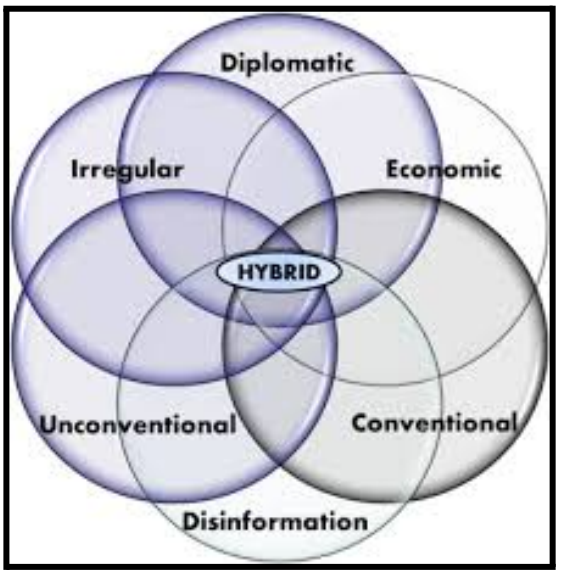

Image 1: Venn Diagram Showing the Characteristic of Hybrid Warfare

Hybrid warfare aims to take advantage of a country's weaknesses in politics, the military, the economy, society, information, and infrastructure. The process includes non-kinetic techniques such as misinformation campaigns, cyber operations, and unconventional tactics like guerilla warfare. In hybrid warfare, asymmetric tactics are employed by less powerful parties to oppose stronger adversaries. These methods frequently involve the use of non-state actors and are unconventional. Because of the ambiguity of these approaches, adversaries find it challenging to directly link acts to a particular side. Due to the frequent non-linear effects of hybrid warfare, opponents find it difficult to develop successful counterstrategies.

Moreover, technology, especially digital means for communication, propaganda, and cyberattacks, is a major component of modern hybrid warfare. The quick spread of information via social media can intensify the impact of hybrid strategies, affecting political results and public opinion. As a result, many countries choose to ensure the media at times of crisis. Additionally, the UN has drafted several resolutions and reports on cybersecurity concerns on the matter.

Hybrid Warfare Tactics

A number of noteworthy strategies are employed in hybrid warfare. These include terrorism, economic warfare, political warfare, cyberwarfare, information warfare, guerrilla warfare, and, last but not least, traditional military operations.

Guerrilla warfare is a small-scale, fast-paced combat in which irregulars fight against conventional police and military forces, Since the Peninsular War, it has been known by several names, including mercenaries, partisans, insurgents, irregulars, and rebels. Guerrillas are recognized as terrorists, brigands, bandits, savages, barbarians, and outlaws, but they remain a powerful force in global wars (Britannica)

