Study Guide

NATO

North Atlantic Treaty Organization

Universidad de Navarra | FACULTAD DE DERECHO | UNMUN MODEL OF UNITED NATIONS

Welcome Letter from the Chair:

Dear delegate,

Greetings!

Welcome to the North Atlantic Treaty Organization (NATO) Committee at the University of Navarra Model United Nations (UNMUN) 2025. The Dais is thrilled to have you join us to engage in discussions on some of the most pressing issues of our time.

This year marks the first appearance of the NATO Committee at UNMUN, making this a historic occasion for all of us. We are excited to delve into the following key topics: *evaluating NATO's role and challenges as a counterterrorism actor*; and *addressing defensive strategies in response to hybrid warfare strategies*. To support your research and understanding, we have prepared a comprehensive study guide, which serves as a roadmap to navigate the various aspects of these critical issues.

As this is an intermediate committee, the Dais anticipates delegates who bring a high level of passion, diplomacy, and skill to foster robust debate and learning. This committee is a safe space designed to enhance your knowledge and simulate the operations of the NATO committee. We encourage you to engage in debates with an open mind and a strong commitment; embrace challenges as opportunities for growth.

Delegates, you are the leaders of tomorrow. Take this opportunity to learn from each other and devise solutions for a better world. The Dais is confident that your intellectual curiosity will set a high standard, exceeding the expectations of the conference.

If you have any concerns, doubts, or inquiries, please do not hesitate to reach out to the Dais. Your success is our priority, and we are here to support you in every way possible.

Work hard and do your best—*the Alliance never takes peace for granted*.

Sincerely,

Patricia Eunice Marie de Guzman Macalindong

President

International Relations 4º, University of Navarra

Dario Esteban Rodrigo

Vice President

Data and Business Analytics 3º, IE University

Paula Las Heras Martinicorena

Secretary

International Relations 4º, University of Navarra

About the Committee: North Atlantic Treaty Organization

Description about NATO

The North Atlantic Treaty Organization (NATO) is a political and military alliance created during the Cold War as a mechanism to counter Soviet influence—including all members of the Warsaw Pact—and military presence in central and Eastern Europe after the end of WWII. NATO was founded on April 4th, 1949, in Washington D.C. (*Milestones in the History of U.S. Foreign Relations - Office of the Historian*, n.d.), where the leaders of 12 countries (Haglund, 2024) signed the North Atlantic Treaty, agreeing upon its 14 articles (NATO, n.d.-c).

After the fall of the Soviet Union, NATO was repurposed as a cooperative security organization that sought to foster dialogue with former Warsaw Pact members and to intervene and control conflicts in the European periphery, such as the Balkans or Eastern-most Europe (Haglund, 2024). Although these are some of their functions, NATO's main purpose is to serve as a collective defense mechanism in case one of its member countries is attacked or threatened by any force external to NATO. This is characterized by Article 5 of the North Atlantic Treaty, which states that "an armed attack against one or more of them in Europe or North America shall be considered an attack against them all" (NATO, n.d.-c).

To achieve these goals, NATO has established many different partnerships and dialogues, mainly based on geographic location, with countries external to NATO. These include the Partnership for Peace, in which 18 Eastern European and Central Asian countries are included; the Mediterranean Dialogue, of which 7 Middle Eastern and North African (MENA) countries are part; and the Istanbul Cooperation Initiative, composed of 4 gulf countries. Furthermore, NATO has other dispersed allies denoted as "Partners across the globe", composed of 9 countries in Oceania, Asia and America (NATO, n.d.-a). Although NATO cooperates with these numerous countries, they are not subject to the articles of the North Atlantic Treaty.

NATO is divided into civilian and military structures, with many other supporting organizations and agencies that aid NATO with its operations. The civilian body of NATO, divided between the NATO HQ, the Permanent Representatives and National Delegations, and the International Staff, carries out many of the political and administrative aspects of NATO operations. This includes budgeting, policy planning, and public diplomacy.

On the other hand, NATO also counts with the Military Committee, International Military Staff, and the Allied Command Operations and Transformations offices. These structures are more focused on the militaristic realm of NATO, dealing directly with military action such as troop positioning and management (NATO, n.d.-b).

Significance of NATO in modern geopolitical stability

NATO has proved to be a key factor in preserving global peace and stability. In light of the current geopolitical instability, there is a demand for multifaceted and comprehensive solutions that integrate military strength, diplomacy, and post-conflict stabilization. Only the widest possible coalition of international actors can provide these components effectively (NATO, 2022). As a result, NATO is not only developing security partnerships with countries across the Mediterranean, the Gulf region, and the Pacific area.

The Alliance is also engaging with international and non-governmental organizations involved in institution-building, governance, development, and judiciary reform. Whether helping to build lasting peace in Kosovo, securing the Mediterranean Sea, or providing assistance to the African Union, NATO has been increasing cooperation with other international organizations to leverage their capabilities in reconstruction and civil society building.

Moreover, Russia’s illegal annexation of Crimea in 2014 and its unjustified and unprovoked attack on Ukraine are an alarming reminder of the importance of NATO’s core task: *collective defense* (NATO, 2022). The resulting sense of shared security among NATO members contributes to stability in the Euro-Atlantic area and creates a spirit of solidarity and cohesion within the Alliance. NATO strives to secure a lasting peace in Europe and North America, based on its member countries’ common values of individual liberty, democracy, human rights and the rule of law (NATO, 2022). These shared values unite a diverse group of Allies on both sides of the Atlantic. Thus, NATO embodies the transatlantic bond between them, whereby the security of Allies in Europe and North America is inextricably linked.

Since its founding in 1949, the transatlantic Alliance's flexibility, embedded in its original Treaty, has allowed it to suit the different requirements of different times (NATO, 2022). In the 1950s, the Alliance was a purely defensive organization. In the 1960s, NATO became a political instrument for détente. In the 1990s, the Alliance was a tool for the stabilization of Eastern Europe and Central Asia through the incorporation of new partners and Allies (NATO, 2022). In the first half of the 21st century, NATO faces an ever-growing number of new threats. However, as the foundation stone of transatlantic peace and freedom, NATO is ready to meet these challenges.

NATO's key functions

1. Deterrence and collective defense

Deterrence and defense are fundamental tasks for NATO. The Alliance achieves deterrence by upholding a credible defense posture that integrates a balanced mix of nuclear, conventional, and missile defense capabilities, along with space and cyber capabilities. Allies are significantly bolstering the Alliance's deterrence and defense measures, reinforcing their article 5 commitment to mutual defense.

2. Civilian and military crisis prevention and management

NATO thoroughly considers both military and non-military elements of crisis management, striving to enhance practical collaboration across all levels with pertinent organizations and stakeholders in the planning and execution of operations. This comprehensive approach ensures a coordinated and effective response to crises, leveraging the strengths and capabilities of diverse partners. By integrating civilian and military efforts, NATO aims to address complex security challenges more efficiently. Continuous improvement and adaptation in cooperative practices are key priorities, reinforcing NATO's ability to maintain peace and stability in an ever-evolving global security environment.

3. Security cooperation

Security cooperation is a key aspect of NATO’s mission, involving dialogue and practical cooperation with partners on various political and security-related issues, such as global challenges like terrorism and climate change. These partnerships are mutually beneficial and enhance security for the international community. NATO believes that Euro-Atlantic security is best ensured through a broad network of partner relationships with countries and organizations worldwide. These partnerships contribute significantly to NATO’s core tasks. Over the past two decades, NATO has established structured partnerships with countries in the Euro-Atlantic area, the Mediterranean, and the Gulf region, as well as individual relationships with partners across the globe.

References

Haglund, D. G. (2024, June 15). North Atlantic Treaty Organization (NATO) | History, Structure & Purpose. Encyclopedia Britannica. https://www.britannica.com/topic/North-Atlantic-Treaty-Organization#ref5320

Milestones in the history of U.S. Foreign Relations - Office of the Historian. (n.d.). https://history.state.gov/milestones/1945-1952/nato

NATO. (n.d.-a). NATO’s partnerships. NATO. https://www.nato.int/cps/en/natohq/topics_84336.htm

NATO. (n.d.-b). Structure. NATO. https://www.nato.int/cps/en/natohq/structure.htm#CS

NATO. (n.d.-c). The North Atlantic Treaty. NATO. https://www.nato.int/cps/en/natohq/official_texts_17120.htm

Topic A: Evaluating the Role of NATO and Challenges as a Counterterrorism Actor

Introduction

Terrorism is one of the most significant threats to humanity. The tragic deaths and widespread devastation caused by events such as the September 11, 2001 (9/11) attacks have underscored the urgent need for comprehensive action by states. These actions should focus on promoting the welfare of their citizens and steadfastly upholding human rights. In light of these threats, ensuring the security of every individual is not merely a privilege but a fundamental right. It is the paramount duty of the state to protect its people, safeguarding their lives and freedoms against the scourge of terrorism.

Counterterrorism has been a cornerstone initiative undertaken by international organizations to safeguard the welfare of people and uphold human rights. It is important to note that states implement a wide range of measures across military, political, economic, and legal domains to combat terrorism through various means. Approaches to counterterrorism are diverse and multifaceted, including preventive measures, military interventions, intelligence operations, and diplomatic strategies.

However, not all counterterrorism measures adhere to the principles of human rights and ethical conduct. In some instances, actions taken under the guise of counterterrorism have involved torture and ill-treatment, violating practical, legal, and ethical safeguards designed to prevent such abuses. These actions not only undermine the legitimacy of counterterrorism efforts but also erode trust in the institutions meant to protect and serve the public. It is crucial for counterterrorism strategies to balance security objectives with a steadfast commitment to human rights and the rule of law.

NATO's fundamental goal is to safeguard the Allies' freedom and security by political and military means. This dual approach ensures that NATO can address a broad spectrum of threats, ranging from conventional military aggression to unconventional threats like terrorism and cyberattacks. Politically, NATO fosters dialogue and cooperation among member states, promoting stability and preventing conflicts through diplomatic means. The alliance's political dimension is vital for consensus-building and collective decision-making, ensuring that all member states have a voice in shaping NATO's policies and strategies. Militarily, NATO maintains a robust and ready force capable of deterring and defending against any threats to the security of its members. This includes maintaining a state of readiness, conducting joint training exercises, and developing capabilities to respond swiftly to crises. The integrated military structure of NATO allows for seamless coordination and interoperability among the armed forces of member states, enhancing the alliance's overall effectiveness.

