Committee: Disarmament and International Security (GA1)

Issue: Hybrid Warfare: The future of war

Student Officer: Nefeli Papadimitriou

Position: Deputy President

PERSONAL INTRODUCTION

Dear delegates,

My name is Nefeli Papadimitriou, I am sixteen years old and in the eleventh grade at Arsakeio Psychikou. It is an honour for me to be serving as Deputy President of the DISEC committee in this year's ATSMUN.

Whether you may be an experienced delegate or a newcomer, I would like to personally welcome you to our committee. Having participated in many conferences over the past two years, I can assure you that each conference presents the perfect opportunity to enhance your public speaking skills and increase your knowledge in international affairs, while meeting captivating individuals. Having been a first-timer myself, I understand that MUN can sometimes be overwhelming and challenging, however I encourage you all to entertain speeches and voice your country's opinions and I will, of course, be there to answer any questions you may have.

Prior to our meeting in the conference, you are more than encouraged to carry out research of your own, regarding your country's interests and specific research on our committee's topics. This study guide is meant to act as a foundation for your work and should not be your only means of preparation. Should you have any questions about this guide, or about the conference and procedures, do not hesitate to reach out via email: marnef.pap@gmail.com .

Looking forward to meeting and collaborating with you,

Nefeli.

INTRODUCTION

As our societies evolve and technology progresses, so do war tactics. Hybrid warfare is a combination of traditional warfare, such as military action and espionage, with a wide range of unconventional tactics, for example irregular warfare, propaganda, political interference, economic blockades and cyberattacks, in order to achieve strategic objectives. Given its broadness, there is no universally accepted definition of "hybrid warfare"[1]. Nevertheless, all agree that it is the future of war, since it provides tactics that allow any nation or group to potentially strongarm adversaries that are superior in traditional warfare alone. This advantage in the offensive poses a challenge when defending against hybrid warfare, hence cooperation is required to adequately respond to hybrid operations or try and prevent them, if possible.

The term "hybrid warfare" itself is rather new, since it appeared in prominent political studies in the first years of the 21st century. [2,3] However, this type of warfare may be dated back at least 3000 years, to the Peloponnesian War (431-404 BC) between Athens and Sparta in Greece. Nevertheless, it is the proliferation of digital technologies over the last 50 years that has enriched its range of tactics and has increased its effectiveness, over traditional warfare alone. Its lack of clear definition has also blurred the lines between war and peace. Therefore, hybrid warfare poses a multifaceted threat to the global security landscape, as the enforcement of traditional defence doctrines becomes increasingly difficult.

This also makes the work of the UN and other international organisations more complex. Within the UN, the GA1 DISEC committee and the Security Council are normally responsible for tackling global security risks and issues, but the nature of

---

[1] *""Hybrid warfare." Wikipedia, http://en.wikipedia.org/wiki/Hybrid_warfare . Accessed 1 July 2023.*

[2] Mattis, James N., and Frank Hoffman. "Future Warfare: The Rise of Hybrid Wars | Proceedings - November 2005 Vol. 131/11/1,233." *U.S. Naval Institute*, https://www.usni.org/magazines/proceedings/2005/november/future-warfare-rise-hybrid-wars . Accessed 2 July 2023.

[3] Hoffman, Frank (2007). Conflict in the 21st Century: The Rise of Hybrid Wars (PDF). Arlington, Virginia: Potomac Institute for Policy Studies. https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf

hybrid warfare makes it difficult to even be able to classify an incident as a hybrid assault. For example, how can a nation ask its allies for assistance when its aggressor employs solely unconventional war tactics? How can an international organisation intervene when war is not declared and no traditional warfare takes place in the field?

DEFINITION OF KEY TERMS

Hybrid Warfare

The concurrent use of traditional warfare and unconventional tactics, with the goal of undermining the adversary's defence forces and exploiting possible weak links in his organisation. This military tactic essentially creates a 'grey zone' where the lines between war and peace are blurred, via irregular warfare, propaganda, cyber-attacks, political pressure, economic blockades and other measures to further confuse the adversary as to what may be considered an act of war. Sometimes hybrid attacks go undetected by the targeted state or non-state, especially when traditional warfare is not occurring.[4]

Traditional Warfare

State-on-state conflict between organised and well-defined actors whose primary concern is to issue assaults on the adversary's military forces with the aim of gaining and holding ground. The use of espionage may be considered part of traditional warfare.[5]

Irregular Warfare

Violent struggle among state and nonstate actors (armed groups acting as state proxies) for legitimacy and influence over the relevant populations. Due to military asymmetry and the political nature of the struggle, the use of force mostly takes

[4] Bilal, Arsalan. "Hybrid Warfare – New Threats, Complexity, and 'trust' as the Antidote." NATO Review, 30 Nov. 2021, www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html.

[5] Fabian, Sandor. "Irregular Versus Conventional Warfare: A Dichotomous Misconception - Modern War Institute." West Point, 14 May 2021, http://mwi.usma.edu/irregular-versus-conventional-warfare-a-dichotomous-misconception . Accessed 2 July 2023.

unconventional or unorthodox forms (terrorism, counter-terrorism, drone attacks etc.).[6]

Propaganda

The alteration and manipulation of information (facts, rumours, lies, half-truth) to influence public opinion and of the opponent's fighting forces at the time of traditional warfare.[7]

Cyber-Attack

An attack via cyberspace, through the use of a computer network with the goal of disrupting, altering, removing information, or to steal confidential intelligence, or to destroy the integrity of the data stored in a specific computer or network. [8]

Political interference

The attempt to gain partisan or regional advantage by shaping the production of a statistical product against the judgement of a non-partisan and apolitical statistical agent.[9] For example, governments in some countries force utilities to hire more workers than they need, perhaps to provide patronage or in the belief that this creates jobs.[10]

Guerilla warfare

---

[6] Ucko, David H., and Thomas A. Marks. "Redefining Irregular Warfare: Legitimacy, Coercion, and Power - Modern War Institute." Modern War Institute -, 18 October 2022, https://mwi.westpoint.edu/redefining-irregular-warfare-legitimacy-coercion-and-power/ . Accessed 21 July 2023.

[7] "Propaganda." Encyclopædia Britannica, 18 May 2023, www.britannica.com/topic/propaganda.

[8] Editor, CSRC Content. "Cyber Attack - Glossary | CSRC." NIST Computer Security Resource Center, http://csrc.nist.gov/glossary/term/Cyber_Attack . Accessed 2 July 2023

[9] Political Interference in Statistics - European Parliament, http://www.europarl.europa.eu/cmsdata/163746/Prevost.pdf Accessed 2 July 2023.