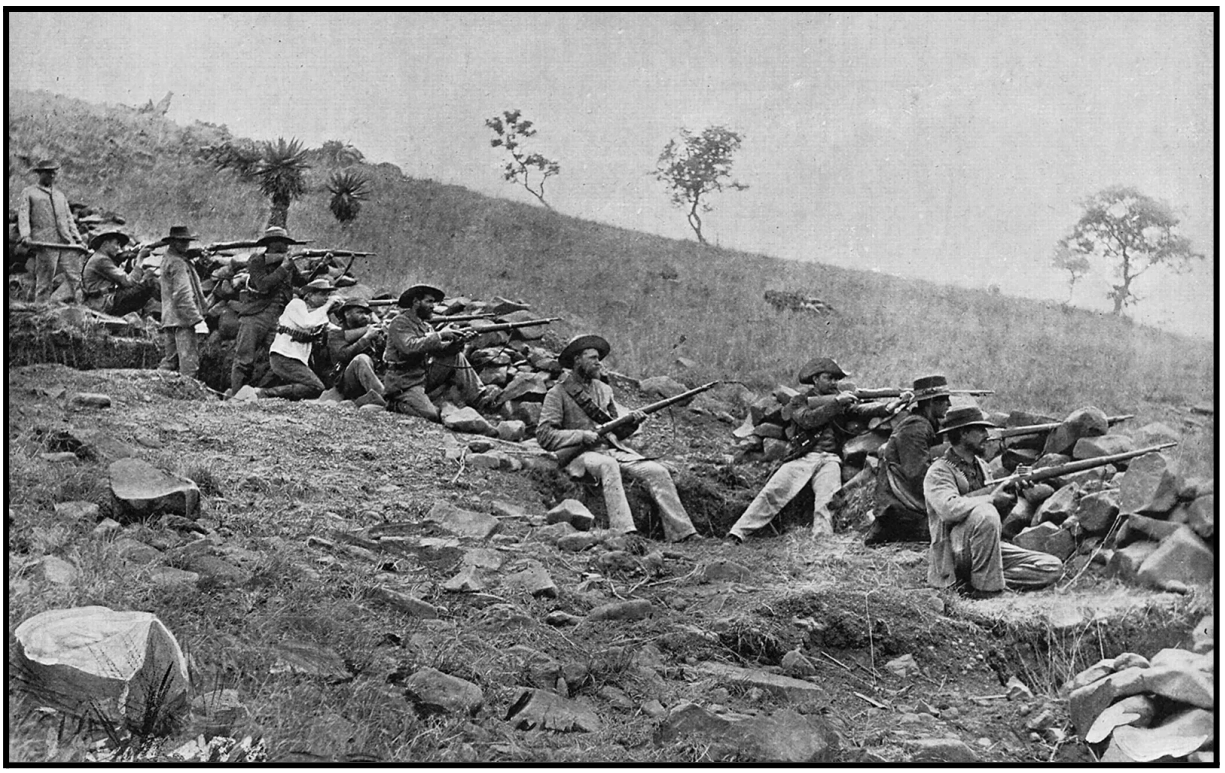

Image 2: Guerrilla Warfare

Furthermore, cyber warfare is another frequently used area. It involves attacking an adversary's information systems to interfere with, weaken, or alter their capabilities. Some examples are hacking into vital infrastructure, stealing private information, or initiating denial-of-service attacks. This strategy uses misinformation campaigns, psychological manipulation, and propaganda to strategically employ information to change public opinion and behavior, manipulate political results, or cause confusion or disagreement among the target audience.

Frequently, hybrid warfare employs non-state actors, also known as proxy organizations, to conduct military operations on behalf of a state or organization, enabling the sponsoring state to accomplish its goals without direct participation or possible retaliation.

Image 3: Proxy War Cartoon

Hybrid actors also undermine an adversary's financial stability and popular support through economic strategies, diplomatic initiatives, legal measures, and political meddling, which is also known as lawfare. They can use trade dependencies or conduct cyberattacks against financial institutions. In addition, they can influence government and policy in another state by supporting particular candidates or providing funds to political parties.

History of Hybrid War

Hybrid warfare has roots in the Peloponnesian War, in which the Spartans and Athenians employed irregular soldiers and direct military engagement. Coming closer to the 21st Century. The American Revolutionary War in the 1700s also combined regular army operations with local militia tactics. In the 1800s, Rafael Carrera blended traditional military operations with guerilla warfare. Hybrid elements were also present in the Napoleonic Wars, where Spanish insurgents and British soldiers worked together.

Image 4: Hybrid Warfare in the Vietnam War

Modern Examples

Israel–Hezbollah War

The 2006 Lebanon War was a significant dispute between Israel and Hezbollah. The conflict began with a cross-border Hezbollah attack that killed three Israeli troops and kidnapped two more. Hezbollah used the captive soldiers to pressure a deal to exchange prisoners. The Israeli government blamed Hezbollah, which turned this conflict into a war against Lebanon.