NATO remains the principal security instrument of the transatlantic community and an expression of its common democratic values. The alliance embodies the collective defense principle, enshrined in Article 5 of the North Atlantic Treaty, which states that an attack against one member is considered an attack against all. This principle not only deters potential aggressors but also reinforces the commitment of member states to stand together in defense of their shared values and interests. Moreover, NATO's operations and missions extend beyond its member states, contributing to international peace and stability. Through partnerships and cooperative security arrangements, NATO engages with countries around the world, promoting democratic governance, rule of law, and human rights. The alliance's efforts in crisis management, conflict prevention, and cooperative security highlight its role as a cornerstone of global security architecture, dedicated to preserving the ideals of freedom, democracy, and collective defense.

Keywords

1. **Counterterrorism:** “measures designed to combat or prevent terrorism” (Merriam-Webster, 2024).

2. **Human Rights:** “rights inherent to all human beings, regardless of race, sex, nationality, ethnicity, language, religion, or any other status” (United Nations, n.d.).

3. **Collective defense:** “an attack against one Ally is considered as an attack against all Allies…The principle of collective defense is enshrined in Article 5 of the North Atlantic” Treaty (North Atlantic Treaty Organization, n.d.).

4. **Deterrence:** “theory that criminal penalties do not just punish violators, but also discourage other people from committing similar offenses by instilling doubt or fear of the consequences (Minnesota House of Representatives, 2019).”
5. **Cybersecurity:** “art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information” (State of Nevada, 2021).
6. **Crisis Management:** “identification of a threat to an organization and its stakeholders in order to mount an effective response to it” (Hayes, 2024).

Background/Context

The significance of NATO’s formation

The formation of NATO signaled an early commitment to countering various threats. Initially established to provide collective defense and protect its members from the Soviet Union during the Cold War, NATO's scope quickly expanded to address a wide range of security concerns. The security environment further shifted with Russia’s annexation of Crimea in 2014 and the full-scale invasion in 2022. NATO's proactive approach, which included intelligence sharing, joint military exercises, and coordinated strategies, underscored the alliance's adaptability in responding to evolving threats and its long-term commitment to maintaining international stability.

NATO’s role in counterterrorism evolved significantly after the 9/11 attacks, which profoundly reshaped global security priorities. In response to this act of terrorism, NATO invoked Article 5 of the North Atlantic Treaty for the first time in its history, declaring that an attack against one member was an attack against all. This marked a significant shift in NATO’s strategic concept, emphasizing the need to combat terrorism as a primary security concern.

Subsequent updates to NATO's Strategic Concept reflected this new focus, incorporating comprehensive counterterrorism measures into its core objectives. The alliance's post-9/11 reorientation included enhancing rapid response capabilities, strengthening intelligence cooperation, and expanding partnerships with non-member countries. These efforts highlighted NATO's crucial role in international security, dedicated to countering the persistent threat of terrorism while upholding the principles of collective defense and mutual support.

Expansion of NATO’s counterterrorism strategies

1. *NATO's Strategic Concepts and the Inclusion of Counterterrorism*

NATO’s Strategic Concepts, which outline the alliance's overarching goals and strategies, have increasingly incorporated counterterrorism as a central focus. The shift began prominently after the 9/11 attacks, recognizing terrorism as a major threat to international peace and security. This inclusion has guided NATO’s efforts to adapt and enhance its capabilities to prevent and respond to terrorist activities effectively.

2. *Policy Frameworks and Cooperative Security Measures*

To support its strategic goals, NATO has developed comprehensive policy frameworks and cooperative security measures. These policies ensure a coordinated approach to counterterrorism among member states and partners. They include initiatives to improve intelligence sharing, enhance military readiness, and foster international cooperation. The frameworks facilitate joint exercises, training programs, and operational planning, enabling NATO to respond swiftly and effectively to terrorist threats.

3. *Development of Policies and Frameworks Post-9/11*

In the aftermath of the 9/11 attacks, NATO significantly expanded its counterterrorism policies and frameworks. One of the key developments was the establishment of NATO’s Counter-Terrorism Policy, which outlines the alliance's approach to preventing and responding to terrorist threats. This policy emphasizes the need for comprehensive measures, including deterrence, defense, resilience, and recovery.

NATO has also strengthened its partnerships with various countries and international organizations to enhance global counterterrorism efforts. These partnerships involve collaborative initiatives, such as capacity-building programs, information exchange, and joint operations. NATO's engagement with partners around the world aims to build a unified front against terrorism, leveraging collective expertise and resources.

4. *Key Partnerships and Initiatives*

NATO's counterterrorism initiatives post-9/11 include partnerships with the European Union, the United Nations, and other international organizations. These collaborations focus on areas such as border security, cyber defense, and countering violent extremism. Through initiatives like the Partnership Action Plan against Terrorism (PAP-T) and the Defense Against Terrorism Program of Work (DAT-POW), NATO works to address the root causes of terrorism and enhance the capabilities of member and partner nations.

In summary, the expansion of NATO's counterterrorism strategies is marked by the integration of counterterrorism into its Strategic Concepts, the development of robust policy frameworks, and the strengthening of international partnerships. These efforts underscore NATO's commitment to combating terrorism and ensuring the security of its member states and the broader international community.

Current Status

Operations and Missions

As part of NATO's comprehensive approach to deterrence and defense, NATO's counter-terrorism efforts span a variety of operations and missions, both within its territory and beyond its borders (NATO, 2024).

1. *Global Coalition to defeat the Islamic State of Syria and Iraq (ISIS)*

Since 2017, NATO has been a member of the Global Coalition to Defeat ISIS. As a member of the Coalition, NATO has been playing a key role in the fight against international terrorism, through intelligence-sharing and through its work with partners to project stability in the Euro-Atlantic area and beyond (NATO, 2024). At the 2016 NATO Summit in Warsaw, Allied Leaders agreed to support the Coalition by providing NATO AWACS surveillance aircraft, which began patrols from Konya Airfield in Türkiye in October 2016.

2. *NATO Mission Iraq*

In February 2018, the Alliance decided to launch NATO Mission Iraq, a non-combat advisory and capacity-building mission, at the request of the Iraqi government and the Global Coalition (NATO, 2024). The aim was to strengthen Iraqi security forces and institutions so that they could prevent the return of Daesh/ISIS, to fight terrorism and to stabilize the country. The mission's scope was expanded in February 2021 and August 2023 at the request of the Iraqi government and operating in full respect of Iraq's sovereignty while cooperating closely with other international partners such as the Global Coalition, the UN and the EU (NATO, 2024).

3. *Operation Sea Guardian*

NATO also engages in counter-terrorism efforts at sea through Operation Sea Guardian, a flexible and versatile maritime security operation that is able to perform different maritime security tasks, including countering terrorism at sea if required. Currently, this operation is active in the Mediterranean Sea (NATO, 2024). It succeeded Operation Active Endeavour, which was launched in 2001 under Article 5 of NATO's founding treaty as part of NATO's immediate response to the 9/11 terrorist attacks to deter, detect and, if necessary, disrupt the threat of terrorism in the Mediterranean Sea (NATO, 2024). Active Endeavour was terminated in October 2016.

4. *Afghanistan*

International Security Assistance Force (ISAF) Mission in Afghanistan (2003-2014) was established in order to help the government extend its authority and implement security to prevent the country from becoming a safe haven for international terrorism, after 9/11 and the ties between Al-Qaeda and the Taliban (NATO, 2024). Following the end of ISAF, NATO launched the non-combat Resolute Support Mission (RSM) to train, advise and assist the Afghan security forces, which ended in September 2021, after the Allies decided to withdraw RSM forces starting in May 2021(NATO, 2024).

Strategic review: challenges

1. *Diverse threats and asymmetric warfare*

In the last decade, the globalization of Jihadi extremism and the rise of homegrown terrorism, motivated by both right and left extremist ideologies, have led to major changes in terrorists' strategies and tactics. According to Stoian Karadeli (2021), these include strong connections between terrorist organizations, insurgent groups, and international organized crime; the emergence of homegrown terrorists and "lone wolves" motivated by various ideologies with duplicate tactics; the reliance on complex funding mechanisms; the use of sophisticated audience-oriented propaganda; and access to advanced technologies that enable unconventional high impact operations.

Moreover, the so-called "trinity of terrorism" has made the lines between various group ideologies more blurred, facilitating the symbiotic relationship between the terrorist actors in terms of narrative, strategy, and operational tactics (Karadeli, 2021). While the Salafi-jihadi terrorist threat has become more credible with its constant online presence and the idea of a virtual Caliphate, the long-ignored threat of homegrown terrorism has hit the core of our modern societies, motivated by various extremist ideologies. These evolving trends in terrorism significantly impact NATO's role as a counterterrorism actor by expanding the definition and scope of terrorist threats. NATO allies also acknowledge the imperative of developing the capabilities needed to counter these threats. Key measures include assisting member and partner countries in enhancing their counterterrorism capabilities through training, resource provision, and best practice sharing; and enhancing intelligence sharing and coordination with organizations like the UN, EU, OSCE, and AU. These measures will be further developed in the study guide.

2. *Resource and capability constraints*

The second important aspect is related to the nature of NATO as an organization. Even in its primary military defense responsibility, NATO has no direct access to all the necessary capabilities. According to researchers (Santamato, 2013), with few exceptions such as political consultations and command and control, NATO’s assets and capabilities belong to its members. It is therefore not a coincidence that its planning process (the NDPP) represents one of the pillars of its integrated military structure. Through the NDPP, nations coordinate and apportion their capabilities to the Alliance’s level of ambition. In case of need, a Transfer of Authority (ToA) mechanism allows national forces to fall under the control of NATO’s Supreme Commander. Recently, and as a result of NATO’s operational experience and the development of a comprehensive approach to operations, the NDPP has expanded to encompass selected non-military capabilities, such as the area of logistics, stabilization, and reconstruction (NATO, 2024). However, these capabilities remain under national control, even when made available for NATO operations, posing challenges for integration and coordination, especially in counterterrorism (Santamato, 2013).

The policy guidelines link NATO's counterterrorism efforts to the NDPP but fail to connect NATO directly with national agencies responsible for relevant assets. This indirect access, mediated through various NATO committees, adds complexity and challenges due to national interagency processes (Santamato, 2013).