[10] "Addressing Improper Political Interference – How Can Persons Performing Regulatory Functions or Developing Regulatory Instruments Protect Their Work from Improper Political Interference While, at the Same Time, Maintaining Accountability to the Political Wishes of the Population?" Https://Regulationbodyofknowledge.Org, regulationbodyofknowledge.org/faq/low-income-fragile-and-low-capacity-countries/how-can-persons-performing-regulatory-functions-or-developing-regulatory-instruments-protect-their-work-from-improper-political-interference-while-at-the-same-time-maintaining-accountability-to-the/. Accessed 2 July 2023.

A type of warfare executed by fast-moving groups of people in small-scale attacks in a region controlled by a regular, steady force.[11]

Coup d'état

The sudden and possibly violent overthrow of an existing government body by a small rogue group.[12]

Espionage

The practice of spying or using spies to obtain information about the plans and activities especially of a foreign government or an adversary's army.[13]

Economic Blockade

An embargo on trade with a country or region, intended to damage or dislodge the government.[14]

Disinformation

Deliberately false information whose intention is to mislead – a tactic that may be used as part of hybrid warfare. Not to be confused with misinformation, which is unintentionally false or inaccurate information.[15]

---

[11] "Guerrilla warfare Definition & Meaning." Dictionary.com, https://www.dictionary.com/browse/guerrilla-warfare . Accessed 7 August 2023.

[12] "Coup d'etat | Definition, Examples, & Facts." Britannica, https://www.britannica.com/topic/coup-detat . Accessed 7 August 2023.

[13] "Espionage Definition & Meaning." Merriam-Webster, www.merriam-webster.com/dictionary/espionage . Accessed 2 July 2023.

[14] "Economic Blockade Definition and Meaning: Collins English Dictionary." Economic Blockade Definition and Meaning | Collins English Dictionary, www.collinsdictionary.com/dictionary/english/economic-blockade . Accessed 2 July 2023.

[15] "Misinformation and Disinformation." American Psychological Association, www.apa.org/topics/journalism-facts/misinformation-disinformation . Accessed 2 July 2023.

BACKGROUND INFORMATION

Historical background

The phenomenon of war is as old as mankind itself. And as man evolved, so did war tactics. One should possibly consider the Peloponnesian War (431-404 BC) between Athens and Sparta in Ancient Greece as the first historical example of hybrid warfare.[16] The reason is that both adversaries formed coalitions and employed a combination of traditional warfare, economic blockades and political interference. Historically, elements of hybrid warfare could also be found in the Byzantine era (330 – 1453 AC)[17], where the Byzantines formed alliances, such are treaties and arranged marriages, performed naval blockades and maritime raids, used propaganda, irregular warfare (proxy forces, militias, allied tribes) and political interference, as subversion and rebellions. Similar examples of hybrid warfare may be found in the American Revolutionary War (1775 – 1783)[18], in which the revolutionaries employed irregular warfare, while both parties embarked on propaganda. Irregular warfare was employed by guerrilla groups, which can be defined as unofficial military groups attempting to alter the regime via sudden attacks on official military forces.[19]

However, one must reach the 20th century for hybrid warfare to become a norm during wartime. The first broad use of hybrid warfare was during the Second World War (1939-1945), where, besides traditional warfare and espionage, irregular warfare, for instance guerilla groups performing sabotage and propaganda, was greatly used usually by resistance groups against the occupation forces. Also, espionage and intelligence gathering took a sharp turn, with the creation of the early

[16]Cartwright, Mark, and Nicholas Sekunda. "Peloponnesian War." *World History Encyclopedia*, https://www.worldhistory.org/Peloponnesian_War/ . Accessed 2 July 2023.
[17]Cartwright, Mark, and Lars Brownworth. "Byzantine Empire." *World History Encyclopedia*, 19 September 2018, https://www.worldhistory.org/Byzantine_Empire/ . Accessed 2 July 2023.
[18]Shy, John W., and Joseph J. Ellis. "American Revolutionary War." *Wikipedia*, https://en.wikipedia.org/wiki/American_Revolutionary_War . Accessed 3 July 2023.
[19] "GUERRILLA | English meaning - Cambridge Dictionary." *Cambridge Dictionary*, https://dictionary.cambridge.org/dictionary/english/guerrilla . Accessed 21 July 2023.

computer by the British to decipher the Enigma-encoded messages for German military operations[20].

Following the Second World War, the Cold War era between the US and the Soviet Union occurred from 1945 to 1991, where hybrid warfare was the norm given that direct traditional warfare was avoided. [21] This included extensive propaganda, proxy wars that also happened in Korea, Vietnam, Afghanistan and various localised wars in Africa and Latin America during that time period, economic blockades as the one in Cuba, political interference as the Soviet invasions in Hungary in 1956 and Prague 1968 and US-led coup d'états in various countries around the world, and at its end, the first cyber warfare incidents with the not-so-advanced technology of that time. For example, in 1950 North Korea, which was supported by the Soviet Union and China, invaded South Korea in order to reunite the whole of Korea under a communist regime. This triggered the intervention of the USA and its allies to support South Korea in order to stop communist expansion.

The 20th century ends with the Post Cold War era, when the demise of the Soviet Union led to multiple localised conflicts in Europe, as in the Balkans, but also Chechnya and Nagorno-Karabakh, where traditional warfare was combined with irregular warfare, propaganda as well as extensive political interference[22].

Hybrid warfare in the 21st century

The turn of the 21st century was marked by the 9/11 attacks in the US in 2001[23], which marked a shift in traditional warfare from a nation-to-nation battle to a battle of a nation against an extremist group that transcends national borders. It also redefined the term of asymmetric, also known as irregular, warfare, since airline hijackings and suicide attacks committed by just 19 militants exerted a huge blow to

---

[20] "Enigma machine." Wikipedia, https://en.wikipedia.org/wiki/Enigma_machine . Accessed 3 July 2023.

[21] "Cold War." Wikipedia, https://en.wikipedia.org/wiki/Cold_War . Accessed 3 July 2023.

[22] "Key points about 1990s Balkan wars - JusticeInfo.net." Justice Info, 22 March 2016, https://www.justiceinfo.net/en/26457-key-points-about-1990s-balkan-wars.html . Accessed 3 July 2023.

[23] History.com editors. "September 11 Attacks." September 11 Attacks: Facts, Background & Impact | HISTORY, https://www.history.com/topics/21st-century/9-11-attacks . Accessed 15 July 2023.

a superpower like the USA.[24] Since then, irregular warfare with the inclusion of military drone attacks and mostly cyber warfare have taken the lead in hybrid warfare, due to the development of the related technology.