Image 5: Areas Targeted in Israel - Hezbollah War

The war in Lebanon served as an epitome of hybrid warfare. Hezbollah used guerrilla warfare and psychological operations, while Israel and Hezbollah utilized bombings and ground assaults with highly advanced surveillance and weaponry. Through media manipulation and propaganda, Hezbollah presented itself as an armory against Israeli invasion. (Britannica)

Russia's annexation of Crimea

As part of its 2014 military operation in Crimea, Russia used unmarked troops referred to as "little green men." In a contentious referendum, most voters favored joining Russia after the Crimean parliament. In March 2014, the annexation of Crimea into the Russian Federation was formally signed by President Vladimir Putin.

Image 6: Crimea Map

In Crimea, hybrid warfare includes information warfare, using unmarked soldiers, and taking advantage of local support. Unmarked soldiers refer to Russian soldiers whose uniforms lack symbol and are not recognized for their criminal acts. Furthermore, Russia employs propaganda efforts to influence opinions both domestically and internationally, taking advantage of some Crimea people's pro-Russian feelings to enable military operations and changes to administration without encountering strong opposition (The Economist)

Russo-Ukrainian War

Hybrid warfare techniques were used in the Russo-Ukrainian War. Russia has targeted vital systems, including communications networks and electricity grids, with cyberattacks to interfere with Ukrainian infrastructure. Furthermore, by falsely defending military operations and portraying Ukraine as a danger to Russian security, information warfare has been employed to manipulate public opinion. Moreover, Russia has maintained plausible deniability over its military engagement in eastern Ukraine by using proxy militias to gain influence (BBC & Demirkıran)

ISIL advance into Iraq

The intricate nature of modern warfare significantly rose with the 2014 invasion of Iraq by ISIL. ISIL used hybrid warfare with unconventional strategies, including terrorism and illegal activity. They employed roadside bombs, kidnappings, and psychological operations on social media to establish governance, political legitimacy, and territorial control over places it had taken over. To prevent ISIL's territorial progress, the Iraqi government used a combination of local militias, Kurdish peshmerga soldiers, and U.S. air assistance (Glenn et al.)

China - Taiwan

China and Taiwan have complex historical, political, and military relations. After retreating to Taiwan in 1949 after the Chinese Civil War, the Republic of China asserted its territorial claims. China approached Taiwan using a range of hybrid warfare strategies, such as military pressure through frequent incursions into Taiwan's air defense identification zone, cyber operations targeting government systems, economic coercion through trade restrictions and tariffs, and disinformation campaigns spreading false narratives, aiming to erode public confidence, sow discord across the country, and intimidate Taiwanese authorities and people (Solmaz).

Belarus Border Crisis

A wave of migrants trying to enter the European Union through Belarus, mainly to Poland, Lithuania, and Latvia, is the hallmark of the Belarus border crisis. 2020 elections received criticism from the world community owing to being neither free nor fair, which was the reason behind the sanctions initially imposed on Belarus. Lukashenko's regime deliberately facilitated irregular migration flows into the EU as a form of retaliation against sanctions. Lukashenko's administration purposefully allowed unauthorized migration into the EU in retaliation for sanctions (Wikipedia).

Timeline of Important Events

Date:	Event:
1916	Guerrilla warfare and British assistance were used in the Arab Revolt against the Ottoman Empire.
1944	The Soviet Union conquered the Tuvan People's Republic, signifying an early hybrid warfare instance.
1955-1975	Both the US and North Vietnam used hybrid strategies throughout the Vietnam War; the US used the CIA to fund different groups in Cambodia and Laos, while the Soviet Union supported the Viet Cong.
1998	A unipolar system dominated by the American military was established after the Cold War ended.
2003	The US invaded Iraq, marking the significance of hybrid warfare.
2006	Hezbollah and Israel's 2006 conflict occurred. Hezbollah was a proxy for Iran.
2014	Russia annexes Crimea using hybrid methods such as military force, propaganda, and cyber operations against Ukraine.
2014	ISIL used both conventional and irregular methods in its hybrid strategy against the Iraqi military. Iraq similarly responded with a combination of traditional air power, Kurdish peshmerga, and opposition forces.
2016	During the Warsaw Summit, NATO addressed hybrid threats, focusing on collective defense against state and non-state actors' hybrid warfare methods.