3. *Need to reconcile the horizontal and cross-cutting nature of the terrorist threat with the vertical reality of Alliance policies and structures.*

The policy guidelines for NATO's counterterrorism efforts face significant challenges due to a lack of clear structure and authority (Santamato, 2013). While establishing a counterterrorism section at NATO headquarters is a step forward, it doesn't resolve the confusion about roles and responsibilities. The guidelines fail to integrate counterterrorism efforts conceptually and strategically within NATO's overall structure.

The Terrorism Task Force (TTF), which is meant to coordinate these efforts, lacks executive power, leading to a gap in management and authority (Santamato, 2013). This results in counterterrorism activities being poorly coordinated and potentially treated as secondary to other military priorities. The absence of a clear command and control structure for counterterrorism within NATO risks diminishing the effectiveness of its counterterrorism policies (Santamato, 2013).

4. *Policy Developments: Recent policy changes and declarations related to counterterrorism.*

The 2022 NATO Strategic Concept shows notable continuity with the previous 2010 document in terms of content on terrorism and counterterrorism. However, this continuity does not adequately reflect the significant changes in the actors, scenarios, and trends of global terrorism in the last decade (Reinares, 2022). The new strategy lacks a collective reflection on how NATO operations and missions have influenced the evolution of the terrorist threat over the past 12 years. Only vague mentions are made of "learned lessons" in crisis management, including Afghanistan, applicable to the fight against terrorism.

Furthermore, both the 2022 and 2010 Strategic Concepts recognize terrorism as a direct threat to the security of citizens of allied countries and to international peace. Both documents recognize that terrorism continues to spread and that instability and conflict in certain regions contribute to this threat (Reinares, 2022). NATO remains committed to providing the necessary means of deterrence and defense against terrorism and to intensifying international cooperation.

The 2022 Strategic Concept includes some new nuances. It now describes terrorism as the "most direct asymmetric threat" to NATO allies and addresses terrorism "in all its forms and manifestations," suggesting a broader scope that includes Jihadist terrorism and other forms of terrorism, such as extreme right or state-sponsored (Reinares, 2022). Specific regions such as Africa and the Middle East, particularly North Africa and the Sahel, are identified as terrorism-prone areas. The strategy also specifies greater cooperation with the United Nations and the European Union (NATO, 2022).

Main Actors and Stakeholders

The Allies

When talking about terrorist members, groups or organizations, it is important to mention that NATO does not have a list system in which it names or recognizes them as such. This remains a national competence, leading to political and strategic divergences among NATO allies.

Türkiye has demanded “more solidarity” from NATO allies in its fight against terrorism. "It is not possible for us to accept the crooked relationship that some of our allies have established especially with the PYD/YPG, the extension of the terrorist organization PKK in Syria.” Türkiye defends that the YPG militia is a terrorist organization, closely tied to the Kurdistan Workers Party (PKK) militant group. Türkiye, the United States, and the European Union have listed the PKK as a terrorist organization; the YPG, however, has not. According to Dincel (2024), Türkiye has long expressed its complaints about the United States working with the PKK/YPG on the pretext of fighting Daesh/ISIS. Meanwhile, the international community has expressed its concerns about the oppression that the Kurdish people suffer in Türkiye. This treatment is the great point of dissension between the United States and Türkiye, since they are unconditional allies of the superpower, but at the same time a political and security threat to the stability of Türkiye (Martos, n.d.).

Furthermore, last year, Türkiye accused the BBC of supporting terrorists after the network aired a report on why Kurdish and Yazidi women join the PKK to fight ISIS. They have also used it as leverage on Sweden to delay the country’s accession to the Alliance. The Nordic country has amended its constitution, changed its laws, significantly expanded its counter-terrorism cooperation against the PKK, and resumed arms exports to Türkiye; all steps set out in the Trilateral Memorandum agreed in 2022 (NATO, 2024).

At the same time, Türkiye supports groups such as the Muslim Brotherhood, Hamas, ETIM/TIP, Al Nusra, and other Al Qaeda affiliates, which are considered terrorist organizations by countries such as China, Russia, the United States, the European Union, Israel, Egypt, and other Arab Gulf states. Türkiye's support to these groups has led Israel to formally complain to NATO and has prompted Germany to criticize Türkiye's ambitions for EU membership. These contradictions put NATO's legitimacy, coherence, and mission in jeopardy and therefore is an important challenge to tackle.

Partner Countries and International organizations

NATO is affected by and can affect political and security developments beyond its borders. To address counterterrorism, NATO seeks to strengthen its outreach to and cooperation with partner countries and international organizations (NATO, 2024). This includes improved threat analysis, more consultations, and the development of appropriate capabilities. Efforts can focus on one country or be multilateral within a regional framework and can include civilian and military activities.

<u>Consultations and Information Sharing:</u> NATO aims to ensure shared awareness of the terrorist threat and vulnerabilities among Allies and partners (NATO, 2024). Activities offered to partners in this area include partner briefings to Allies in various formats, staff-to-staff talks with visiting delegations, engaging partner experts from academia or think tanks to share expertise and opportunities for information and intelligence sharing.

<u>Training, Education, and Exercises:</u> This cooperation involves working with NATO Centres of Excellence (COE) and carrying out tailored workshops and training courses through the Science for Peace and Security (SPS) Programme, which promotes dialogue and practical cooperation between NATO member states and partner countries based on scientific research, technological innovation, and knowledge exchange (NATO, 2024a). For example, in 2023, partners from the Middle East and North Africa attended a CBRN Awareness for First Responders Course at the Joint Chemical, Biological, Radiological and Nuclear defense COE in order to build awareness of CBRN threats and the capacity of these partners to coordinate across military and civilian lines of response efforts. Additionally, NATO will

provide advisory support through the NATO defense Education Enhancement Programme (DEEP) for the standardization of counterterrorism education in Bosnia and Herzegovina and the Republic of Moldova (NATO, 2024c). As a result of multinational collaboration through the Partnership for Peace Consortium, NATO launched its first standardized curriculum on counterterrorism in June 2020, aiming to support interested Allies and partners in enhancing their capacities to develop national skills and improve counterterrorism strategies. The curriculum also serves as a reference document to support partner countries in addressing their education and training requirements relevant for fighting terrorism, under the framework of DEEP (NATO, 2024c). In 2021, the Alliance began using this standardized curriculum to deliver online courses to participants of the Odessa Military Academy and the National Defense University in Kyiv, Ukraine.

Capability Development and Support to Operations: Involves defense Against Terrorism Programme of Work (DAT-POW) and direct support to operations, such as Operation Active Endeavour, ISAF, and KFOR (NATO, 2024). Partners also bring their knowledge, experience, and resources to NATO's initiatives in advancing counter-terrorism capabilities. For example, Australia and New Zealand are part of the DAT-POW community and participate in the work on Electronic Counter Measures for Radio Controlled Improvised Devices.

Moreover, NATO provides defense and Related Security Capacity Building (DCB) packages to partners through a request driven process. These are programmes that provide strategic advice and practical assistance to partners, helping them build capacity in areas where NATO has expertise (NATO, 2023). For instance, the defense and Related Security Capacity Building package for Jordan was reviewed in 2021 and now comprises 15 initiatives, including some that are specifically aimed at supporting Jordan in its counterterrorism efforts, such as strategic communications, the non-proliferation of small arms and light weapons, maritime and land border security, and the development of a curriculum for Jordan's counter-terrorism education and training. Counterterrorism is also a high priority for partners such as Mauritania and Tunisia, for whom Allies agreed to include new DCB packages at the June 2022 Madrid Summit (NATO, 2024).

Science and Technology Cooperation: Programmes covering this domain include cooperation through the SPS Programme Collaboration with the Science & Technology organization (STO). Counterterrorism is one of the key priorities of the NATO SPS Programme; it enhances cooperation and dialogue between scientists and experts from Allies and partners, contributing to a better understanding of the terrorist threat, the development of detection and response measures, and the fostering of a network of experts (NATO, 2024). Activities coordinated by the SPS Program include: workshops, training courses, and multi-year research and development projects that contribute to identifying methods for the protection of critical infrastructure, supplies, and personnel; human factors in defense against terrorism; technologies to detect explosive devices and illicit activities; and risk management, best practices, and use of new technologies in response to terrorism (NATO, 2023a).

For example, since 2018, the SPS Program has overseen the Detection of Explosives and firearms to counter terrorism (DEXTER). This initiative aims to develop an integrated system of sensors and data fusion technologies capable of detecting explosives and concealed weapons in real time to help secure mass transport infrastructures, such as airports, metro, and railway stations (NATO, 2023a). DEXTER was successfully tested in a live demonstration at a metro station in Rome, Italy in May 2022. Eleven governmental and research institutions from five NATO Allies (Finland, France, Germany, Italy, and the Netherlands) and three partner countries (the Republic of Korea, Serbia, and Ukraine) have participated in DEXTER.

Civil Emergency Planning and Crisis Management: Activities offered to partners in this area include a strong cooperation with the Euro-Atlantic Disaster Response Coordination Centre (EADRCC) and the development of relevant training opportunities and exercises (NATO, 2024).

Cooperation with International organizations

NATO cooperates with the United Nations, the European Union, the Global-Counter Terrorism Forum, the International Criminal Police Organization – INTERPOL (ICPO–INTERPOL), and the Organization for Security and Co-operation in Europe (OSCE) to ensure that views and information are shared and that appropriate action can be taken more effectively in the fight against terrorism (NATO, 2024).

NATO works closely with the UN Counter-Terrorism Committee and its Executive Directorate as well as with the Counter-Terrorism Implementation Task Force and many of its component organizations, including the UN Office on Drugs and Crime (NATO, 2024). NATO's Centres of Excellence, and education and training opportunities are often relevant to UN counter-terrorism priorities, as is the specific area of explosives management. For instance, in March 2019, NATO and the UN launched a joint project to improve CBRN[1] resilience in Jordan, which has since been completed (NATO, 2024).

NATO and the European Union are both dedicated to tackling terrorism and the spread of weapons of mass destruction. They frequently share information on counter-terrorism initiatives and related efforts, such as protecting civilian populations from CBRN threats (NATO, 2024). Ongoing interactions and discussions with the European External Action Service's counter-terrorism section, the Council of the EU Counter-terrorism Coordinator, and other EU entities help to ensure alignment and mutual support.