The first example of a cyber weapon was the Stuxnet worm, which was discovered on systems in Iran in 2010; however, it is believed that it was released as early as 2005. [25] The Stuxnet worm was possibly developed jointly by the USA and Israel, targeting Iran's nuclear program. Since then, various forms of cyber warfare have been noted that can be broadly categorised into: a) advanced persistent threats,[26] for example, long-term cyber-espionage efforts launched by states, as the Operation Olympic Games in 2010-2012,[27] a joint US-Israeli effort targeting Iran's nuclear program, b) cyber-attacks, such as short-term attacks sponsored by states, like the Russian attacks on Georgia in 2008 and Ukraine since 2014,[28] the Chinese campaign APT1 in 2013[29] against the USA and its allies and the North-Korean attack on Sony Pictures in 2014.[30]

[24]"Asymmetric Warfare | RAND." RAND Corporation, https://www.rand.org/topics/asymmetric-warfare.html . Accessed 3 July 2023

[25] "Stuxnet." Wikipedia, https://en.wikipedia.org/wiki/Stuxnet . Accessed 3 July 2023.

[26]"Advanced persistent threat." Wikipedia, https://en.wikipedia.org/wiki/Advanced_persistent_threat . Accessed 3 July 2023.

[27] "Operation Olympic Games." Wikipedia, https://en.wikipedia.org/wiki/Operation_Olympic_Games . Accessed 3 July 2023

[28] "What the Russian Invasion Reveals About the Future of Cyber Warfare." Carnegie Endowment for International Peace, 19 December 2022, https://carnegieendowment.org/2022/12/19what-russian-invasion-reveals-about-future-of-cyber-warfare-pub-88667 . Accessed 3 July 2023.

[29] "APT1: Exposing One of China's Cyber Espionage Units." Homeland Security Digital Library, 19 February 2013, https://www.hsdl.org/c/apt1-exposing-one-of-chinas-cyber-espionage-units/ . Accessed 3 July 2023.

[30]"The 2014 Sony hacks, explained." Vox, 3 June 2015, https://www.vox.com/2015/1/20/18089084/sony-hack-north-korea . Accessed 3 July 2023

Figure 1: Metaphor on hybrid warfare[31]

Hybrid warfare and the rule of law

As mentioned in the introduction, there is no universally accepted definition of the term "hybrid warfare".[1] Its broadness has also blurred the lines between war and peace, since nowadays a nation or a group could employ solely unconventional war tactics without any traditional warfare. Obviously, this tactic cannot win a war, but can severely undermine the target's infrastructure or ability to defend, which may be equivalent to or a precursor of traditional warfare. This "blurred" definition has also impeded international organisations from clearly defining a hybrid attack as an act of war or leaving the hybrid warfare in a legal grey area. For example, in 2018, the Council of Europe in its Resolution 2217[32] states that in case of a hybrid war, a state uses physical force against another one, the latter is permitted to invoke, based on Article 51 of the Charter of the United Nations, the basic humanitarian right of self-defence[33]. This kind of legal blurriness impedes international organisations from developing their doctrines to fully consider hybrid warfare as acts of war. However, there have been some moves towards this direction, as the NATO council communique after the Warsaw 2016 summit, which first mentions countering hybrid

---

31 "Sakharov Conference on Trolls, Disinformation and Hybrid Warfare." *VDU*, 14 May 2019, https://www.vdu.lt/en/sakharov-conference-on-trolls-disinformation-and-hybrid-warfare/ . Accessed 16 July 2023.

32 "Legal challenges related to hybrid war and human rights obligations", Resolution 2217 (2018), Council of Europe. https://pace.coe.int/pdf/5bc36f80a3d8fd42b21f66f8fae0396fabc6b3f7ed2dcff4afb86217e9e8eabd/res.%202217.pdf Accessed 21 July 2023.

33 "United Nations Charter (full text) | United Nations." *the United Nations*, https://www.un.org/en/about-us/un-charter/full-text . Accessed 7 August 2023.

warfare as part of collective defence, via invoking Article 5 of the NATO Treaty, thus upscaling hybrid warfare to crossing the threshold of an armed attack[34].

MAJOR COUNTRIES AND ORGANISATIONS INVOLVED

China

It has been said that the tactic of hybrid warfare was firstly theorised in Unrestricted Warfare[35] (1999), a book written by Chinese military strategists Qiao Liang and Wang Xiangsui. In current times, China has been expanding influence in the Middle East, via a cooperation agreement with Iran that endorses military cooperation and intelligence sharing. In 2019, China was accused of making an attempt at 'guerrilla war at sea', when the Philippine army detected 275 ships near Thitu Island[36]. The ships were said to be equipped with Chinese satellite navigation systems that enabled them to collect intelligence, track and transfer locations and send the aforementioned information to numerous addresses. Regardless, all allegations were denied by China[37]. Therefore, China was the first to theorise the concept of hybrid warfare and is also active upon the issue.

Democratic People's Republic of Korea (DPRK)

An important part of North Korea's external policy is to ensure the world is aware that their arsenal of nuclear weapons is enough to wage nuclear war at any given moment[38]. In 2017, for example, North Korea declared the achievement of both

[34] "Warsaw Summit Communiqué issued by NATO Heads of State and Government (2016)." NATO.int, 1 July 2022, https://www.nato.int/cps/en/natohq/official_texts_133169.htm . Accessed 7 August 2023.

[35] Liang, Qiao and Xiangsui, Wang. "Unrestricted Warfare", People's Liberation Army Literature and Arts Publishing House (解放军文艺出版社), February 1999

[36] "Timeline: China's Maritime Disputes." Council on Foreign Relations, https://www.cfr.org/timeline/chinas-maritime-disputes . Accessed 21 July 2023.

[37] Kraska, James, and Michael Monti. "ANALYSIS - Hybrid warfare and maritime militia in China." Anadolu Agency, 2 July 2020, https://www.aa.com.tr/en/analysis/analysis-hybrid-warfare-and-maritime-militia-in-china/1897259 . Accessed 11 July 2023.

[38] Kahn, Herman, and Patrick M. Cronin. "North Korea's Hybrid and Nuclear Warfare Challenge." Hudson Institute, 22 October 2022, https://www.hudson.org/arms-control-nonproliferation/north-korea-hybrid-nuclear-warfare-challenge-patrick-cronin . Accessed 10 July 2023

an intercontinental ballistic missile and hydrogen bomb capacity. North Korea has also been accused of cyber-attacks, including the Sony Pictures Hack in 2014, which compromised important data. [39] Consequently, North Korea is very active on the issue of hybrid warfare and possibly has the nuclear weapons necessary to execute certain threats.