2016	China has been accused of engaging in hybrid warfare in the South China Sea and against Taiwan.
2018	The European Union created frameworks to address the hybrid threats, emphasizing defense against cyberattacks and misinformation.
2021	Belarus engaged in hybrid warfare through its use of migration as a weapon in response to sanctions imposed by the EU and other Western nations following the controversial 2020 presidential elections
2024	Russia's hybrid threats lead the EU to enact additional sanctions.

Related Documents

- Budapest Convention on Cybercrime
- Council of Europe Resolution 2217 (2018)
- NATO Resolution 445 (2018)
- Council of Europe Resolution 14523 (2018)
- UN Report of the Committee on Information A/79/21 (2024)
- Countering disinformation for the promotion and protection of human rights and fundamental freedoms Report of the Secretary-General A/77/287 (2024)
- European Council meeting (27 June 2024)– Conclusions 15/45 (2024)

Past Solution Attempts

Military strategy and response have continuously evolved, as seen by previous attempts to combat hybrid warfare. Other than the document provided in the above section and the conferences listed on the important events timeline, there is no contemporary attempt to tackle the issue. The repeating nature of the issue proves that the current conventions and resolutions passed on the agenda item are insufficient and are not enforced fully.

Possible Solutions

A multifaceted strategy is required to combat hybrid threats, which includes launching public awareness campaigns, improving cyber and intelligence capabilities, fortifying multilateral security alliances, and creating counter-hybrid support teams. While cyber defense programs can enhance situational awareness, details outlined in public awareness campaigns can lessen the impact of misinformation campaigns if they can reach the majority of the public and educate them on how hybrid warfare and misinformation campaigns are used. Furthermore, outlining and enforcing a new legislative and regulatory framework is necessary, as the current conventions are insufficient.

Useful Links

- NATO Library - Hybrid Warfare Resources: https://natolibguides.info/hybridwarfare/books
- Turkish National Defense University's Booklet on Hybrid Warfare: https://www.msu.edu.tr/eng/Documents/Hybrid%20Warfare.pdf
- "Hybrid Warfare Challenges" published on Security & Defence Quarterly: https://securityanddefence.pl/Hybrid-warfare-challenges,103239,0,2.html

- The Economist: https://www.google.com/aclk?sa=l&ai=DChcSEwifqNDOiZmKAxU_ZUECHQZnAJgYABAAGgJ3cw&ae=2&aspm=1&co=1&ase=2&gclid=Cj0KCQiApNW6BhD5ARIsACmEbkW4xsPrtO9NABkZgGqhCC0kEAGYh0PNMKh9O8fqbeJFFyAOfJ4bykgaAlmHEALw_wcB&sig=AOD64_06pmaZv6TB03veTqljQ-vsN8bkWA&q&nis=4&adurl&ved=2ahUKEwix9srOiZmKAxWARPEDHbTIBu8Q0Qx6BAgSEAE
- Britannica: https://www.britannica.com/topic/asymmetrical-warfare

Bibliography

"2006 Lebanon War | Description & Facts | Britannica." *Www.britannica.com*, www.britannica.com/event/2006-Lebanon-War. Accessed 8 Dec. 2024.

Baugh, Sue. "Proxy War | Armed Conflict." *Encyclopædia Britannica*, 2019, www.britannica.com/topic/proxy-war. Accessed 7 Dec. 2024.

BBC. "What Is Hezbollah in Lebanon and Will It Go to War with Israel?" *Www.bbc.com*, 3 Nov. 2023, www.bbc.com/news/world-middle-east-67307858.

Bendern, Samantha de. "Belarus Is New Weapon in Putin's Hybrid Warfare Arsenal." *Chatham House – International Affairs Think Tank*, 18 Aug. 2021, www.chathamhouse.org/2021/08/belarus-new-weapon-putins-hybrid-warfare-arsenal. Accessed 7 Dec. 2024.

Brown, David. "Ukraine Invasion: Russia's Attack in Maps." *BBC News*, www.bbc.com/news/world-europe-60506682. Accessed 8 Dec. 2024.