In addition, NATO has established strong ties with the OSCE's Transnational Threats Department, particularly its Action against Terrorism Unit. Common areas of focus include gender and terrorism, border security, a comprehensive approach to counterterrorism, and countering terrorist financing (NATO, 2024).

NATO also works closely with INTERPOL in the fight against terrorism. A significant aspect of this collaboration involves the sharing of battlefield evidence and information between military and law enforcement agencies (NATO, 2024). For example, INTERPOL provides expertise for NATO training programs aimed at southern partners.

Furthermore, NATO engages with other regional organizations to address terrorism. In April 2019, NATO and the African Union (AU) conducted their first joint counter-terrorism training in Algiers (NATO, 2024). By December 2019, NATO had hosted its inaugural counter-terrorism dialogue with the AU. Since then, the AU's African Centre for the Study

[1] malicious use of Chemical, Biological, Radiological and Nuclear materials or weapons with the intention to cause significant harm or disruption.

and Research on Terrorism has been updating Allies regularly, and additional cooperative efforts are in progress.

Non-State Actors

1. Salafi-jihadi terrorist organizations: These include groups like ISIS and Al-Qaeda, which have established a strong presence and influence globally, using sophisticated propaganda and maintaining a virtual Caliphate (Karadeli, 2021).
2. Homegrown terrorists and lone wolves: These individuals are motivated by various extremist ideologies, both right-wing and left-wing, and operate independently or in small groups, making them difficult to detect and counter (Karadeli, 2021).
3. Insurgent groups: These groups often collaborate with terrorist organizations and engage in guerrilla warfare and other forms of asymmetrical combat (Karadeli, 2021).
4. International organized crime networks: These networks often overlap with terrorist organizations, providing funding, resources, and logistical support (Karadeli, 2021).
5. Extremist ideological groups: These include both right-wing and left-wing extremists who use terrorism to further their political agendas (Karadeli, 2021).
6. Cyberterrorists: Individuals or groups who use advanced technology to conduct cyber-attacks, disrupt critical infrastructure, or spread extremist propaganda (Karadeli, 2021).
7. Symbiotic terrorist actors: Groups or individuals who share tactics, strategies, and narratives, blurring the lines between different ideologies and fostering cooperation among various terrorist actors (Karadeli, 2021).

Case Studies

NATO’s Response to the September 11, 2001, Attacks

The September 11, 2001, terrorist attacks on the United States marked a pivotal moment for NATO. For the first time in its history, NATO invoked Article 5 of the North Atlantic Treaty. This invocation led to a significant shift in the role of NATO, transitioning from a traditional defensive alliance to an active participant in global counterterrorism efforts. The subsequent mission included support for the US-led invasion of Afghanistan and broader counterterrorism measures.

The question arises with the effectiveness of NATO’s Collective Defense Response, given the fact that it was the first time that NATO invoked Article 5.

- How effectively did NATO's invocation of Article 5 contribute to the global counterterrorism effort, particularly in the early stages of the Afghanistan conflict? Did NATO’s collective defense and support contribute to the dismantling of al-Qaeda infrastructure?

- What were the limitations and challenges faced by NATO in executing its role post-9/11? Consider issues such as the speed of response, coordination with non-NATO allies, and the integration of different national policies and strategies.

At the same time, the invocation of NATO continues to bring long-term impacts, and strategic adaptation must be addressed.

- How did NATO adapt its strategies and capabilities in response to the evolving nature of global terrorism post-9/11? Did NATO successfully transition from a primarily defensive alliance to an effective counterterrorism actor?

- How did individual NATO member states' contributions and varying national policies impact the alliance’s overall effectiveness in counterterrorism? What role should member states play in enhancing or reforming NATO’s counterterrorism strategies?

Russia's Annexation of Crimea

In 2014, Russia's annexation of Crimea from Ukraine was a significant geopolitical event that challenged the international order and NATO's role in countering aggression. The annexation not only violated Ukraine's sovereignty but also raised concerns about the security of NATO's Eastern European members. This situation prompted NATO to reassess its strategies for collective defense and deterrence in the face of hybrid threats and regional aggression.

NATO is challenged to study its effectiveness against regional aggression.

- How effective were NATO's responses, including enhanced defense postures and increased deployments to Eastern Europe, in deterring further Russian aggression? Did these measures achieve their intended goals of reassuring member states and maintaining regional stability?
- Military and Political Coordination: Was NATO's response well-coordinated among member states and aligned with broader international sanctions and diplomatic efforts? Did NATO effectively integrate its military strategies with political and economic measures to counter Russia's actions?

Consequently, there are implications to the strategic and operational adaptation of the organization.

- How did the annexation of Crimea highlight the challenges of hybrid warfare and non-traditional threats? What adaptations did NATO need to make to address these new types of threats, including information warfare and unconventional military tactics?
- Member States' Roles and Responsibilities: How did the annexation affect the roles and responsibilities of NATO member states in terms of collective defense and regional security? What more can member states do to support NATO's strategic adaptations and enhance collective security?

Supporting Materials

1. NATO’s Policy Guidelines on Counter-Terrorism: https://www.nato.int/cps/en/natohq/official_texts_228154.htm
2. NATO's Post-Cold War Relevance in Counter Terrorism: https://kuscholarworks.ku.edu/bitstream/handle/1808/21874/Maness_ku_0099M_14667_DATA_1.pdf?isAllowed=y&sequence=1
3. From blueprints to battlefields: How to ensure NATO’s future readiness: https://www.atlanticcouncil.org/blogs/new-atlanticist/from-blueprints-to-battlefields-how-to-ensure-natos-future-readiness/

Topic B: Addressing Defensive Strategies in Response to Hybrid Warfare Strategies

Introduction

The concept of hybrid warfare was first proposed by the US Marine Corps Lieutenant Colonel Frank G. Hoffman in 2006. Although there is no universally agreed definition of hybrid warfare, initially, it was considered a model of military action that combined conventional war procedures and irregular war (guerrillas, insurgencies, terrorism), and could include an indiscriminate use of violence and take place in a scenario where the distinction between combatants and non-combatants does not exist.

However, starting in the 1990s and especially in the early 2000s, the growing influence of audiovisual media and the digital revolution created the perfect environment for the development of the informational or cognitive domain, which has added to traditional media the infinite possibilities offered by the network of networks: The Internet. Actions such as espionage, sabotage and subversion are now carried out using cybernetic tools, which are difficult to regulate and to trace, and may be used alongside conventional operations. Thus, NATO states that hybrid threats "combine military and non-military as well as covert and overt means, including disinformation, cyber-attacks, economic pressure, deployment of irregular armed groups and use of regular forces". Moreover, "hybrid methods are used to blur the lines between war and peace and attempt to sow doubt in the minds of target populations. They aim to destabilize and undermine societies".

In addition, it is essential to consider that the speed, scale, and intensity of hybrid threats have increased during the last decade. Being prepared to prevent, counter, and respond to hybrid attacks, whether by state or non-state actors, is a top priority for NATO. This is linked with a worrying novelty: these hybrid strategies are no longer only used by non-state actors. The Strategic Concept approved at the Madrid Summit in 2022 warns of China and Russia's use of hybrid threats and their effects, even to the extent that Article 5 of the Washington Treaty might be invoked.

Russia’s activities in Crimea and the Donbas region of Ukraine provide a prominent example of hybrid warfare in action. NATO Secretary General Jens Stoltenberg described Russia’s actions as: “[using] proxy soldiers, unmarked Special Forces, intimidation and propaganda, all to lay a thick fog of confusion; to obscure its true purpose in Ukraine; and to attempt deniability.” It is important to remember how in 2014, Russia occupied Crimea through an operation of deception, accompanied by irregular tactics of disinformation, agitation and cyberattacks, aimed at installing a pro-Russian separatist insurgency in the Ukrainian region of Donbas. Seven years later, these hybrid tactics have been precursors to the invasion of Ukraine. Therefore, the Russian Federation uses sophisticated hybrid strategies, including political interference, malicious cyber activities, economic pressure and coercion, subversion, aggression and annexation. Coercive military posture and rhetoric are also used as part of the country’s hybrid strategies to achieve its political goals and undermine the rules-based international order.

Furthermore, NATO considers that China’s “malicious hybrid and cyber operations and its confrontational rhetoric and disinformation target Allies and harm Alliance security.” China uses its economic leverage to create strategic dependencies and enhance its influence by controlling key technological and industrial sectors, as well as critical infrastructure, and strategic materials and supply chains. (Nishizawa, 2023)

Considering all this, NATO is prepared to assist any Ally facing hybrid threats as part of its collective defense. The Alliance has developed a strategy for its role in countering hybrid warfare to help address these threats. Since 2016, NATO has declared that “hybrid actions against one or more members could lead to the invocation of Article 5 of the North Atlantic Treaty.” By July 2022, NATO leaders had endorsed comprehensive preventive and response options to counter hybrid threats. Another significant step was the creation of a hybrid analysis branch in NATO’s Joint Intelligence and Security Division to improve situational awareness. Additionally, NATO is enhancing its coordination with partners such as the European Union to address these threats more effectively. (NATO, 2024b)

NATO has a strategy for its role in countering hybrid warfare and stands ready to defend the Alliance and all Allies against any threat, whether conventional or hybrid. (NATO, 2024b)

Keywords

1. **Hybrid Warfare:** Although there is no straightforward definition, it is widely recognised that hybrid warfare is a strategic military theory that blends many different types of conventional and unconventional warfare strategies, alongside other methods of influence such as propaganda, diplomacy and cyberwarfare, among other strategies. Frank Hoffman first adopted this term in his 2006 paper "Conflict in the 21st Century: The Rise of Hybrid Wars" (G. Hoffmann, 2007).

2. **Asymmetric Warfare:** A warfare scenario in which two forces with greatly varying military power employ different tactics based on the available equipment of the mentioned forces (Merriam-Webster Dictionary, 2024).

3. **Guerilla Warfare:** Warfare strategy employed in asymmetric warfare scenarios in which a smaller military force engages a bigger military force in many small encounters. The main objectives of guerilla warfare strategies are to disrupt, sabotage, or delay the enemy's logistics and military operations (*Guerrilla Warfare*, n.d.).

4. **Cognitive Warfare:** Activities carried out alongside other tools and strategies to gain influence over behaviors and attitudes at different scales (individual, community or societal level) to gain a strategic advantage on an adversary's non-military population (NATO, 2024).