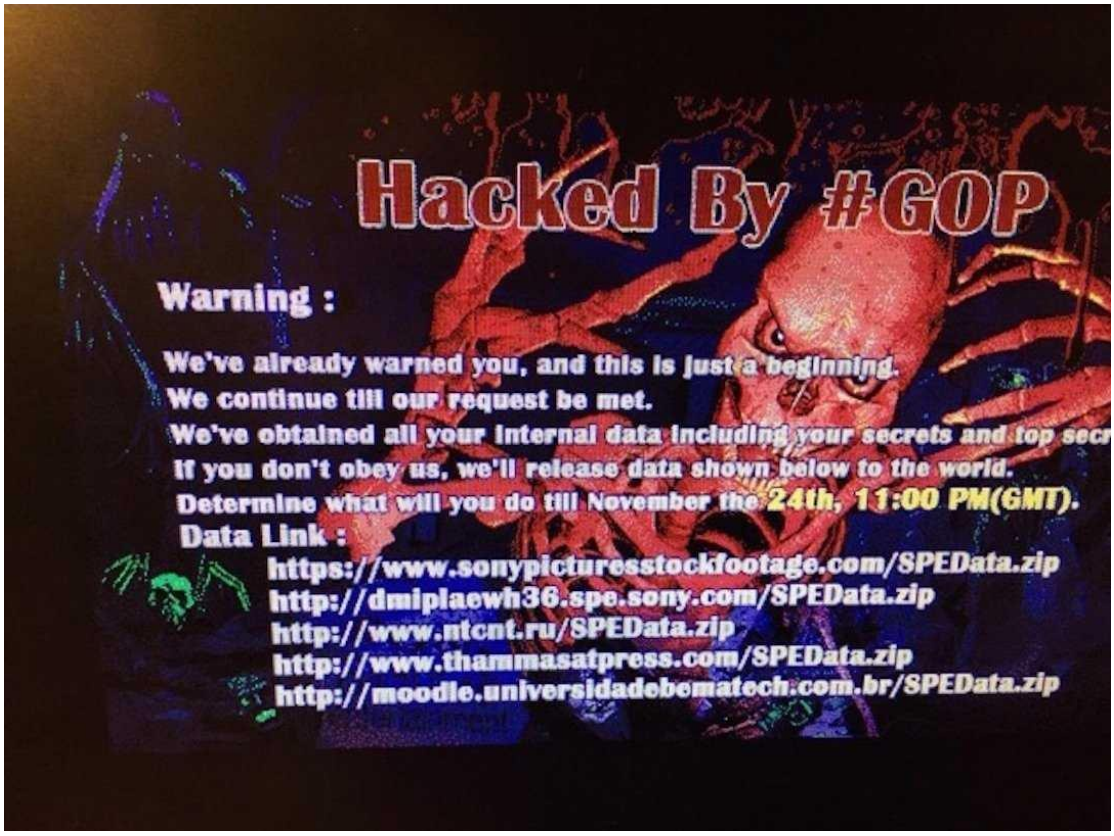

Figure 2: The picture Sony employees saw on their screens the morning of the North Korean attack on Sony Pictures in 2014[40]

Iran

Iran applies hybrid warfare in the Middle East, primarily targeting energy companies with the aim of disrupting the power balance. Iran has been trying to gain influence in the Middle East, via signing cooperation agreements with both the Russian Federation in January 2021 and China in March of the same year. In May 2019, more than half of the oil production facilities of Saudi Arabia were taken offline for

[39] "The 2014 Sony hacks, explained." Vox, 3 June 2015, https://www.vox.com/2015/1/20/18089084/sony-hack-north-korea . Accessed 15 July 2023.
[40] "The 2014 Sony hacks, explained." Vox, 3 June 2015, https://www.vox.com/2015/1/20/18089084/sony-hack-north-korea . Accessed 16 July 2023.

weeks, due to drone attacks against the central production facility in the country. Iranian proxies, Yemen's Houthi rebels, supported by Iran, attacked with ballistic missiles and drones bearing explosives the Ras Tanura port, a Saudi Arabian oil port.

Additionally, Iranian drones pose an important hybrid threat, as the technology has been sent to Iraq, Yemen and Syria. This, along with the extremely hostile Iranian policy against Israel, render the situation of Iran versus Israel quite critical as the threat is proved to be real.[41] Iran's potential as a hybrid threat is great, since it possesses the infrastructure needed and nothing has yet been done to decrease the threat level.

Russian Federation

The Kremlin considers hybrid warfare to be a type of war; a definition more precise than other countries' where it may be thought of as a policy. In fact, the conflicts with Ukraine, Syria, Libya and Venezuela are classified as hybrid wars, according to the Russian government. Furthermore, Russian Military Forces support that hybrid warfare will replace traditional and conventional warfare as the future of war. Because of this belief, Russia is currently adapting military systems and doctrines in order to be able to enforce hybrid warfare as the centre of operations.

A first example of Russian hybrid war is the 2008 attack on Georgia, while another example is the operation in Crimea in 2014, which was conducted by 'little green men', a group of Russian soldiers.[42] The Russian invasion in Ukraine in 24th February 2022 has also been classified as a 'special operation' by the Russian president Vladimir Putin, though certain targeted infrastructure attacks could be attributed to a 'terror campaign' on civilians.[43] Russia's belief that hybrid warfare is

[41] Momi, Rachele. "The Iranian Hybrid Warfare Operations in the Middle East." Grey Dynamics, 26 October 2021, https://greydynamics.com/the-iranian-hybrid-warfare-operations-in-the-middle-east/ . Accessed 10 July 2023.
[42] "Russian Hybrid Warfare." Institute for the Study of War, https://www.understandingwar.org/report/russian-hybrid-warfare . Accessed 11 July 2023.
[43] Baker, Michael S., et al. "Russia's Hybrid Warfare in Ukraine Threatens Both Healthcare & Health Protections Provided by International Law." NCBI, 23 January 2023, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9881440/ . Accessed 11 July 2023

indeed the future of war renders it a considerable threat in the matter of hybrid operations.

Figure 3: "New Eastern Europe" magazine 2020 issue on Russia's war in Georgia in 2008.[44]

United States

The US is currently suspended in a competition among themselves, Russia and China regarding the subject of military advancement and strategic tactics. In fact, some US allies have expressed concern that the US has not responded effectively to past hybrid attacks. Officially, the US claims not to apply hybrid warfare, nonetheless the technological infrastructure and capabilities necessary definitely exist. Regardless of the official statements, several of their known operations and organisations such as surveillance operations, the NSA, the CIA and the FBI suggest otherwise.[45]

European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE)

[44] "Issue 4/2020 The Kremlin's Hybrid War. The case of Georgia." New Eastern Europe, 8 July 2020, https://neweasterneurope.eu/2020/07/08/issue-4-2020-the-kremlins-hybrid-war-the-case-of-georgia/ . Accessed 16 July 2023.

[45] Polymeropoulos M, Iyer A.. "US Adversaries Have Been Mastering Hybrid Warfare. It's Time to Catch Up." Atlantic Council, 23 Feb. 2022, www.atlanticcouncil.org/blogs/new-atlanticist/us-adversaries-have-been-mastering-hybrid-warfare-its-time-to-catch-up/?mkt_tok=NjU5LVdaWC0wNzUAAAGCf81vtizCHdTDKbFDPUl2eD9L3mmHxzTnTn5264GHUxtuScOsuv-UhcjURT0YZVmnBUxKB3cbZJRcYeima3j4CM6ndPYDkzM_eRy-DDZd . Accessed July 15 2023.