Cambridge University Press. "Cambridge Dictionary." *Cambridge Dictionary*, Cambridge University Press, 2024, dictionary.cambridge.org/. Accessed 7 Dec. 2024.

Chivvis, Christopher. *Understanding Russian "Hybrid Warfare" and What Can Be Done about It*. 2017, www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf. Accessed 7 Dec. 2024.

Clark, Mason. "Institute for the Study of War." *Institute for the Study of War*, Sept. 2020, www.understandingwar.org/report/russian-hybrid-warfare. Accessed 7 Dec. 2024.

*COMMITTEE on the CIVIL DIMENSION of SECURITY 215 CDS 18 E Rev.1 Fin Original: English RESOLUTION 445 on UPDATING the RESPONSES to RUSSIA'S HYBRID TACTICS *.* www.nato-pa.int/download-file?filename=/sites/default/files/2018-11/RESOLUTION%20445%20-%20UPDATING%20THE%20RESPONSES%20TO%20RUSSIA%E2%80%99S%20HYBRID%20TACTICS.pdf. Accessed 8 Dec. 2024.

Demirkıran, Özlem. "A New Hybrid War Arena: Russia's Interventions in Ukraine in 2014 and 2022." *Dergi Park*, 2022. Accessed 8 Dec. 2024.

Erol, Mehmet Seyfettin, and Şafak Oğuz. *Akademik Bakış Hybrid Warfare Studies and Russia's Example in Crimea* Hibrit Savaş Çalışmaları ve Kırım'daki Rusya Örneği*. 2015, dergipark.org.tr/tr/download/article-file/74059. Accessed 7 Dec. 2024.

Gasier, Laris. "Chinese Hybrid Warfare Approach and the Logic of Strategy(Volume 23, No. 1, 2022.)." *Nsf-Journal.hr*, 2022, www.nsf-journal.hr/nsf-volumes/focus/id/1368. Accessed 7 Dec. 2024.

Glenn, Cameron, et al. "Timeline: The Rise, Spread and Fall of the Islamic State." *Wilson Center*, 28 Oct. 2019, www.wilsoncenter.org/article/timeline-the-rise-spread-and-fall-the-islamic-state.

"Guerrilla Warfare - Origins of Modern Guerrilla Warfare." *Encyclopedia Britannica*, www.britannica.com/topic/guerrilla-warfare/Origins-of-modern-guerrilla-warfare. Accessed 8 Dec. 2024.

Hoffman, Frank, et al. "The Future of Hybrid Warfare." *Www.csis.org*, July 2024, www.csis.org/analysis/future-hybrid-warfare. Accessed 7 Dec. 2024.

"Hybrid Warfare in Vietnam – How to Win a War despite Military Defeat - Hybrid CoE - the European Centre of Excellence for Countering Hybrid Threats." *Hybrid CoE - the European Centre of Excellence for Countering Hybrid Threats*, 2017, www.hybridcoe.fi/news/hybrid-warfare-in-vietnam-how-to-win-a-war-despite-military-defeat/. Accessed 8 Dec. 2024.

"Institute for the Study of War." *Institute for the Study of War*, www.understandingwar.org/backgrounder/chinese-communist-partys-theory-hybrid-warfare. Accessed 7 Dec. 2024.

Mansoor, Peter. *Introduction Hybrid Warfare in History*. assets.cambridge.org/97811070/26087/excerpt/9781107026087_excerpt.pdf.

Merriam-Webster. "Merriam-Webster Dictionary." *Merriam-Webster.com*, 2024, www.merriam-webster.com/. Accessed 7 Dec. 2024.

Mumford, Andrew. "The New Era of the Proliferated Proxy War." *The Strategy Bridge*, 16 Nov. 2017, thestrategybridge.org/the-bridge/2017/11/16/the-new-era-of-the-proliferated-proxy-war. Accessed 8 Dec. 2024.