5. **Information Warfare:** A group's attempt to corrupt the integrity, veracity and content of another organization's information via many strategies such as fake news, censorship, or sabotage of communication channels (Bingle, 2023). Usually used as a means to an end in cognitive warfare scenarios.

6. **Propaganda:** The distribution of information, including facts, arguments, rumors, half-truths, or falsehoods, to influence public opinion. (Smith, 2024).

7. **Cyberattacks:** An attack launched at an organization's computer system, network or digital infrastructure that attempts to steal, expose or destroy information, disrupt information technology (IT) systems, and/or disable a service powered by the targeted network (*What Is a Cyberattack? | IBM*, n.d.).

8. **Cybersecurity:** The systems and protocols an organization's IT network have in place to defend itself from cyberattacks (*What Is Cybersecurity? | IBM*, n.d.).

9. **Weaponization:** The act of making something usable as a weapon or that it fulfils the role of such (Oxford Dictionary, n.d.). In terms of hybrid warfare, weaponization can range from the physical/tangible (migrants, energy) to the intangible (information, elections).

10. **Proxy:** A person or organization that has authorization to act for another one (Merriam-Webster Dictionary, 2024b). In terms of warfare, proxies are Non-State-Actors or Non-State-Affiliated Belligerent Groups funded by a state or organization to unofficially act as them to promote their interests.

11. **Coercion:** The act of persuading a third party to do something via force or threats (Collins Dictionary, n.d.). In terms of hybrid warfare, coercion can be diplomatic, economic, military, or resource based.

Background/Context:

History of Hybrid Warfare

Although Hybrid warfare is a recent phenomenon, many of the elements that are part of hybrid warfare can be traced back to ancient times. These elements often took the form of the weaponization of many elements such as food, water, and/or disease, as was the case in the Siege of Caffa in 1346, in which individuals struck with the Black Plague were lunged into Caffa's walls via catapults and cannons to inflict this deadly disease into their enemies (Wheelis, 2002). Other types of elements that now belong to hybrid warfare have also been used in ancient times, such as information warfare, coercion, and/or guerilla warfare strategies. Guerrilla warfare strategies have been reported to be used by Alexander the Great (Asprey, 1999) and have even been mentioned in Sun Tzu's Art of War, two centuries before Alexander the Great was born (The Editors of Encyclopaedia Britannica, 1998).

It was not until recent history, during the Cold War, that hybrid warfare started truly taking shape. Both main participants in the Cold War, during their fight for influence and the spread of their ideology, employed many innovative tools and strategies that helped establish what is now known as hybrid warfare. It is imperative to note that NATO has been fighting hybrid threats since its inception in 1949, as its main purpose was to serve as a political and military defensive force against the USSR (*Milestones in the History of U.S. Foreign Relations - Office of the Historian*, n.d.). Therefore, the use of hybrid tactics, by both sides, was key to expanding their respective agendas worldwide as none, at least at that time, of the hybrid strategies employed could count as direct attacks, therefore evading direct conflict.

The Cold War saw the rise of the use of proxies as belligerent groups, in which neither NATO or the USSR directly or indirectly supported one or more sides from an active conflict. This phenomenon, called proxy warfare (Baugh, 2023), was very prominent in Cold War era conflicts, such as the Soviet invasion of Afghanistan via Operation Cyclone (L. Barlett & S. Steele, 2003); the Korean War via direct involvement of the USA and Mao’s China, as well as via direct support from the USSR (AlliiertenMuseum, 2024); and even the Vietnam War, in which the Eastern Bloc provided and showed support to North Vietnamese forces while the USA and the Western Bloc were involved directly by supporting South Vietnam (CVCE, n.d.). The use of proxies was, and is, often a popular course of action to take due to financial and legal reasons, such cases are the USA’s use of mujahadeen or Iran’s use of Hezbollah to promote their agendas (Byman, 2018).

Paired up with the use of proxies, the Cold War gave rise to the use of information warfare. Given that IT systems like the ones available today did not exist at the time, cyber warfare was not as prominent, and the smaller cyberattacks that were carried out, mostly involved data theft and system disruption. Although both of the main parties involved in the Cold War were engaged in a computing arms race (Marine Corps University, n.d.), most of the information warfare strategies and operations were carried out in the physical world. Espionage and thus data theft saw an exponential increase in presence, granting both sides of the conflict different strategies to adopt to achieve the same goal. While the Western Bloc opted to invest and develop espionage technologies thus pioneering in cybersecurity, the Eastern Bloc chose to delve deeper to the human aspect, expanding their knowledge and capabilities about cognitive warfare (Macrakis, 2010). Furthermore, the use of propaganda (*Cold War Policies, Propaganda, & Speeches - Student Center | Britannica.com*, 2020) from both sides also showed early signs of engaging in information warfare and cognitive warfare, thus stressing the need for both sides to develop strategies to counter these methods.

Beyond the Cold War, hybrid warfare has been present in many conflicts in recent history. The weaponization of critical infrastructure and public services has become a significant challenge in the landscape of hybrid warfare. The targeting of public infrastructure, such as schools and hospitals is prohibited by the Geneva Convention (Human Rights Watch, 2014), however, there are no international laws that prohibit the "peaceful" military use of such buildings and facilities, purposes which include but are not limited to barracks and logistics centers (GCPEA, 2012). This occurred in the Russo-Ukrainian War, where Ukrainian forces have taken advantage of these policies and mobilized troops to schools and placed equipment near them to discourage Russian forces from engaging in direct combat (Gorbunova, 2024). Russian authorities have received international criticism for targeting these facilities while also engaging in the same practices of repurposing schools as barracks and logistics centers (Human Rights Watch, 2023), thus employing unconventional tactics that can be related to hybrid warfare.

Furthermore, Russian forces have taken advantage of Rules of Engagement (RoE) policies from Ukrainian and Western forces through the use and deployment of "Little Green Men"-soldiers that first appeared on the Ukrainian battlefield in 2014 and were characterized by wearing Russian standard issue uniform and equipment while wearing no flag to represent their side. Given that their allegiance to the Russian invading forces could not be proven and President Putin stated that these soldiers were part of "self-defense groups", no direct action could be taken towards these individuals; this allowed them to quickly advance and expand Russian presence in the region (Shevchenko, 2014).

Other noteworthy cases of the use of hybrid tactics can be seen in the South China Sea and the Middle East. In the South China Sea, Chinese forces have been employing numerous coercion and harassment methods to promote and impose their agenda on Taiwan. Most notably, China has engaged in what is known as "Gray Zone" warfare, which involves carrying out operations that cannot be quickly identified neither as direct aggressions–thus warring activities–nor as peaceful actions (Lim & Ang, 2024). China's use of non-state actors (NSAs) as proxies inside of Taiwan and their constant aerial and naval military operations around the island seek to harass Taiwanese authorities and discourage Taiwan's separatist movement and ideals, thus strategically benefitting the CCP (Aukia, 2023). In the Middle East, more specifically Lebanon and Syria, where insurgent groups such as Hezbollah have taken advantage of many tools in the hybrid warfare arsenal. Aside from being able to exploit all of the elements that belong to any Non-State-Actor (NSA), such as being able to operate across borders, civilian integration, as well as their exemption from having to follow international humanitarian law and all other rules established by many conventions; Hezbollah has taken part in numerous information warfare, propaganda, and cognitive warfare campaigns. Hezbollah's mantra is "If you haven't captured it on film you haven't fought." It dictates how the group effectively uses information warfare and propaganda to create a positive sentiment by showcasing their achievements and feats in the battlefield(Clarke, 2017). Aside from their dominance of information warfare, Hezbollah also has a presence in Lebanese politics as aside from a militant group they also have a political party (The Editors of Encyclopaedia Britannica, 2024), which allows them to play on as sides of the coin (both as non-state and state actors) and thus enjoy the strategic benefits that come with each. They have established alliances with Iran through their capabilities as a political party (Robinson, 2024), while also launching attacks on Israel Defense Forces (IDF) outposts in Northern Israel (Gritten, 2024), all while acting as an NSA.

The rise and exponential implementation of IT systems in organizations and networks have created a weak point in the critical infrastructure of the nation and organization. One of the most famous instances of critical infrastructure being disrupted via IT systems sabotage is that of the colonial pipeline hack of 2021. In May of 2021, a ransomware attack was carried out on the Colonial Pipeline, a very important oil pipeline that provides fuel for a great part of the East Coast. This ransomware attack forced the pipeline to shut down for a couple of days, causing massive fuel shortages and supply chain disruptions. This caused damages in the millions of dollars and even forced President Biden to declare a national state of emergency (Kerner, 2022).

Relevant Theory and Current Status:

Given that hybrid warfare is a recent phenomenon, and that there is no set definition for it, many academics have attempted to study its implications and intricacies. Among those studies, Kilcullen's Liminal Warfare framework stands out as a tool to identify and classify hybrid threats (Kilcullen, 2019). Kilcullen's liminal maneuver framework establishes different operation categories separated by detection thresholds, based on the level of knowledge on the existence of the threat/operation and the sponsor of such. Represented as a pyramid, Kilcullen establishes the density of operations in each category, with the operations in which less is known to be more frequent than those in which one has more information about them.

Kilcullen also established that the more that is known about an operation, and therefore the more it moves towards the top of the pyramid, the more actions can be taken, as it grants leaders more information and therefore justification and context to carry out another defensive operation to counter the offensive one. This framework has proven to be particularly useful in detecting and classifying different threats and operations in recent history, such as identifying the tactics and strategies involved in Russia's annexation of Crimea through their use of hybrid tactics in the form of the "Little Green Men" (Arizona State University, 2020), by identifying this operation as a *Covert Operation*, Ukrainian forces and their allies were able to approach the situation in a different manner and carry out further efforts to cross the attribution and then the response threshold.