The Hybrid CoE was founded in 2017 in Helsinki by the first nine participating states being Finland, Sweden, UK, Latvia, Lithuania, Poland, France, Germany and the USA, NATO and the EU. The Hybrid CoE analyses and studies various hybrid warfare strategies, explores the capabilities of new technologies and their potential uses in a hybrid context and forms ways of countering and responding to hybrid threats[46]. These attempts are solely focused on studying hybrid warfare and developing anti-hybrid techniques.

North Atlantic Treaty Organisation (NATO)

Since 2016, NATO declared that any hybrid threats made against any member state could be reason enough to invoke Article 5 of the North Atlantic Treaty[47]. Article 5 essentially states that any armed attack against one Member will be considered an armed attack against all Members and, if necessary, will provide assistance to the direct victim of the aforementioned act of violence. In 2018, it was decided to form counter-hybrid teams that will act to assist any Ally facing a hybrid warfare attack, should they request it. Furthermore, experts have been analysing the hybrid strategies used by the Russian Federation and China[48]. Regardless, since there is no solid anti-hybrid defence mechanism yet, all of these efforts could be characterised as a work-in-progress.

TIMELINE OF EVENTS

Date	Description of event
431-404 B.C.	The Peloponnesian war between Athens and Sparta in Ancient Greece, where both adversaries formed coalitions and employed a combination of traditional warfare, economic blockades and political interference.

[46]"COI Strategy and Defence." Hybrid CoE, https://www.hybridcoe.fi/coi-strategy-and-defence/ . Accessed 12 July 2023.
[47]"Topic: Collective defence and Article 5." NATO, https://www.nato.int/cps/en/natohq/topics_110496.htm . Accessed 12 July 2023.
[48]"Topic: Countering hybrid threats." NATO, https://www.nato.int/cps/en/natohq/topics_156338.htm . Accessed 12 July 2023.

1775-1783	The American Revolutionary War, where the revolutionaries employed irregular warfare (guerilla groups), while both parties embarked on propaganda.
1939-1945	The Second World War, where, besides traditional warfare, irregular warfare and propaganda were greatly used.
1946-1991	The Cold War between the USA and the Soviet Union and their respective allies, when without traditional warfare, espionage, proxy conflicts (Korea, Vietnam, Afghanistan), irregular warfare, propaganda (the one against the other) were extensively used.
1991-today	The Post Cold War era in Europe, where the demise of the Soviet Union led to multiple localised conflicts in the Balkans, but also Chechnya, Nagorno-Karabakh, etc., where traditional warfare was combined with irregular warfare (ethnic guerilla groups), propaganda (fake news of massacres, etc.).
February 1999	Chinese war strategists Qiao Liang and Wang Xiangsui publish "Unrestricted Warfare", theorising the concept of hybrid warfare and supporting their belief that it is the future of war.
11 September 2001	The series of airline hijackings and suicide attacks committed by 19 militants associated with the Islamic extremist group al-Qaeda against targets in the United States (Word Trade Center, Pentagon, etc.) changed the doctrine of US foreign policy to officially include hybrid warfare.
November 2005	The term "hybrid warfare" first appears in US Naval documents.[49]
December 2007	"Hybrid wars" are defined as the form of war in the 21st Century by Frank Hoffman.[50]

[49] Mattis, Lieutenant General James N., and Lieutenant Colonel Frank Hoffman. "Future Warfare: The Rise of Hybrid Wars." U.S. Naval Institute, 4 Sept. 2019, www.usni.org/magazines/proceedings/2005/november/future-warfare-rise-hybrid-wars.

[50] *Conflict in the 21st Century - Potomac Institute, www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf . Accessed 2 July 2023.*

June 2010	Discovery of the Stuxnet worm, possibly the first cyber weapon, possibly developed jointly by USA and Israel, targeting Iran's nuclear program.
2011-today	The Syrian Civil War, which involves a complex combination of traditional warfare, irregular warfare (proxy forces), political interference, cyberattacks and propaganda, by many counter-acting nations and groups.
2014-today	Russia's involvement with Ukraine, which includes besides traditional warfare (in Crimea in 2014, and Eastern Ukraine since 2022), propaganda, cyber-attacks, and political interference (support for separatist groups, pressure for referendum voting).
8-9 July 2016	NATO council communique after Warsaw summit[51] first mentions countering hybrid warfare as part of collective defence (via invoking Article 5 of the NATO Treaty), thus upscaling hybrid warfare to crossing the threshold of an armed attack[52].
15 December 2016	Security Council Resolution 2325 is formed. It is possibly the first resolution that examines terrorism from the angle of cyber-attacks and cybersecurity, as well as referencing the malevolent use of new technologies, connecting it with hybrid warfare.
26 April 2018	Resolution 2217 of the Council of Europe deals with legal challenges related to hybrid war and human rights obligations.[53]

PREVIOUS ATTEMPTS TO SOLVE THE ISSUE

UNSC Resolutions on the issue of cyber-attacks, terrorism and the use of technology

[51] Nato. "Warsaw Summit Communiqué Issued by NATO Heads of State and Government (2016)." NATO, www.nato.int/cps/en/natohq/official_texts_133169.htm . Accessed 2 July 2023.

[52] Aurel Sari and Arnis Lauva, et al. "Hybrid Threats and the United States National Security Strategy: Prevailing in an 'Arena of Continuous Competition.'" EJIL, 18 Jan. 2018, www.ejiltalk.org/hybrid-threats-and-the-united-states-national-security-strategy-prevailing-in-an-arena-of-continuous-competition/ .

[53] "Legal challenges related to hybrid war and human rights obligations", Resolution 2217 (2018), Council of Europe. https://pace.coe.int/pdf/5bc36f80a3d8fd42b21f66f8fae0396fabc6b3f7ed2dcff4afb86217e9e8eabd/res.%202217.pdf Accessed 21 July 2023.

Although there is no resolution or doctrine solely dedicated to and explicitly concerning hybrid warfare, the Security Council has made attempts to resolve and counter the financing of terrorist groups with Security Council Resolution 2325 (2016)[54] and to develop strategies to prevent and counter terrorism-generated cyber-attacks and propaganda. With Security Council Resolution 2354 (2017)[55], the use of new technologies for harmful purposes is tackled, another element of hybrid warfare. Notably, these resolutions do not explicitly mention hybrid warfare, but tackle some of its branches instead.

NATO's Readiness Action Plan

In 2014, NATO adopted the Readiness Action Plan, also known by the initials RAP. [56] The RAP focuses on ameliorating the alliance's readiness and response to threats, including but not limited to hybrid threats, even though they are not mentioned explicitly. Furthermore, NATO is closely collaborating with the EU and the European Centre of Excellence for countering hybrid threats. The NATO-EU collaboration also consists of conducting exercises to react to cyber-attacks.[57] The RAP is a great way to enhance collaboration and relations between member-states, a unity that could prove useful in the face of a hybrid attack.