Murat Yeşiltaş. "Israel-Hezbollah War Will Be Costly." *SETA*, 29 June 2024, setav.org/en/opinion/israel-hezbollah-war-will-be-costly. Accessed 7 Dec. 2024.

NATO. "NATO's Response to Hybrid Threats." *NATO*, 2021, www.nato.int/cps/en/natohq/topics_156338.htm. Accessed 7 Dec. 2024.

Newton, Michael. “The Chinese Roots of Hybrid Warfare.” *CEPA*, 10 Aug. 2022, cepa.org/article/the-chinese-roots-of-hybrid-warfare/. Accessed 7 Dec. 2024.

Oxford Dictionary. “Oxford Languages.” *Oxford Languages*, Oxford University Press, 2024, languages.oup.com/google-dictionary-en/. Accessed 7 Dec. 2024.

ÖZEL, Yücel, and Ertan İNALTEKİN. *Shifting Paradigm of War*. 2017, www.msu.edu.tr/eng/Documents/Hybrid%20Warfare.pdf. Accessed 7 Dec. 2024.

“PACE Website.” *Coe.int*, 2018, assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=24762. Accessed 8 Dec. 2024.

Robert Brown Asprey. “Guerrilla Warfare | Military Tactics.” *Encyclopædia Britannica*, 13 Apr. 2018, www.britannica.com/topic/guerrilla-warfare. Accessed 7 Dec. 2024.

Secretary-General, UN. “Countering Disinformation for the Promotion and Protection of Human Rights and Fundamental Freedoms :: Report of the Secretary-General.” *Digitallibrary.un.org*, Aug. 2022, digitallibrary.un.org/record/3987886?ln=en&v=pdf.

Solmaz, Tarık. “China’s Hybrid Warfare against Taiwan: Motives, Methods, and Future Trajectory.” *Regionalsecurity.org.au*, 2024, regionalsecurity.org.au/article/chinas-hybrid-warfare-against-taiwan-motives-methods-and-future-trajectory/. Accessed 7 Dec. 2024.

Staff, SWJ. "How Russia's Hybrid Warfare Is Changing | Small Wars Journal by Arizona State University." *Small Wars Journal by Arizona State University*, 17 July 2023, smallwarsjournal.com/2023/07/17/how-russias-hybrid-warfare-changing/. Accessed 6 Dec. 2024.

The Economist. "Crimea Is Still in Limbo Five Years after Russia Seized It." *The Economist*, The Economist, 8 June 2019, www.economist.com/europe/2019/06/08/crimea-is-still-in-limbo-five-years-after-russia-seized-it. Accessed 8 Dec. 2024.

Thiele, Ralph. *ISPSW Strategy Series: Focus on Defense and International Security the New Colour of War - Hybrid Warfare and Partnerships the New Colour of War - Hybrid Warfare and Partnerships*. 2015, www.files.ethz.ch/isn/194330/383_Thiele.pdf.

"Timeline - EU Response to Russia's Invasion of Ukraine." *Www.consilium.europa.eu*, www.consilium.europa.eu/en/policies/eu-response-ukraine-invasion/timeline-eu-response-ukraine-invasion/. Accessed 8 Dec. 2024.

United Nations Report of the Committee on Information. documents.un.org/doc/undoc/gen/n24/163/34/pdf/n2416334.pdf. Accessed 8 Dec. 2024.

"War by All Means: The Rise of Hybrid Warfare." *Cidob.org*, Barcelona Center for International Affairs, 2022, www.cidob.org/en/publications/war-all-means-rise-hybrid-warfare. Accessed 7 Dec. 2024.

Wikipedia Contributors. “Hybrid Warfare.” *Wikipedia*, Wikimedia Foundation, 24 Dec. 2019, en.wikipedia.org/wiki/Hybrid_warfare. Accessed 7 Dec. 2024.

Wither, James K. “Defining Hybrid Warfare.” *Marshall Center*, www.marshallcenter.org/sites/default/files/files/2020-05/pC_V10N1_en_Wither.pdf. Accessed 7 Dec. 2024.