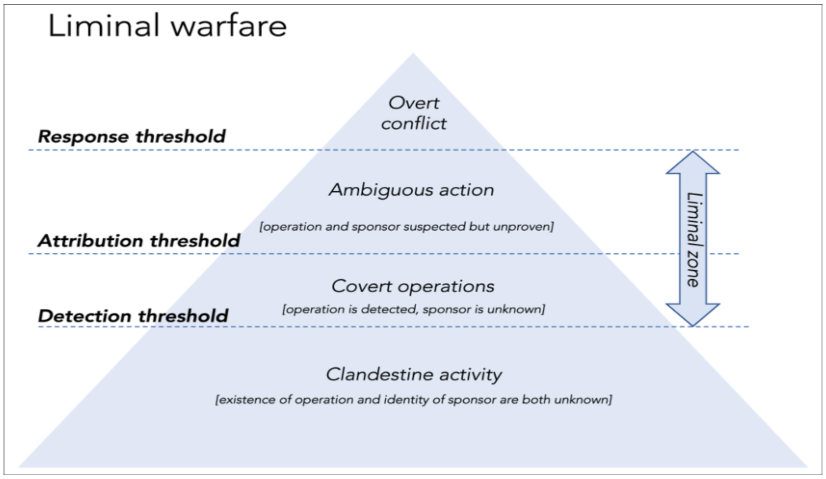
Liminal warfare
Overt conflict
Response threshold
Ambiguous action
[operation and sponsor suspected but unproven]
Attribution threshold
Covert operations
[operation is detected, sponsor is unknown]
Detection threshold
Clandestine activity
[existence of operation and identity of sponsor are both unknown]
Liminal zone

Figure 1: Kilcullen's Liminal Manoeuvre Framework (Kilcullen, 2019)

The main limitation of Kilcullen's framework is that it cannot be applied to operations and activities that transcend beyond the conventional defense and military realm (not excluding cyber operations and other related forms of sabotage). In terms of coercion and gaining influence on different regions of the world, as is the case with China's *Belt and Road Initiative* (BRI), a Chinese investment project that is present in many corners of the globe. The original purpose of the BRI is to develop regional infrastructure to create new trade routes between Asia and the rest of the world, and therefore promote economic activity in the countries and areas involved in the project (Jie & Wallace, 2022).

The project has successfully integrated 150 countries (including countries which are not officially recognised by the international community, most prominently Palestina) in Central Asia, East and West Africa, South and Central America as well as the Indo-Pacific and Europe (Wang, n.d.). Because of this project, China has been accused of engaging in hybrid warfare strategies by engaging in debt-trap diplomacy with some nations involved in the project (Nishizawa, 2023), raising concerns from the Global North and NATO regarding China's position as a threat due to the perception of neo-colonial and imperialist attitudes (Kleven, 2019). Diplomatic coercion, via a plethora of strategies such as the one adopted by the CCP, is considered a hybrid warfare strategy as it allows for influence and control of a country's decision-making and regional politics.

Another method of influence and control over a population, which has grown in popularity in the last decade, is that of propaganda. Throughout history, propaganda has been controlled and produced mainly by state-run institutions and other large institutions with great reach of communication (*Mass Media and Propaganda in 20th Century Europe*, 2022). However, the rise of social media and the democratization of communication and information thanks to the internet has allowed for a record high amount of information to be in circulation at once. It is estimated that every day, over 400 million terabytes of information are uploaded into the web (Duarte, 2024). The anonymous nature of the internet, and the lack of regulation in some aspects, allows for states and organizations to post propaganda in disguise, as the parties involved in creating and distributing said propaganda may employ fake accounts with no ties whatsoever to the government, influencers (as was the case with Russia (Atanesian, 2023)) or fake/half-fake news, the latter of which is the most used to promote and push ideologies or political positions.

Given the immense amount of data uploaded to the internet every day, it is very hard to verify the integrity and veracity of the applicable uploaded content. With the rise of AI, the amount of information that is true further decreases. As of 2019, only 60% of the traffic on the internet is by humans, the rest is done by bots and other AI masquerading as people (Read, 2018). Although COVID was the inflexion point for fake news awareness, we can see that although the general population has been more educated on the existence of these malicious pieces of information, many of these false news and information recollections are being posted by both states and non-state entities, both of which having the power to mobilise the population and create chaos as was the case with the recent English defense League (EDL) riots in Britain.

Disinformation regarding the identity of the main culprit behind the stabbing of three English girls, mainly his origin and religious identity which were thought to be Muslim and an illegal immigrant into the UK, police later debunked these facts but riots took over the streets of England and many ethnic and religious minorities in the main cities of the UK were attacked by furious EDL members (Mohamed, 2024). At the institutional and state level, the use of fake news as seen in the previous example is not as prominent, but rather instead the labelling of certain pieces of information as fake or censorship of content due to community guideline violations is commonly used, as is the case with many Lebanese journalists reporting on the current situation in the Gaza strip seeing their content being taken down of free-use platforms such as Twitter, Instagram or Facebook. Their accounts, aside from being hacked, were also mass reported, therefore reducing the veracity of their posts in the eyes of the social media companies thus making the system automatically flag these posts due to pattern recognition (Ersen, 2024).

Fraudulent news and propaganda are being spread mostly in cyberspace nowadays, as over 85% of adults in Europe and the USA gather most of their news from a smartphone, tablet or other device that connects to the internet (Atske, 2024). This means that cyberspace is one of the most important fronts in hybrid wars, as not only can parties engage in various forms of information warfare, but also in a variety of other forms of cyberattacks that target the vast computer networks and systems that efficiently power and help manage critical infrastructure. Cyberattacks on critical infrastructure have increased by over 70% in recent years (Yubico & Financial Times, n.d.), intending to gain control of or shut down the infrastructure's systems, as was seen with the colonial pipeline hack but most recently with Sweden's governmental network at the beginning of 2024. On January 19th, the Swedish government reported a major cyber incident amidst their integration into NATO. Government infrastructure which was critical to carry out the necessary bureaucratic steps to ensure Sweden's integration into NATO, alongside other public and private entities across many sectors, faced a ransomware attack carried out by the Akira Ransomware group, a collective of Russian hackers that were known to target government entities for profit (Adriaan, 2024).

However, ever since Sweden engaged in talks with NATO revolving around their accession, the nation has been a target for pro-Kremlin hacker groups that constantly launched ransomware attacks on their governmental IT infrastructure. This has led many NATO members to believe that Russian authorities are responsible for these attacks rather than hacker groups, which are used as proxies by the Kremlin (Blair & Blair, 2024). Sweden is still facing constant cyberattacks to this day.

With the scope of hybrid warfare being so vast, and to maintain oneself below the many thresholds that the liminal warfare framework establishes, many states and NSAs have taken to weaponizing different elements, such as information, energy, food or even migrants to further achieve their goals. The main goal of weaponizing these things is to disguise an artificial crisis or threat as a natural one. Such is the case with the Russo-Polish border, in which there has been a migration crisis since the start of the Russo-Ukrainian conflict.

Although first thought to be a natural migration crisis, immigrants from Syria, Iraq and Somalia, among others, consistently flooded the Estonian, Finnish and Polish borders with Russia and Belarus (McBride, 2023). This immigration crisis distracted the EU, giving them another "front" which they had to defend, making them lose focus on the Ukrainian front. Because of this, suspicions started arising on whether this was an artificial crisis. When questioned, the Kremlin denied all of the allegations (McBride, 2023. Although the sponsors were not ultimately confirmed, countries such as Finland closed all of their land borders to Russia as a defense mechanism (Walker, 2024), labelling Russia's practice as "Lawfare"

(Łubiński, 2021). Russia has also been known to weaponize energy, as throughout the entirety of the conflict, and as a response to the many sanctions imposed by the west, they have drastically raised gas prices with the purpose of weaponizing this energy source. Not only were they making energy more expensive for Europe while maintaining low prices for their Chinese allies (Reuters, 2023), but also recently reached its highest point since December of last year, as of August 10th (Reuters, 2023).

Proxies are still being consistently used by many states. Iran has been known to still fund Hezbollah, and therefore use them as a proxy (Robinson, 2024), the USA has and still employs military contractors as part of their combat forces (Shevchenko, 2014) and many other states use other organizations such as social activism groups, national and transnational criminal organizations or even other countries. One of the lesser-known cases of transnational criminal organizations being used as proxies are in the form of the many Mexican drug cartels. In order to sabotage the social cohesion of the United States, and also take advantage of the rampant opioid epidemic present in the country, Chinese brokers sold finished fentanyl to Mexican organizations, but after new policies were adopted, they switched to selling the raw ingredients so that it could be fabricated there.

Among the Mexican organizations that were making deals with China, some were discovered to be Mexican drug cartels that were smuggling fentanyl to the USA (Felbab-Brown, 2024). The most challenging part in identifying these organizations through these trades is that the chemicals are largely legal and used in the manufacturing of other legal pharmaceuticals but are often used to make dangerous opioids such as fentanyl (Felbab-Brown, 2024). Although these sellers are independent from the government, suspicions of CCP intervention in the drug’s supply chain have been raised to the point where the US government has placed sanctions on the country’s pharmaceutical industry (John et al., 2023). One of the Kremlin’s main proxies surprisingly is not a big hacker group (Lyngaas, 2024), Wagner Corps (Rondeaux, 2019) or even African rebels (Lawal, 2024), but rather their neighboring country: Belarus.

Russian authorities have been using Belarus as a tool to surpass western sanctions for years, even across the entire duration of the Russo-Ukrainian war up until now (Brzozowski, 2022). Belarus has been a key player in Russia’s alleged operation focusing on weaponizing migrants, as it served as a leeway to Poland (Niedzielski & Sokolowski, 2024), it has also been suspected that they have contributed to the Kremlin's use of Little Green Men by deploying Belarussian troops to contribute to the Kremlin's efforts (Stepanovych, 2023).