European Centre of Excellence for Countering Hybrid Threats- Hybrid CoE

Via the Hybrid 101 Course, a training course for member-states of the EU and NATO, the Hybrid CoE attempts to increase participating states' understanding of hybrid threats through lectures, videographic material, case studies and, finally, a dilemma game to test their abilities and comprehension. In close collaboration with the EU, the Hybrid CoE provides support to better respond to and prevent hybrid

[54] "Security Council Adopts Resolution 2325 (2016), Calling for Framework to Keep Terrorists, Other Non-State Actors from Acquiring Weapons of Mass Destruction | UN Press." *UN Press*, 15 December 2016, https://press.un.org/en/2016/sc12628.doc.htm . Accessed 12 July 2023.
[55] "Countering violent extremism and terrorist narratives | Security Council - Counter-Terrorism Committee (CTC)." *the United Nations*, https://www.un.org/securitycouncil/ctc/content/countering-violent-extremism-and-terrorist-narratives . Accessed 12 July 2023.
[56] "Topic: Readiness Action Plan." *NATO*, 1 September 2022, https://www.nato.int/cps/en/natohq/topics_119353.htm . Accessed 14 July 2023.
[57] "NATO and EU discuss defence against hybrid warfare." *NATO*, 15 March 2019, https://www.nato.int/cps/en/natohq/news_164603.htm?selectedLocale=en . Accessed 14 July 2023.

warfare, specifically working with the Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats. In close collaboration with NATO, Hybrid CoE provides hybrid advisors for exercises and wargames, as well as works with NATO-related centres of excellence that are trying to tackle the same problem.[58] The Hybrid CoE is certainly effective regarding preparing and educating about hybrid attacks, as raising awareness is equally important to organising defence mechanisms.

Figure 4: The European Centre of Excellence for countering hybrid threats is neither an EU nor a NATO body, but a freestanding legal entity.[59]

OSCE's cybersecurity efforts and reestablishment attempts.

The OSCE has been making steady steps to ensure cybersecurity and transparent contact among member-states, thus helping to secure nations from cyber-attacks.[60] The organisation is engaged in conflict prevention and resolution, via providing meditational aid and dialogue facilitation between previously conflict-struck states and communities[61]. The OSCE also carries out monitoring missions and offers support to states and communities suffering the effects of hybrid attacks, such

[58] "Training and exercises." Hybrid CoE, https://www.hybridcoe.fi/training-and-exercise/ . Accessed 14 July 2023.
[59] Hagelstam, Axel. "NATO Review - Cooperating to counter hybrid threats." NATO.int, 23 November 2018, https://www.nato.int/docu/review/articles/2018/11/23/cooperating-to-counter-hybrid-threats/index.html . Accessed 16 July 2023.
[60] "Confidence building measures to enhance cybersecurity in focus at OSCE meeting in Vienna." OSCE, 7 November 2014, https://www.osce.org/cio/126475 Accessed 15 July 2023.
[61] "Conflict prevention and resolution." OSCE, https://www.osce.org/conflict-prevention-and-resolution . Accessed 15 July 2023.

as Ukraine.[62] Plotting anti-cyber-attack strategies goes a long way towards combating hybrid warfare and reestablishment attempts help reconstruct unity and prevent future hybrid attacks.

POSSIBLE SOLUTIONS

Develop legal frameworks and norms to explicitly address hybrid warfare

Firstly, hybrid warfare should be given an explicit definition that is acceptable in international fora. More generally, legal frameworks and norms are required to be developed or updated, which will include regulations on cyber operations, disinformation and unconventional warfare, regardless of whether these are employed by states or non-state actors. Any procured international agreements should be internationally ratified, as the 2017 Tallinn Manual that provides guidance on the application of international law to cyber operations. [63] Such legal frameworks will secure accountability of hybrid assailants, as a deterrent of such tactics in the future.

Enhance international cooperation to counter hybrid warfare

No country can address hybrid warfare on its own. Hence, international cooperation among member states via multilateral agreements, regional alliances or international organisations should be enhanced. This includes sharing information, intelligence and best practices in addressing hybrid attacks, but also implementing early warning systems, real-time threat assessments and joint response mechanisms. One such example is the agreement between the EU and NATO to enhance their cooperation for countering hybrid threats. Such international cooperations are expected to act as deterrents for hybrid warfare in the future.

[62] "OSCE Special Monitoring Mission to Ukraine (closed)." OSCE, https://www.osce.org/special-monitoring-mission-to-ukraine-closed . Accessed 15 July 2023.
[63] Schmitt, Michael N., editor. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press, 2017. Accessed 15 July 2023.

Advance infrastructure resilience and raise public awareness regarding hybrid threats

Design and maintenance of infrastructure may not have been updated to address hybrid tactics. Therefore, it is important to enhance the resilience of (at least critical) infrastructure to withstand and recover from hybrid threats, for example cyber-attacks in energy grids, transportation networks and communication systems, which entails investing in cybersecurity measures or in defence against unconventional attacks such as drone attacks. Concurrently, public awareness campaigns need to be implemented, focusing on countering disinformation on promoting media/digital literacy. It is important that the public becomes educated on hybrid threats, their impact and on how to identify them. Such actions will help as deterrents of hybrid assailants, but will also help mitigate the consequences of hybrid attacks on society.

Re-invent defence strategies

New defence strategies should consider the multidimensional nature of hybrid threats. Thus, they should combine state-of-the-art conventional military capabilities with robust cyber-defence, advanced intelligence gathering and counter-propaganda mechanisms, such as fact-checking and accurate information dissemination. The defence strategies that deal with unconventional war tactics require investment in research and development of advanced technologies, such as Artificial Intelligence (AI) and machine learning, aiming at detecting and countering hybrid threats more effectively. One such example is the introduction of hybrid threats in the 2017 National Security Strategy of the USA.[64] Similar strategies have been issued by other NATO countries, too. However, fully effective defence against hybrid threats can only be achieved via international cooperation.

[64] National Security Forum, 13 June 2023, https://nationalsecurityforum.org/wp-content/uploads/2018/01/NSS-Final-12-18-2017-0905-2.pdf . Accessed 15 July 2023.

Promote technology transfer from private sector and towards developing countries to aid in their hybrid war defence

Big tech companies are generally pioneers in the advancement of the technology employed in hybrid warfare. Hence, fostering partnerships between governments and the private sector will aid in addressing hybrid warfare more effectively. More importantly, the technological gap between developed and developing countries makes the latter much more vulnerable to hybrid attacks. Hence, providing assistance and capacity-building support to developing countries under hybrid threat, particularly in areas such as cybersecurity, intelligence gathering and countering disinformation, may act as crucial deterrents for hybrid warfare in the future.