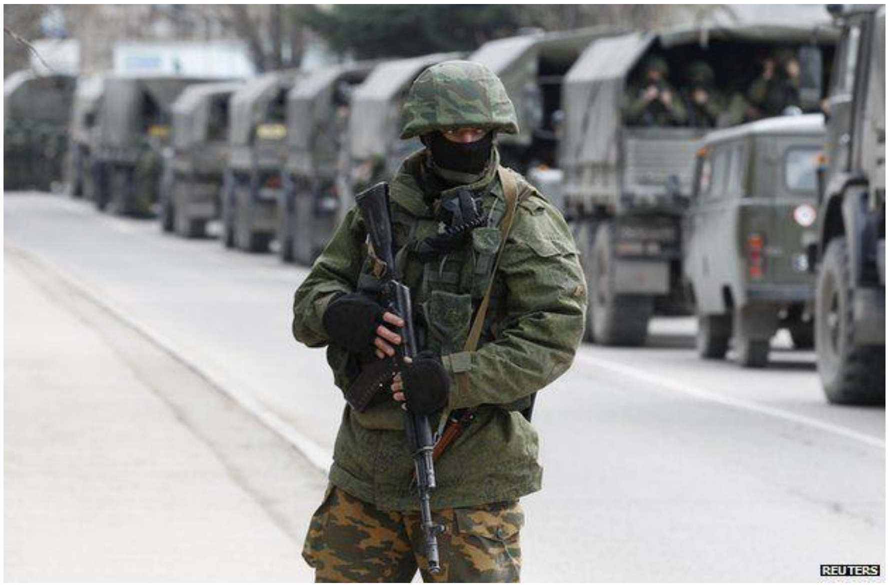

Figure 2: Little Green Man wearing Russian GRU uniform (Shevchenko, 2014)

Main Actors and Stakeholders

NATO Member States & Allies

NATO and its allies have been battling hybrid threats and engaging in hybrid warfare and defense since its inception. Given the many attempts from external forces to hinder NATO activities and well-being through hybrid tactics, such as the case of the delay in Sweden's incorporation into NATO caused by Russian hackers, NATO is in constant need to develop and refine their already existing strategies and frameworks (such as PDD (NATO, 2024b) or their many anti-propaganda and misinformation programs) to better counter these threats. NATO must develop these frameworks to protect its interconnected and global network and to facilitate the introduction of new members as was the case with Sweden.

Non-NATO Member States

Non-NATO states are also vulnerable and prone to be victims to different hybrid strategies. These states are more prone to information warfare, considering the major international media outlets are western and from NATO member states, and also diplomatic-economic warfare. Many non-NATO countries, such as China or Russia, have received numerous economic sanctions and demands from the international community, among many "anti-disinformation" campaigns. These countries, faced with numerous threats of economic and information warfare, seek to expand and explore their arsenal of hybrid strategies to match NATO's conventional arsenal and roster of different hybrid defense mechanisms.

Civilian populations

Civilians, independently of their country of origin or residence, are especially vulnerable to hybrid warfare as they are the main target of certain hybrid strategies. Sabotage of essential services such as energy, food or transport, among others, directly affect civilian populations negatively, and can pose a threat to their general wellbeing and can even result in injury or death. Furthermore, civilian populations are especially prone to information warfare due to the rise of social media and unmoderated, unverified content.

Private Institutions

Some private institutions and companies that provide vital services or products to the general population as well as to the government are often targeted in hybrid operations. Telecommunication companies and internet providers, financial institutions, and cloud storage services are some of the most common and targeted privately owned infrastructure and servers by hybrid strategies. Not only does this directly affect civilian populations within a nation's borders, but can even affect international civilian populations, other important private institutions or even governmental/public agencies and institutions, including the military and their defense mechanisms.

Media Outlets

Media outlets, and social media platforms, are often targeted by both state and non-state actors in different ways in order to engage in different forms of information warfare. Media outlets are often censored, used for propaganda or victims of cyberattacks or extortion. Furthermore, with the rise of independent journalism and social media, the credibility of the information presented by these outlets is disputed and is therefore exploited to push false news or biased, half-truths.

Non-state actors/Belligerent Groups

NSAs, both belligerent and non-belligerent, are both often used in hybrid strategies as tools for larger actors, such as states, as part of their hybrid strategies to carry out a wide range of different operations without engaging in a full-scale conflict. Primarily, NSAs are employed in operations whose goals would not be achieved if they surpassed either the detection, attribution or response threshold present in Kilcullen’s liminal warfare framework. NSAs employed by state to act as proxies do not necessarily have to be belligerent groups, as has been the case throughout history with the mujahadeen (Byman, 2018) or Wagner corps, but hacker groups or other organizations such as media outlets can also be employed as proxies to engage in hybrid strategies.

List of References:

References Topic A:

1. Collective defence – Article 5. (n.d.). North Atlantic Treaty Organization. https://nato-intl.com/collective-defence-article-5/#:~:text=Collective%20defence%20means%20that%20an,attacks%20against%20the%20United%20States
2. Cybersecurity Awareness. (2021). State of Nevada. https://dem.nv.gov/Resources/Cybersecurity_Awareness/#:~:text=Cybersecurity%20is%20the%20art%20of,integrity%2C%20and%20availability%20of%20information
3. Definition of counterterrorism. (2024). Merriam-Webster. https://www.merriam-webster.com/dictionary/counterterrorism
4. Dincel, S. (2024, July 11). Türkiye expects NATO allies to adopt its non-discriminatory approach to fight terrorists. www.aa.com.tr. https://www.aa.com.tr/en/turkiye/turkiye-expects-nato-allies-to-adopt-its-non-discriminatory-approach-to-fight-terrorists/3272551#
5. Do Criminal Laws Deter Crime? Deterrence Theory in Criminal Justice Policy: A Primer. (2019). Minnesota House of Representatives. https://www.house.mn.gov/hrd/pubs/deterrence.pdf
6. Hayes, A. (2024, August 15). Crisis management: Definition, how it works, types, and example. Investopedia. https://www.investopedia.com/terms/c/crisis-management.asp#:~:text=Crisis%20management%20refers%20to%20the,an%20effective%20response%20to%20it
7. Stoian Karadeli, A. (2021). NATO Defense Against Terrorism. European Security & defense ·, 6, 2021. https://www.utrgv.edu/pass/_files/documents/nato-defense-against-terrorism.pdf
8. Santamato, S. (2013). The New NATO Policy Guidelines on Counterterrorism: Analysis, Assessments, and Actions Strategic PerSPectiveS 13. https://inss.ndu.edu/Portals/68/Documents/stratperspective/inss/Strategic-Perspectives-13.pdf

9. NATO. (2024, July). Countering terrorism. NATO. https://www.nato.int/cps/en/natohq/topics_77646.htm#:~:text=NATO%27s%20Counter%2DTerrorism%20Policy%20Guidelines
10. NATO. (2024c, July). Defense Education Enhancement Programme (DEEP). NATO. https://www.nato.int/cps/en/natohq/topics_139182.htm
11. NATO. (2023). Press statement following the meeting between Türkiye, Sweden, and the NATO Secretary General. NATO. https://www.nato.int/cps/en/natohq/news_217147.htm
12. NATO. (2024a, April 29). Science for Peace and Security. NATO. https://www.nato.int/cps/en/natohq/78209.htm
13. Martos, Á. (n.d.). . Global Affairs and Strategic Studies. Facultad de Derecho. Global Affairs and Strategic Studies. https://www.unav.edu/web/global-affairs/detalle/-/blogs/turquia-en-la-otan-claves-de-un-futuro-incierto
14. Reinares, F. (2022, July 11). OTAN, nuevo Concepto Estratégico y antiterrorismo. Real Instituto Elcano. https://www.realinstitutoelcano.org/analisis/otan-nuevo-concepto-estrategico-y-antiterrorismo/
15. United Nations. (n.d.). Human rights. https://www.un.org/en/global-issues/human-rights#:~:text=Human%20rights%20are%20rights%20inherent,and%20education%2C%20and%20many%20more

References Topic B:

1. Adriaan. (2024, January 30). Intel Brief: Sweden endures major cyber incident ahead of NATO accession. *Dyami*. https://www.dyami.services/post/intel-brief-sweden-endures-major-cyber-incident-ahead-of-nato-accession
2. AlliiertenMuseum. (2024, February 5). *The Korean War (1950-1953) - AlliiertenMuseum*. https://www.alliiertenmuseum.de/en/thema/korean-war-1950-1953/
3. Arizona State University. (2020, August 26). *Contemporary Liminal Warfare: A case study, David Kilcullen | Future Security Initiative*. https://futuresecurity.asu.edu/events/contemporary-liminal-warfare-case-study-david-kilcullen
4. Asprey, R. B. (1999, July 26). *Guerrilla warfare | Facts, Definition, & Examples*. Encyclopedia Britannica. https://www.britannica.com/topic/guerrilla-warfare
5. Atanesian, B. G. (2023, September 1). *Ukraine war: Putin influencers profiting from war propaganda*. https://www.bbc.com/news/world-europe-66653837
6. Atske, S. (2024, August 7). News platform fact sheet. *Pew Research Center*. https://www.pewresearch.org/journalism/fact-sheet/news-platform-fact-sheet/
7. Aukia, J. (2023). China's hybrid influence in Taiwan: Non-state actors and policy responses. In *Hybrid CoE* (ISBN 978-952-7472-68-2). The European Centre of Excellence for Countering Hybrid Threats. https://www.hybridcoe.fi/wp-content/uploads/2023/04/20230406-Hybrid-CoE-Research-Report-9-Chinas-hybrid-influence-in-Taiwan-WEB.pdf
8. Baugh, L. S. (2023, August 31). *Proxy war | Definition, History, Examples, & Risks*. Encyclopedia Britannica. https://www.britannica.com/topic/proxy-war
9. Bingle, M. (2023, September 25). *What is information warfare?* University of Washington Jackson School of International Studies. https://jsis.washington.edu/news/what-is-information-warfare/
10. Blair, A., & Blair, A. (2024, May 3). Sweden's Nato accession: a cyberattack-filled saga. *Army Technology*. https://www.army-technology.com/features/swedens-nato-accession-a-cyberattack-filled-saga/?cf-view

11. Brzozowski, A. (2022, July 29). *Russia uses Belarus as proxy to bypass Western sanctions, opposition warns*. www.euractiv.com. https://www.euractiv.com/section/europe-s-east/interview/russia-uses-belarus-as-proxy-to-bypass-western-sanctions-opposition-warns/
12. Byman, D. L. (2018, May 21). Why engage in proxy war? A state's perspective. *Brookings*. https://www.brookings.edu/articles/why-engage-in-proxy-war-a-states-perspective/
13. Clarke, C. (2017, September 19). *How Hezbollah came to dominate information warfare*. RAND. https://www.rand.org/pubs/commentary/2017/09/how-hezbollah-came-to-dominate-information-warfare.html
14. *Cold War Policies, Propaganda, & Speeches - Student Center | Britannica.com*. (2020, October 19). Student Center. https://www.britannica.com/study/cold-war-policies-propaganda-and-speeches
15. Collins Dictionary. (n.d.). Coercion. In *Collins Dictionary*. https://www.collinsdictionary.com/dictionary/english/coercion
16. CVCE. (n.d.). *The Vietnam War*. https://www.cvce.eu/en/education/unit-content/-/unit/55c09dcc-a9f2-45e9-b240-eaef64452cae/5ad21c97-4435-4fd0-89ff-b6bddf117bf4
17. Duarte, F. (2024, June 13). Amount of data created daily (2024). *Exploding Topics*. https://explodingtopics.com/blog/data-generated-per-day
18. Ersen, E. T. (2024, January 6). *Social media censoring pro-Palestine voices, says Lebanese activist, claiming Israeli influence*. Anadolu Ajansi. https://www.aa.com.tr/en/middle-east/social-media-censoring-pro-palestine-voices-says-lebanese-activist-claiming-israeli-influence/3101663
19. Felbab-Brown, V. (2024, March 21). China, Mexico, and America's fight against the fentanyl epidemic. *Brookings*. https://www.brookings.edu/articles/china-mexico-and-americas-fight-against-the-fentanyl-epidemic
20. G. Hoffmann, F. G. H. (2007). Conflict in the 21st century: Rise of hybrid wars. In *The Commonwealth Institute*. Potomac Institute for Policy Studies. https://www.comw.org/qdr/fulltext/0712hoffman.pdf

21. GCPEA. (2012, November 20). *Lessons in War: Military use of schools and other education institutions during conflict - World*. ReliefWeb. https://reliefweb.int/report/world/lessons-war-military-use-schools-and-other-education-institutions-during-conflict
22. Gorbunova, Y. (2024). "Tanks on the Playground." In *Human Rights Watch*. https://www.hrw.org/report/2023/11/09/tanks-playground/attacks-schools-and-military-use-schools-ukraine
23. Gritten, D. (2024, June 12). *Hezbollah fires rocket barrages at Israel after commander killed*. https://www.bbc.com/news/articles/c6pp01dge3no
24. *Guerrilla Warfare*. (n.d.). https://carlcgsc.libguides.com/guerrillawarfare
25. Human Rights Watch. (2014). Commentary on the guidelines for protecting schools and universities from military use during armed conflict. In *Human Rights Watch*. https://protectingeducation.org/wp-content/uploads/documents/documents_commentary_on_the_guidelines.pdf
26. Human Rights Watch. (2023, November 9). Ukraine: War's toll on schools, children's future. *Human Rights Watch*. https://www.hrw.org/news/2023/11/09/ukraine-wars-toll-schools-childrens-future
27. Jie, Y., & Wallace, J. (2022, December 19). What is China's Belt and Road Initiative (BRI)? *Chatham House*. https://www.chathamhouse.org/2021/09/what-chinas-belt-and-road-initiative-bri
28. John, T., Xiong, Y., Culver, D., & Rappard, A.-M. (2023, March 30). The US sanctioned Chinese companies to fight illicit fentanyl. but the drug's ingredients keep coming. *CNN*. https://edition.cnn.com/2023/03/30/americas/fentanyl-us-china-mexico-precursor-intl/index.html
29. Kerner, S. M. (2022, April 26). *Colonial Pipeline hack explained: Everything you need to know*. WhatIs. https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know
30. Kilcullen, D. (2019). The evolution of unconventional warfare. *Scandinavian Journal of Military Studies*, *2*(1), 61–71. https://doi.org/10.31374/sjms.35

31. Kleven, A. (2019, May 6). *Belt and Road: colonialism with Chinese characteristics*. Lowy Institute. https://www.lowyinstitute.org/the-interpreter/belt-road-colonialism-chinese-characteristics
32. L. Barlett, D., & S. Steele, J. (2003, May 13). The Oily Americans. *Time*. https://web.archive.org/web/20081204024027/http://www.time.com/time/magazine/article/0,9171,450997-92,00.html
33. Lawal, S. (2024, August 8). Mali's spat with Kyiv: Is the Russia-Ukraine war spilling over into Africa? *Al Jazeera*. https://www.aljazeera.com/news/2024/8/8/malis-spat-with-kyiv-is-the-russia-ukraine-war-spilling-over-into-africa
34. Lim, T., & Ang, E. (2024, April 20). Comparing Gray-Zone tactics in the Red Sea and the South China Sea. *The Diplomat*. https://thediplomat.com/2024/04/comparing-gray-zone-tactics-in-the-red-sea-and-the-south-china-sea/
35. Łubiński, P. (2021). Hybrid warfare or hybrid threat – the weaponization of migration as an example of the use of lawfare – Case study of Poland. *Polish Political Science Yearbook*, *51*, 1–13. https://doi.org/10.15804/ppsy202209
36. Lyngaas, S. (2024, April 17). Russia-linked hacking group suspected of carrying out cyberattack on Texas water facility, cybersecurity firm says. *CNN*. https://edition.cnn.com/2024/04/17/politics/russia-hacking-group-suspected-texas-water-cyberattack/index.html
37. Macrakis, K. (2010). Technophilic Hubris and Espionage Styles during the Cold War. *Isis*, *101*(2), 378–385. https://doi.org/10.1086/653104
38. Marine Corps University. (n.d.). *Cold War computer arms race*. https://www.usmcu.edu/Outreach/Marine-Corps-University-Press/MCU-Journal/JAMS-vol-14-no-2/Cold-War-Computer-Arms-Race/
39. *Mass media and propaganda in 20th century Europe*. (2022, August 4). Europeana. https://www.europeana.eu/en/exhibitions/mass-media-and-propaganda-in-20th-century-europe
40. McBride, J. (2023, November 30). *Weaponized migration in eastern Europe's frozen North: Do not overlook Russian hybrid warfare - Modern War Institute*. Modern War

Institute. https://mwi.westpoint.edu/weaponized-migration-in-eastern-europes-frozen-north-do-not-overlook-russian-hybrid-warfare/

41. Merriam-Webster Dictionary. (2024a). asymmetrical. In *Merriam-Webster Dictionary*. https://www.merriam-webster.com/dictionary/asymmetric
42. Merriam-Webster Dictionary. (2024b). proxy. In *Merriam-Webster Dictionary*. https://www.merriam-webster.com/dictionary/proxy
43. *Milestones in the history of U.S. Foreign Relations - Office of the Historian*. (n.d.). https://history.state.gov/milestones/1945-1952/nato
44. Mohamed, E. (2024, August 2). Southport stabbing: What led to the spread of disinformation? *Al Jazeera*. https://www.aljazeera.com/news/2024/8/2/southport-stabbing-what-led-to-the-spread-of-disinformation
45. NATO. (2024a). *Cognitive Warfare*. ALLIED COMMAND TRANSFORMATION. https://www.act.nato.int/activities/cognitive-warfare
46. NATO. (2024b, March 7). *Countering hybrid threats*. https://www.nato.int/cps/en/natohq/topics_156338.htm
47. Niedzielski, R., & Sokolowski, C. (2024, June 4). *Why Poland says Russia and Belarus are weaponizing migration to benefit Europe's far-right | AP News*. AP News. https://apnews.com/article/poland-belarus-migrants-russia-ukraine-59d6050c2ea6853de3154150e8c9dcb5
48. Nishizawa, T. (2023, September 19). China's double-edged debt trap. *East Asia Forum*. https://eastasiaforum.org/2023/09/19/chinas-double-edged-debt-trap/
49. Oxford Dictionary. (n.d.). *weaponization*. Oxford Advanced Learner's Dictionary. https://www.oxfordlearnersdictionaries.com/definition/english/weaponization
50. Read, M. (2018, December 26). How much of the internet is fake? *Intelligencer*. https://nymag.com/intelligencer/2018/12/how-much-of-the-internet-is-fake.html
51. Reuters. (2023, September 8). Russia Gas price seen much lower for China than for Europe. *Reuters*. https://www.reuters.com/business/energy/russia-gas-price-seen-much-lower-china-than-europe-document-2023-09-08/
52. Robinson, K. (2024, July 31). What is Hezbollah? *Council on Foreign Relations*. https://www.cfr.org/backgrounder/what-hezbollah

53. Rondeaux, C. (2019, November 7). *Decoding the Wagner Group: Analyzing the role of private military security contractors in Russian proxy warfare*. New America. https://www.newamerica.org/future-security/reports/decoding-wagner-group-analyzing-role-private-military-security-contractors-russian-proxy-warfare/
54. Shevchenko, V. (2014, March 11). *"Little green men" or "Russian invaders"?* BBC News. https://www.bbc.com/news/world-europe-26532154
55. Smith, B. L. (2024, August 8). *Propaganda | Definition, History, Techniques, Examples, & Facts*. Encyclopedia Britannica. https://www.britannica.com/topic/propaganda
56. Stepanovych, R. (2023, March 27). *Belarus participated in the invasion of Ukraine as "Little Green Men." Zaborona investigation*. Заборона. https://zaborona.com/en/belarus-participated-in-the-invasion-of-ukraine/
57. The Editors of Encyclopaedia Britannica. (1998, July 20). *Guerrilla | Insurgency, Strategy & Tactics*. Encyclopedia Britannica. https://www.britannica.com/topic/guerrilla#ref69779
58. The Editors of Encyclopaedia Britannica. (2024, August 14). *Hezbollah | Meaning, history, & Ideology*. Encyclopedia Britannica. https://www.britannica.com/topic/Hezbollah
59. Walker, A. (2024, August 6). *Border and migration politics and the Kremlin's hybrid war*. UK In a Changing Europe. https://ukandeu.ac.uk/border-and-migration-politics-and-the-kremlins-hybrid-war/
60. Wang, C. N. (n.d.). *Countries of the Belt and Road Initiative (BRI) – Green Finance & Development Center*. https://greenfdc.org/countries-of-the-belt-and-road-initiative-bri/
61. *What is a Cyberattack? | IBM*. (n.d.). https://www.ibm.com/topics/cyber-attack
62. *What is Cybersecurity? | IBM*. (n.d.). https://www.ibm.com/topics/cybersecurity
63. Wheelis, M. (2002). Biological warfare at the 1346 siege of Caffa. *Emerging Infectious Diseases, 8*(9), 971–975. https://doi.org/10.3201/eid0809.010536
64. Yubico & Financial Times. (n.d.). *How critical infrastructure across the globe is targeted by cyber-attacks*. Financial Times.

https://www.ft.com/partnercontent/yubico/how-critical-infrastructure-across-the-globe-is-targeted-by-cyber-attacks.html?twclid=21cfxzwcksjpdwr0qo3nr6vxiw