Further Reading

- Bilal, Arsalan. "Hybrid Warfare – New Threats, Complexity, and 'trust' as the Antidote." NATO Review, 30 Nov. 2021, www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html.
- "Legal challenges related to hybrid war and human rights obligations", Resolution 2217 (2018), Council of Europe. https://pace.coe.int/pdf/5bc36f80a3d8fd42b21f66f8fae0396fabc6b3f7ed2dcff4afb86217e9e8eabd/res.%202217.pdf Accessed 21 July 2023.
- "Security Council Adopts Resolution 2325 (2016), Calling for Framework to Keep Terrorists, Other Non-State Actors from Acquiring Weapons of Mass Destruction | UN Press." UN Press, 15 December 2016, https://press.un.org/en/2016/sc12628.doc.htm . Accessed 12 July 2023.

BIBLIOGRAPHY

"Addressing Improper Political Interference – How Can Persons Performing Regulatory Functions or Developing Regulatory Instruments Protect Their Work

from Improper Political Interference While, at the Same Time, Maintaining Accountability to the Political Wishes of the Population?" https://regulationbodyofknowledge.org/faq/low-income-fragile-and-low-capacity-countries/how-can-persons-performing-regulatory-functions-or-developing-regulatory-instruments-protect-their-work-from-improper-political-interference-while-at-the-same-time-maintaining-accountability-to-the/ . Accessed 2 July 2023.

"Advanced persistent threat." Wikipedia, https://en.wikipedia.org/wiki/Advanced_persistent_threat . Accessed 3 July 2023.

"Asymmetric Warfare | RAND." RAND Corporation, https://www.rand.org/topics/asymmetric-warfare.html . Accessed 3 July 2023

Aurel Sari and Arnis Lauva, et al. "Hybrid Threats and the United States National Security Strategy: Prevailing in an 'Arena of Continuous Competition.'" EJIL, 18 Jan. 2018, www.ejiltalk.org/hybrid-threats-and-the-united-states-national-security-strategy-prevailing-in-an-arena-of-continuous-competition/ .

Baker, Michael S., et al. "Russia's Hybrid Warfare in Ukraine Threatens Both Healthcare & Health Protections Provided by International Law." NCBI, 23 January 2023, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9881440/ . Accessed 11 July 2023

Bilal, Arsalan. "Hybrid Warfare – New Threats, Complexity, and 'trust' as the Antidote." NATO Review, 30 Nov. 2021, www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html.

Cartwright, Mark, and Lars Brownworth. "Byzantine Empire." World History Encyclopedia, 19 September 2018, https://www.worldhistory.org/Byzantine_Empire/ . Accessed 2 July 2023.

Cartwright, Mark, and Nicholas Sekunda. "Peloponnesian War." World History Encyclopedia, https://www.worldhistory.org/Peloponnesian_War/ . Accessed 2 July 2023.

"COI Strategy and Defence." Hybrid CoE, https://www.hybridcoe.fi/coi-strategy-and-defence/ . Accessed 12 July 2023.

"Cold War." Wikipedia, https://en.wikipedia.org/wiki/Cold_War . Accessed 3 July 2023.

"Confidence building measures to enhance cybersecurity in focus at OSCE meeting in Vienna." OSCE, 7 November 2014, https://www.osce.org/cio/126475 Accessed 15 July 2023.

"Conflict in the 21st Century" - Potomac Institute, www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf . Accessed 2 July 2023.

"Conflict prevention and resolution." OSCE, https://www.osce.org/conflict-prevention-and-resolution . Accessed 15 July 2023.

"Countering violent extremism and terrorist narratives | Security Council - Counter-Terrorism Committee (CTC)." the United Nations, https://www.un.org/securitycouncil/ctc/content/countering-violent-extremism-and-terrorist-narratives . Accessed 12 July 2023.

"Coup d'etat | Definition, Examples, & Facts." Britannica, https://www.britannica.com/topic/coup-detat . Accessed 7 August 2023.

"CSDP structure, instruments and agencies | EEAS." EEAS, https://www.eeas.europa.eu/eeas/csdp-structure-instruments-and-agencies_en . Accessed 14 July 2023.

"Economic Blockade Definition and Meaning: Collins English Dictionary." Economic Blockade Definition and Meaning | Collins English Dictionary, www.collinsdictionary.com/dictionary/english/economic-blockade . Accessed 2 July 2023.

Editor, CSRC Content. "Cyber Attack - Glossary | CSRC." NIST Computer Security Resource Center, http://csrc.nist.gov/glossary/term/Cyber_Attack . Accessed 2 July 2023

"Enigma machine." Wikipedia, https://en.wikipedia.org/wiki/Enigma_machine . Accessed 3 July 2023.

"Espionage Definition & Meaning." Merriam-Webster, www.merriam-webster.com/dictionary/espionage . Accessed 2 July 2023.

Fabian, Sandor. "Irregular Versus Conventional Warfare: A Dichotomous

Misconception - Modern War Institute." West Point, 14 May 2021, http://mwi.usma.edu/irregular-versus-conventional-warfare-a-dichotomous-misconception . Accessed 2 July 2023.

"GUERRILLA | English meaning - Cambridge Dictionary." Cambridge Dictionary, https://dictionary.cambridge.org/dictionary/english/guerrilla . Accessed 21 July 2023.

"Guerrilla warfare Definition & Meaning." Dictionary.com, https://www.dictionary.com/browse/guerrilla-warfare . Accessed 7 August 2023.

History.com editors. "September 11 Attacks." September 11 Attacks: Facts, Background & Impact | HISTORY, https://www.history.com/topics/21st-century/9-11-attacks . Accessed 15 July 2023.

Hoffman, Frank (2007). Conflict in the 21st Century: The Rise of Hybrid Wars (PDF). Arlington, Virginia: Potomac Institute for Policy Studies. https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf

"Hybrid warfare." Wikipedia, http://en.wikipedia.org/wiki/Hybrid_warfare . Accessed 1 July 2023.

Kahn, Herman, and Patrick M. Cronin. "North Korea's Hybrid and Nuclear Warfare Challenge." Hudson Institute, 22 October 2022, https://www.hudson.org/arms-control-nonproliferation/north-korea-hybrid-nuclear-warfare-challenge-patrick-cronin . Accessed 10 July 2023

"Key points about 1990s Balkan wars - JusticeInfo.net." Justice Info, 22 March 2016, https://www.justiceinfo.net/en/26457-key-points-about-1990s-balkan-wars.html . Accessed 3 July 2023.

Kraska, James, and Michael Monti. "ANALYSIS - Hybrid warfare and maritime militia in China." Anadolu Agency, 2 July 2020, https://www.aa.com.tr/en/analysis/analysis-hybrid-warfare-and-maritime-militia-in-china/1897259 . Accessed 11 July 2023.

"Legal challenges related to hybrid war and human rights obligations",

Resolution 2217 (2018), Council of Europe. https://pace.coe.int/pdf/5bc36f80a3d8fd42b21f66f8fae0396fabc6b3f7ed2dcff4afb86217e9e8eabd/res.%202217.pdf Accessed 21 July 2023.

Liang, Qiao and Xiangsui, Wang. "Unrestricted Warfare", People's Liberation Army Literature and Arts Publishing House (解放军文艺出版社), February 1999

Mattis, James N., and Frank Hoffman. "Future Warfare: The Rise of Hybrid Wars | Proceedings - November 2005 Vol. 131/11/1,233." U.S. Naval Institute, https://www.usni.org/magazines/proceedings/2005/november/future-warfare-rise-hybrid-wars . Accessed 2 July 2023.

"Misinformation and Disinformation." American Psychological Association, www.apa.org/topics/journalism-facts/misinformation-disinformation . Accessed 2 July 2023.

Momi, Rachele. "The Iranian Hybrid Warfare Operations in the Middle East." Grey Dynamics, 26 October 2021, https://greydynamics.com/the-iranian-hybrid-warfare-operations-in-the-middle-east/ . Accessed 10 July 2023.

"National Security Forum, 13 June 2023, https://nationalsecurityforum.org/wp-content/uploads/2018/01/NSS-Final-12-18-2017-0905-2.pdf . Accessed 15 July 2023.

"NATO and EU discuss defence against hybrid warfare." NATO, 15 March 2019, https://www.nato.int/cps/en/natohq/news_164603.htm?selectedLocale=en . Accessed 14 July 2023.

NATO. "Warsaw Summit Communiqué Issued by NATO Heads of State and Government (2016)." NATO, www.nato.int/cps/en/natohq/official_texts_133169.htm . Accessed 2 July 2023.

"Operation Olympic Games." Wikipedia, https://en.wikipedia.org/wiki/Operation_Olympic_Games . Accessed 3 July 2023

"OSCE Special Monitoring Mission to Ukraine (closed)." OSCE, https://www.osce.org/special-monitoring-mission-to-ukraine-closed . Accessed 15 July 2023.

"Political Interference in Statistics - European Parliament,

http://www.europarl.europa.eu/cmsdata/163746/Prevost.pdf Accessed 2 July 2023.

Polymeropoulos M, Iyer A. "US Adversaries Have Been Mastering Hybrid Warfare. It's Time to Catch Up." Atlantic Council, 23 Feb. 2022, www.atlanticcouncil.org/blogs/new-atlanticist/us-adversaries-have-been-mastering-hybrid-warfare-its-time-to-catch-up/?mkt_tok=NjU5LVdaWC0wNzUAAAGCf81vtizCHdTDKbFDPUl2eD9L3mmHxzTnTn5264GHUxtuScOsuv-UhcjURT0YZVmnBUxKB3cbZJRcYeima3j4CM6ndPYDkzM_eRy-DDZd . Accessed July 15 2023.

"Propaganda." Encyclopædia Britannica, 18 May 2023, www.britannica.com/topic/propaganda.

"Russian Hybrid Warfare." Institute for the Study of War, https://www.understandingwar.org/report/russian-hybrid-warfare . Accessed 11 July 2023.

Schmitt, Michael N., editor. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press, 2017. Accessed 15 July 2023.

"Security Council Adopts Resolution 2325 (2016), Calling for Framework to Keep Terrorists, Other Non-State Actors from Acquiring Weapons of Mass Destruction | UN Press." UN Press, 15 December 2016, https://press.un.org/en/2016/sc12628.doc.htm . Accessed 12 July 2023.

"Security Council Adopts Resolution 2325 (2016), Calling for Framework to Keep Terrorists, Other Non-State Actors from Acquiring Weapons of Mass Destruction | UN Press." UN Press, 15 December 2016, https://press.un.org/en/2016/sc12628.doc.htm . Accessed 12 July 2023.

Shy, John W., and Joseph J. Ellis. "American Revolutionary War." Wikipedia, https://en.wikipedia.org/wiki/American_Revolutionary_War . Accessed 3 July 2023.

"Stuxnet." Wikipedia, https://en.wikipedia.org/wiki/Stuxnet . Accessed 3 July 2023.

"Timeline: China's Maritime Disputes." Council on Foreign Relations,

https://www.cfr.org/timeline/chinas-maritime-disputes . Accessed 21 July 2023.

"Topic: Collective defence and Article 5." NATO, https://www.nato.int/cps/en/natohq/topics_110496.htm . Accessed 12 July 2023.

"Topic: Countering hybrid threats." NATO, https://www.nato.int/cps/en/natohq/topics_156338.htm . Accessed 12 July 2023.

"Topic: Readiness Action Plan." NATO, 1 September 2022, https://www.nato.int/cps/en/natohq/topics_119353.htm . Accessed 14 July 2023.

"Training and exercises." Hybrid CoE, https://www.hybridcoe.fi/training-and-exercise/ . Accessed 14 July 2023.

Ucko, David H., and Thomas A. Marks. "Redefining Irregular Warfare: Legitimacy, Coercion, and Power - Modern War Institute." Modern War Institute -, 18 October 2022, https://mwi.westpoint.edu/redefining-irregular-warfare-legitimacy-coercion-and-power/ . Accessed 21 July 2023.

"United Nations Charter (full text) | United Nations." the United Nations, https://www.un.org/en/about-us/un-charter/full-text . Accessed 7 August 2023.

"Warsaw Summit Communiqué issued by NATO Heads of State and Government (2016)." NATO.int, 1 July 2022, https://www.nato.int/cps/en/natohq/official_texts_133169.htm . Accessed 7 August 2023.

MULTIMEDIA SOURCES

Hagelstam, Axel. "NATO Review - Cooperating to counter hybrid threats." NATO.int, 23 November 2018, https://www.nato.int/docu/review/articles/2018/11/23/cooperating-to-counter-hybrid-threats/index.html . Accessed 16 July 2023.

"Issue 4/2020 The Kremlin's Hybrid War. The case of Georgia." New Eastern Europe, 8 July 2020, https://neweasterneurope.eu/2020/07/08/issue-4-2020-the-kremlins-hybrid-war-the-case-of-georgia/ . Accessed 16 July 2023.

"Sakharov Conference on Trolls, Disinformation and Hybrid Warfare." VDU, 14 May 2019, https://www.vdu.lt/en/sakharov-conference-on-trolls-disinformation-and-hybrid-warfare/ . Accessed 16 July 2023.

"The 2014 Sony hacks, explained." Vox, 3 June 2015, https://www.vox.com/2015/1/20/18089084/sony-hack-north-korea . Accessed 16 July 2023.